5-7-2015

Reputational Privacy and the Internet: A Matter for Law?

Elizabeth Anne Kirley

REPUTATIONAL PRIVACY & THE INTERNET: A MATTER FOR LAW?

Elizabeth Anne Kirley

A Dissertation Submitted to
the Faculty of Graduate Studies
in Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

Graduate Program In Law
Osgoode Hall Law School
York University
Toronto Ontario

May 2015

ABSTRACT

Reputation - we all have one. We do not completely comprehend its workings and are mostly unaware of its import until it is gone. When we lose it, our traditional laws of defamation, privacy, and breach of confidence rarely deliver the vindication and respite we seek due, primarily, to legal systems that cobble new media methods of personal injury onto pre-Internet laws. This dissertation conducts an exploratory study of the relevance of law to loss of individual reputation perpetuated on the Internet. It deals with three interrelated concepts: reputation, privacy, and memory. They are related in that the increasing lack of privacy involved in our online activities has had particularly powerful reputational effects, heightened by the Internet's duplicative memory. The study is framed within three research questions: 1) how well do existing legal mechanisms address loss of reputation and informational privacy in the new media environment; 2) can new legal or extra-legal solutions fill any gaps; and 3) how is the role of law pertaining to reputation affected by the man-computer interoperability emerging as the Internet of Things? Through a review of international and domestic legislation, case law, and policy initiatives, this dissertation explores the extent of control held by the individual over her reputational privacy. Two emerging regulatory models are studied for improvements they offer over current legal responses: the European Union's General Data Protection Regulation, and American Do Not Track policies. Underscoring this inquiry are the challenges posed by the Internet's unique architecture and the fact that the trove of references to reputation in international treaties is not making its way into domestic jurisprudence or daily life. This dissertation examines whether online communications might be developing a new form of digital speech requiring new legal responses and new gradients of personal harm; it also

proposes extra-legal solutions to the paradox that our reputational needs demand an overt sociality while our desire for privacy has us shunning the limelight. As we embark on the Web 3.0 era of human-machine interoperability and the Internet of Things, our expectations of the role of law become increasingly important.

DEDICATION

This dissertation is dedicated to Jean and Austin – my sky, my earth

ACKNOWLEDGMENTS

To Jerry: my lifeline & companion in this and all my misadventures

For the sheer joy they bring: Liam Austin & Evan Michael

For their wisdom: Michael, Peggy, Brian, Mary, Peter, Martha, and Lauren

For their enduring friendship: Jan, Jay, Maria, Bill, Troy, Giovanni & John

For the lessons they teach: Dan, Stacey, Colin, Jasmine, Katie, Mike, Jamie, Anne, Colleen, Craig, Mary, Steve, Trish, Roy, Chris, Reid, Dan, Lara, Leena, Austin, Leland & Adam

For collegiality: Stephen, Betty, John, Mary, Thea, Pascale, Carolyn, Christine, Fariborz & Michael

For his infectious curiosity: Fr. Kevin Kirley CSB

For building my resolve and teaching me the craft: Margaret & Liora

Merci bien!

TABLE OF CONTENTS

Abstract……...ii
Dedication……...…iv
Acknowledgments……...…v
Table of Contents……...…vi
List of Tables……...……..ix
List of Illustrations……...……x

CHAPTER 1 Reputational Risks On the Internet……1

1.0 Introduction……...……...…1
1.1 The Challenge……..…2
1.2 The Medium: A (very) Brief History of the Internet…….…….....5
1.3 Law's Purpose in Online Societies…….....…..15
1.4 Limits to the Study: Of Apples and Oranges…….....….....16
1.5 Methodology……..……..…...20
1.6 Scope and Outline…….....….....22
1.7 Importance of the Study…….....24

CHAPTER 2 Literature Review……...…….....25

2.0 Introduction…….....25
2.1 Theorizing Reputation……..…..25
2.2 Theorizing Memory……..,…....46
2.3 Theorizing Privacy……...….....57
2.4 Privacy as a Social Construct……..72
2.5 Gaining Oblivion: the Right to be Forgotten…….....76

CHAPTER 3 The Technology Of Reputational Harm……....84

3.0 Introduction…….....84
3.1 Technological Idiosyncrasies of Digital Media…….....84
a Reconfiguring Information Bits…….....84
b Cloud Storage, Anonymity, and Attribution …….....87
i Anonymity & Attribution…….....88
ii Encoding, Encryption, & Hashing…….....90
iii Sharded or Fragmented Data…….....91
c Geolocation & Other Surveillance Capabilities……..…92
d Distinguishing Processor, Controller, & Publisher…….....96
e The Speed and Ambit of Dissemination……...….....99
f Memory and Durability: the Half Life Debate……..……...103
g Is Digital Speech Different?.....105

3.2 How Harm is Done.....108
a Exposure Harms: Technology & Case Examples.....108
i Exposure by Other Users.....108
ii Exposure by Self.....115
iii Exposure by Journalists.....121
b Disclosure Harms.....122
i Mishandling of Big Data.....122
ii Studies of Big Data Vulnerability 126
iii Data Brokers.....130
iv Cookies.....133
v Lingering Data & the Power of Internet Companies.....134
3.3 Case Studies.....140
a Exposure: The EU Mosley case.....140
b Disclosure: The US Martin case.....143
c Significance of Mosley & Martin Cases.....145
3.4 Summary.....148

CHAPTER 4 Legal Responses To Reputational Injury.....150

4.0 Introduction.....150
4.1 International, Transnational, & Domestic Response.....151
a Conventions & Declarations.....151
b EU/US Jurisdiction & Choice of Law in Internet Decisions.....168
c Domestic Responses.....179
4.2 Private Law Responses.....182
a What Plaintiffs Seek: Types of Remedy.....182
b Causes of Action.....184
i Defamation.....184
a Conceptual Difference.....185
b Public or Private Law?.....187
c The Requisite Elements.....188
d Internet Defamation.....193
ii Privacy torts.....204
iii Breach of Confidentiality.....209
iv Data Disclosure.....211
c ISP Liability.....216
4.3 Outliers: Criminal Defamation, Insult Laws, Opinion, & Creepiness.....223
a Criminal Defamation.....223
b Insult Laws.....228
c Opinion.....229
d Creepiness.....232
4.4 Reputation Online: Is Digital Speech Different?.....233
4.5 Is the Bench Ready for Digital Speech?.....235
4.6 Summary.....240

CHAPTER 5 "New Legalities" And Other Solutions.....243

5.0 Introduction.....244
5.1 User-Focused Legal Initiatives.....244
a Erasure Laws: The European Harmonized Approach.....244
i A Brief Legislative History.....244
ii Scope and Significance.....246
iii Responses to EUDR with Respect to Reputation.....251
b Do Not Track Laws: The US Sectoral Approach.....256
i A Brief Legislative History.....256
ii Scope and Significance.....258
iii Responses to DNT with Respect to Reputation.....260
c Can EU and US Agree on Data Protection Mechanisms?.....265
5.2 New Legal Responses.....267
a Internet Companies as Controllers: Google Spain.....267
b Reputational Injury as a Tort.....269
c A Discrete Law for Digital Speech.....270
i A Critical Need.....270
ii Aim, Scope, and Form of Speech Law.....275
5.3 Extra-legal Responses.....277
a Online Civic Monitoring.....277
b Online Reputation Ranking Systems.....281
c Expiry Dates.....284
d A Bifurcated Space for Online Speech.....285
5.4 Conclusion.....287

CHAPTER 6 Conclusion & Future Directions.....290

6.0 Summary of Major Findings.....290
6.1 Future Research.....300

Bibliography.....301
Appendices.....366

Appendix A Acronyms.....366
Appendix B Maps, charts, pictographs.....368
Appendix C Lexicon.....374

LIST OF TABLES

Table 1 2013 Broadband Speed Guide (FCC)……..……..100
Table 2 Social Media Profiles: what teens post 2006-2012……..……...……117

LIST OF ILLUSTRATIONS

Map 1.....368
Pictogram.....369
Map 2.....370
Chart 1.....371

CHAPTER 1 REPUTATIONAL RISKS ON THE INTERNET

1.0 Introduction

> Good name in man and woman, dear my lord,
> Is the immediate jewel of their souls:
> Who steals my purse steals trash[.][1]

Reputation is something we all have, treasure beyond wealth, and barely understand. It is a social construct, emerging from our interaction with others. Its loss provokes a profound sting to our sensibilities, but it is our society that feels most betrayed in their misplaced esteem and trust. Reputation poses several ironies: while we consider it our property, its control rests primarily with others. We strive to cultivate favourable impressions through our social interactions, but also crave that private space that hides from public view our more socially undesirable traits. We instinctively look to our laws for vindication and to make our reputation whole when it is injured: law is meted out in a very public forum, however, and so attracts the very publicity we shun. Law takes a somewhat circumspect interest in reputation, contextualizing it within our "family, home and correspondence"[2] or looking for confidential relationships in order to allocate blame. We are expected to provide proof of its loss, and a measure of our lost opportunities when we enter the legal forum, but are usually unaware of its value until it is gone. It is that drunken image the morning after, those shameful headlines that grow more painful with each detail, that tell us we no longer have the jobs, friends, or financial future we possessed the night before.

The Internet should have the capacity to make reputational damage go away.[3] After all, it can take our explanations to most corners of the geophysical world and convey our apologies in seconds. It can keep our denials and retractions available indefinitely and for any viewer. It can even publicize our own version of events, highlight our most admirable accomplishments, and manage our own rehabilitation

---

[1] WILLIAM SHAKESPEARE, OTHELLO: THE MOOR OF VENICE, Act III, Sc III, ll 155-157 (per Iago) as reprinted in The Oxford Shakespeare, Stanley Wells ed. (2008) (Othello).

[2] International Covenant On Civil And Political Rights, S. Executive Rep. 102-23, 999 U.N.T.S. 171, Dec. 16, 1966, Article 17 (ICCPR).

[3] 'Internet' indicates a networking infrastructure connecting millions of computers. The World Wide Web is an information-sharing model that is built on top of the Internet and uses only one of the languages spoken over the Internet. 'New media' is used broadly herein to include any means of mass communication using digital technologies.

campaign. All on an anonymous basis if we no longer seek the limelight. Why, then, is the Internet a contributory cause rather than the definitive answer to the most undesirable of human commodities, the stained reputation?

Our general familiarity with the Internet suggests that the qualities of digital media that make them most attractive for every kind of informational exchange also contribute to the permanence and severity of reputational damage. The offending story or image is conveyed instantaneously, anonymously if desired, in a fragmented fashion, indiscriminately if not directed to selected recipients, without editorial or managerial interception, and without significant cost. The purpose in choosing the Internet or other digital media for inflicting reputational damage is its guarantee of desired results: negative imputations go 'viral', are likely permanent, and appear unlikely to reflect badly on the anonymous perpetrator as forensic efforts at identification are time-consuming, expensive, and can involve even further invasions of the victim's privacy. Such efforts are, on balance, litigation-proof as victims of reputational damage are reluctant to admit their own indiscretions or their lack of privacy mechanisms for their online accounts.

Options for self-help are equally limited: containment (asking the author or photographer or news source to stop the story) is not feasible in light of ubiquitous distribution. Compensation is unlikely if the author of our misfortune is unknown, unrepentant, or without deep pockets. Vindication is chancy if we must reveal more of our private selves in order to prove the story's falsity; and erasure is beyond the technological capabilities of individuals and takes time if requested of the Internet Service Provider (Bell Mobility, for example) or social networking service (Facebook, for one). So we might be left to live with our past mistakes or vulnerabilities at the hands of advancing technologies.

1.1 The Challenge

Close to half the inhabitants of this planet communicate through the Internet, an information and communications system that, within the context of the planet's history,[4] has only been with us for a very few seconds.[5] Understandably, then, we have

[4] Paul S. Braterman, *How Science Figured Out the Age of Earth,* SCI. AMER. (20 Oct. 2013), http://www.scientificamerican.com/article/how-science-figured-out-the-age-of-the-

yet to devise a uniform code of online social behavior, either personal or communal. There circulates throughout the new media environment[6] much more of our private information than we would recognize or ever sanction: we find ourselves in distinctly new technological, cultural, and legal terrain. Online defamation and data disclosure test our laws because their technologies are so novel and their damage so profound.

This dissertation examines individual reputation on the Internet using a wide lens and an exploratory approach. More precisely, it sets as its aim the rethinking of the role of law as a response to online breaches of our *reputational privacy*. I devise that term to define a space we envision where our personally related information and data are kept undisclosed to the wider public in order to avoid any compromising of our future opportunities - social, professional, or financial. I consider two types of reputational harm that might result from our activities or those of others: our *exposure* through online postings that result in defamational harm; and the *disclosure* of our personally identifying information[7] or data without our knowledge or consent that impede our privacy. While recognizing that not all reputational impacts are related to privacy breaches, the latter are considered by this study because they put our private lives at increased online risk, particularly in the hands of the state and other authorities.

This study deals with three interrelated concepts: reputation, privacy, and memory. Those concepts are related in that the increasing lack of privacy involved in our online activities has had particularly powerful reputational effects, heightened by the Internet's susceptibility to misuse by those in authority, among others. In short,

---

earth/http://www.scientificamerican.com/article/how-science-figured-out-the-age-of-the-earth/ (National Sciences Foundation in 1926 adopted the radiometric timescale with which the age of the earth was calculated as 4.55 billion years). *See further* Appendix B, Map 1.

[5] *Timeline of Computer History,* computerhistory.org, http://www.computerhistory.org/timeline/?category=cmptr (reporting the first modern computer was built in 1939, was employed for Allied intelligence at Bletchley Park, England, during World War 2, became available for office use in developed nations in 1966 and for retail sales as a "personal computer" or PC in 1977).

[6] An emergent, more inclusive term than Internet or the Web would be "new media", defined by the New Media Institute as "all that is related to the internet and the interplay between technology, images and sound." *See* Bailey Socha and Barbara Eber-Schmid, *Defining New Media Isn't Easy*, NEW MEDIA, http://www.newmedia.org/what-is-new-media.html.

[7] *See* Paul M. Schwartz & Daniel L. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 85 N.Y.U. L. REV. 1814 (2011) (pointing out that Personally Identifiable Information, the test for privacy protection under US law, is a concept exhibiting a more nuanced meaning than legislators intended).

when it comes to individual reputation, the fact that information is accessed online makes a difference.

My focus is the reputation we exhibit when among the larger public, the "front stage" presentation of self that, with the emergence of our online communications, seems to be invading our backstage life as well. [8] That reconceptualization of the public/private divide is necessary because we are now in a communications era where the Internet has added a layer of technological and conceptual complexity for any user making best efforts to manage her social self.

Online reputational privacy presents a novel challenge for the legal profession as well. For judges, lawyers, and legislators, the task of allocating liability regarding breaches of reputational privacy involves a working knowledge of the online roles of Internet companies, search companies, government regulators, third party Internet users, and the individual cyber-citizen. Web behavior and digital speech present policymakers with completely novel challenges: how to come to terms with a culture of impetuous, unmediated, fractured, hyperbolic communications expressed on devices with duplicative memory and global distribution.

This dissertation poses three research questions: 1) how well do existing legal mechanisms address loss of reputation and informational privacy in the new media environment; 2) can new legal or extra-legal solutions fill any gaps; and 3) how is the role of law pertaining to reputation affected by the man-computer interoperability emerging as the Internet of Things?[9] I draw my legal analyses from international treaties and case law related to the United States (US) and the European Union (EU) and EU members. I choose those jurisdictions for three reasons: 1) the US and EU are the current prominent players in the digital economy; 2) they stem from very different cultural-legal traditions regarding reputation and privacy; and 3) they are under intense political pressure to collaborate in finding solutions to new privacy demands for individual Internet users now that we have entered the era of man-machine interoperability and wearable technologies.

---

[8] As explored in the pre-Internet world by sociologist ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

[9] John Naughton, *The Internet of Things: It's a Really Big Deal,* GUARDIAN (14 June 2014), http://www.theguardian.com/technology/2014/jun/15/networker-internet-of-things-john-naughton-hacking (providing a workable definition of the Internet of Things as a "machine-to-machine" connectivity without human interaction).

The question of whether victims of reputational harm perpetrated on the Web or the Internet would benefit from a discrete legal system, or would prefer a response outside of the legal system altogether, has received relatively little academic attention. Such an inquiry involves theoretical questions about the nature of reputation and how it is affected by concepts of memory and privacy. It also raises practical legal questions about proof of injury, choice of forum, and allocation of liability among Internet users and corporate intermediaries such as Internet companies, advertisers, and content carriers. The particular idiosyncrasies of Internet architecture play a significant part in defining the measure of control the individual Internet user can achieve over her reputation. It follows that the role of law regarding reputation calls out for reexamination. It is my purpose in this inquiry to expand on the observation of Internet scholar David Ardia, that "It's time again to rethink defamation law."[10] As we have moved out of the role of information acquisitor to content generator, and now face the novel role of computer companion, it is time again to rethink law's role involving reputational privacy.

1.2 The Medium: A (very) Brief History of the Internet

The computer in the modern world emerged as an answer to such visions as a "World Brain" by H.G. Wells in the 1930s,[11] an "arithmetical machine of the future" by Vannevar Bush in the 1940s,[12] and an arrangement of "man-computer symbiosis" predicted by J.C.R. Licklider in the 1960s.[13] Those pioneers of modern communications envisioned man-computer cooperation beyond the mere compilation and storage of very

---

[10] David Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. CIV. RTS-CIV. LIB. L. REV. 261, 262 (2010).

[11] H.G. Wells, *World Brain: The idea of a Permanent World Encyclopaedia,* ENCYCLOPEDIE FRANCAISE (Aug. 1937), https://sherlock.ischool.berkeley.edu/wells/world_brain.html (calling for a "unified, if not a centralized, world organ to 'pull the mind of the world together'").

[12] Vannevar Bush, *As We May Think,* ATLANTIC (1 July 1945), http://www.theAtlantic.com/magazine/archive/1945/07/as-we-may-think/303881/. Bush was an American engineer, inventor, and head of the US Office of Scientific Research and Development during WW2.

[13] *Internet Pioneers*, http://www.ibiblio.org/pioneers/licklider.html (describing Licklider as a US computer scientist and psychologist who foresaw the need for networked computers with easy user interfaces, such as point-and-click interfaces, digital libraries, e-commerce, online banking, and software that could migrate to wherever it was needed.

large masses of information, what today we unimaginatively label Big Data. Licklider in particular advocated collaboration between man and computer that would enable decision-making as problems and variables emerged, not as a pre-set computer function.[14] He examined his own work habits and determined that "Much more time went into finding or obtaining information than into digesting it".[15] Man-computer symbiosis could augment human intellect by relieving it from mundane, administrative tasks. Wells presciently foresaw that, "The whole human memory can be, and probably in a short time will be, made accessible to every individual."[16]

The most referenced beginnings of the Internet are the 1970s experiments by the US Department of Defense's Advanced Research Projects Administration (ARPA) to connect the military, defense contractors, and university researchers through dedicated telephone lines with direct access to a few key computers throughout the country.[17] That collaborative approach reflected the perception of American scientists who contributed their expertise to the World War 2 effort that winning the war was "a battle of scientific wits in which outcome depends on who can get there first with best."[18]

The ARPANET continued to support the development of communications protocols[19] in order to transfer data between computer networks. It was just one of many private and public initiatives, however, to shape the Internet. For example, in the 1970s numerous defence networks, the SAGE program that comprised the first airline reservation systems, and the remote computer services industry all contributed to

---

[14] J.C.R. Licklider, *Man-Computer Symbiosis,* IRE Transactions On Human Factors In Electronics, 4-11(March 1960), http://groups.csail.mit.edu/medg/people/psz/Licklider.html.
[15] *Id.*
[16] Wells, *supra* fn 11.
[17] This account is informed by the decision in *Shea on Behalf of American Reporter v. Reno,* 930 F. Supp. 915, 925-26 (S.D.N.Y. 1996) and *A Brief History of the Internet & Related Networks,* Internet Society, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet-related-networks. An account by JOHNNY RYAN, A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE, 8, attributes the origins of the modern Internet and computer to the technological expertise that fueled President D. Eisenhower's military industrial complex during WW2.
[18] Johnny Ryan, *How the atom bomb helped give birth to the Internet,* ARS TECHNICA (21 Feb, 2011), http://arstechnica.com/tech-policy/2011/02/how-the-atom-bomb-gave-birth-to-the-internet/3/.
[19] A protocol is a set of rules for transmitting data between electronic devices, such as computers. In order for computers to exchange information using the same sized packets of information, there must be a preexisting agreement as to how each side will send and receive it. Protocols are established by international or industry-wide organizations.

Internet development. The emergence of the persona computer (PC) in the 1980s brought a basic online email service, information providers such as Lexis and Dialogue, and the first global data communications networks to connect individual users to those services.[20] Compuserve and Prodigy represented the first generation of consumer networking services for personal computers in the 1980s. Videotext services formed the basis for national information infrastructures in many countries during the same period.[21] Those examples point to the simultaneous development of many networking activities, both commercial and private, and contribute to a more nuanced understanding of the origins of the Internet.

As several universities and commercial entities began to link their computers to various types of computer networks using OSI protocols,[22] funds from the US National Science Foundation as well as commercial communications enterprises helped build a high speed dial-up 'backbone' (Sprint and IBM for example) to form a series of linked, overlapping networks, the NSFNet.[23] In Europe, major international backbones such as NORDUNET provided similar connectivity to a growing number of computers on a large number of networks.[24] In Europe and elsewhere, support came from cooperative international efforts or consortium networks and through national research organizations, mostly non-profit entities with focused ideals about how the Internet should run. Within the United States, much of this support came from the federal and state governments for public access, but a considerable contribution was increasingly

---

[20] Martin Campbell-Kelly & Daniel Garcia-Swartz, *The History of the Internet: The Missing Narratives*, SSRN, http://ssrn.com/abstract=867087 (2 Dec. 2005).

[21] "A means of providing a written or graphical representation of computerized information on a television screen". (Dictionary.Com, http://dictionary.reference.com/browse/videotext.)

[22] Perhaps the most important *computer* protocol is OSI (Open Systems Interconnection), a set of guidelines for implementing networking communications between computers. The most important sets of *Internet* protocols are TCP/IP, HTTP, and FTP. (Encyclopedia Britannica, http://www.britannica.com/EBchecked/topic/410357/protocol.)

[23] The National Aeronautics and Space Administration (NASA) and the U.S. Department of Energy contributed additional backbone facilities in the form of the NSINET and ESNET respectively.

[24] Over 100,000 by 2014. The system of protocols which was developed over the course of this research effort became known as the TCP/IP Protocol Suite, after the two initial protocols developed: Transmission Control Protocol (TCP) and Internet Protocol (IP). An Internet protocol (or communicating systems using formats for exchanging messages) delivers packets of data from the source host to the destination host solely based on the IP addresses contained in the packet headers. Communications protocols have to be agreed upon by the parties involved.

made by industry for customer consumption. Private and public infrastructures were not interconnected: frequently, however, public information services, available to any organization with public members, could not afford to link to each potential customer and had to rely on data communications supplied by private telephone and telegraph monopolies.[25]

The original innovators, scientists, and agencies assembled the various components of the Internet with very public goals in mind: the advancement of science and national security.[26] Early enthusiasts envisioned a virtual frontier, what cyber libertarian John Perry Barlow would describe as a terrain "with no elected government, no greater authority than that with which liberty itself always speaks", and a "global social space…independent of the tyrannies [government seeks] to impose".[27] That idealistic rhetoric has been repeated as recently as 2010 with the description of the Internet as "a centrifugal force, user-driven and open."[28]

For other observers, however, such democratic promise quickly dissipated in the early 1990s when The National Science Foundation was dismantled and the US government "handed over the running of the Internet backbone to commercial Internet service providers,"[29] almost all of which locate their corporate headquarters in the continental US. It was, in the words of venture capitalist John Doerr, "the largest legal creation of wealth in the history of the planet."[30] Also provoking considerable controversy for its American power-hold on the assignment of names and numbers to Internet sites is the Internet Corporation for Assigned Names and Numbers (ICANN) that "coordinates these unique identifiers across the world" in furtherance of a global Internet.[31] Standing at the forefront of the "thought experiment"[32] that is the Internet is

---

[25] Campbell-Kelly & Garcia-Swartz, *supra* fn 20 at 13.
[26] Michael Harris, *Book review: 'The Internet is Not the Answer' by Andrew Keen*, WASH. POST (2 Jan. 2015), http://www.washingtonpost.com/opinions/book-review-the-internet-is-not-the-answer-by-andrew-keen/2015/01/02/8627999a-7973-11e4-9a27-6fdbc612bff8_story.html.
[27] John Perry Barlow, *Declaration of the Independence of Cyberspace,* (8 Feb. 1996) as reproduced by the Electronic Frontier Foundation, https://projects.eff.org/~barlow/Declaration-Final.html.
[28] Ryan, *supra* fn 18 at 8.
[29] Harris, *supra* fn 26.
[30] As related by Bill Davidow, *The Internet Is the Greatest Legal Facilitator of Inequality in Human History,* ATLANTIC (28 Jan. 2014), http://www.theAtlantic.com/business/archive/2014/01/the-internet-is-the-greatest-legal-facilitator-of-inequality-in-human-history/283422/.
[31] ICANN website at https://www.icann.org.
[32] ANDREJ SAVIN, EU INTERNET LAW, x (2013) (Internet).

US industry; most of what other countries do is a response or reaction to that dominance. The EU has responded to most of those challenges in ways that are uniquely harmonized within its borders.[33]

The Internet of the early 1990s has been described as "a gray and dreary place devoid of content – like a TV station without programs".[34] The emergence of the World Wide Web in the mid-1990s, a multimedia interface that allows for the transmission of text, pictures, audio, and video collectively known as web pages, popularized and enlivened the Internet with search functions that could retrieve information on just about any topic imaginable. With the arrival of commercial entities such as Netscape, Microsoft, AOL, and Yahoo! the Web was transformed from "an amateur enterprise to a robust commons".[35] For the individual user, the Internet had expanded its information storage function to unlimited research capabilities and democratized information access.

In terms of its operating systems to serve individual users, the computer evolved from a system of "punching up cards to feed into someone else's mainframe"[36] into a network of PCs available on each worker's desk or in individual homes, with installed software that enabled users to give orders to the computer's hardware. Files could be saved on the PC's desktop, distributed throughout the network, or copied onto an external disc and distributed to others. While some owners showed initiative to program their own computers, most simply bought software programmed by others and downloaded it onto their PCs. Generally the computer was function specific, achieving one task for its duration. It was prone to crash if too many complex commands were inputted at too fast a rate. Jonathan Zittrain coined the descriptor "tethered" to characterize the individual's reliance on the network and pre-programmed software, operations we have come to refer to as the Web 1.0. We can characterize the human component in that era as primarily information gatherers.

---

[33] For example, the EU has directives regulating e-privacy (2002/58/EC), legal protection of databases (96/9/EC), distance selling (97/7/EC), data retention (2006/24/EC), electronic commerce (2000/31/EC), data protection (95/46/ED), access to, and interconnection of, electronic communications networks, domain name regulation (EC/733/2002), and implementation of the European Top Level Domain <.eu> (EC 733/2002).

[34] Campbell-Kelly & Garcia-Swartz, *supra* fn 20 at 4.

[35] *Id.* at 5 (suggesting that the Web won out over several competitors).

[36] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT, 2 (2008) (Future of Internet).

The next stage, what has been coined the age of Web 2.0, is marked by its generativity. All users can assume the role of content publisher. Three interlinked trends have emerged featuring the individual during that second more interactive or generative phase: 1) the evolution of the individual from passive consumer to participatory contributor of content; 2) increasing hazards to one's good name prompted by the regeneration of user information by third party users that is enabled by a relatively open or unregulated Internet; and 3) the resultant tension between the individual's need for privacy and the constitutionally recognized right of others to free expression. Regarding the first, individual access to content moved from mainframes located at public institutions to independent network functioning.[37] PCs defined their individual owners as consumers whose tastes influenced a digital market and gave birth to behavioral advertising, or the tracking of individual online search habits as indicators of consumer preferences. In that way, the individual user became a principal component of the digital economy with every excursion online. While those coordinates were presented in code, they nonetheless provided key personal information to commercial interests and to governments alike who sought to study and profile the interests, buying preferences, and illicit intentions of online participants.

The Internet evolved during the 1990s and early years of the new millennium from a limited operating system to one that encouraged generativity or user interactivity. With the later arrival of social media, individuals became publishers in their own right, often without mediation from traditional editing sources.[38] They comprised the "essential quality animating the trajectory of information technology innovation".[39] PCs were connected to, and users communicated with, any possible network of other PCs over the Internet. That generative quality Harvard University's Jonathan Zittrain defines as "a technology's overall capability to produce unprompted change driven by large, varied, and uncoordinated audiences."[40] When these "highly adaptable machines" are linked to a network with limited centralized control, we get

---

[37] Jonathan Zittrain, *The Generative Internet,* 119 HAR. L. REV. 1 (1974) (Generative).
[38] *See contra,* Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience,* 78 GEO. WASH. L. REV. 697 (2010).
[39] Zittrain, Generative, *supra* fn 37 at 1980. This paragraph follows Zittrain's explanation on the openness of the Internet.
[40] *Id.*

> …a grid that is nearly completely open to the creation and rapid distribution of the innovations of technology-savvy users to a mass audience that can enjoy those innovations without having to know how they work.[41]

That development from information acquisitor to content publisher has involved the innovation of numerous communications platforms (social media such as emails, Facebook, LinkedIn, Twitter and Instagram, as well as blogs and videoblogs such as YouTube and Snapchat) and the use of a variety of individually owned devices for searches and transmission (such as laptops and mobile phones). The openness and trust preferred by users of such devices provides a formidable market force that resists regulatory attempts at Internet control. However, as Zittrain observed as early as 1974, that system is "increasingly at odds with itself".[42]

As individual users become publishers of their own content, much of it autobiographical and revealing, that information is consumed and retransmitted by third parties with little regard for the context in which it was created. The ease with which photographs can be taken on mobile phones, tagged with our names, and transmitted to third parties, many of those recipients unknown to us, creates high risks of reputational harm through embarrassment, shame, or the inability to stop an unfavourable image from viral distribution across cyberspace. On the criminal side, the hacking of websites using malicious code causes wide exposure of personally identifying data by state and 'dark net' actors. As a result, the very users who benefit from the open, generative Internet simultaneously seek stability through a more locked down system. That creates an online environment that is the antithesis of that which fostered our original participation. Rather than functioning on trust and collaboration, then, we as consumers find ourselves losing control and demanding locked down encryption, regulation, and the limiting of innovative participation.[43]

American Internet scholar Lawrence Lessig recognized as early as 2000 that individuals could not have it both ways: untrammelled privacy and unlimited access and innovation. Users would have to decide whether they desired a regulated Internet and, if so, regulated by whom. In his words,

---

[41] *Id.*
[42] *Id.* at 1977.
[43] The Internet governance debate, while critical to state and industry participation, constitutes a very broad literature and, as such, is beyond the scope of this dissertation

> Under the influence of commerce, cyberspace is becoming a highly regulable space, where behavior is much more tightly controlled than in real space. But that's not inevi either. *We can-we must-choose what kind of cyberspace we want and what freedoms we will guarantee.* These choices are all about architecture: about what kind of code will govern cyberspace, and who will control it.[44] [emphasis added]

While Lessig attributes human choice with shaping the Internet in a major way, commerce and institutions still contribute to the mounting tension between personal privacy needs and the growing inventory of platforms available for online expression. That tension encapsulates the third trend affecting the reputation of individual users: the constant need to balance their need for privacy and the constitutionally recognized right of others to speak their minds freely. Increasingly we look to law, rather than computer code, to conduct that function.

The sudden growth of the Internet initially caught the American legal system somewhat unprepared.[45] Prior to 1986, the US Congress had introduced very little legislation on electronic forms of telecommunication.[46] In that year, Congress passed the *Electronic Communications Privacy Act (ECPA)*[47] that made illegal certain types of electronic eavesdropping on private communications, such as unauthorized reading of private emails as they were stored in transit. The ECPA extended to electronic mail most of the protections already granted to conventional mail and encompassed radio and data transmissions. Thus began a legislative practice of appending onto extant legislation Internet and Web uses. Almost a decade later the US Senate, in turn, introduced the *Communications Decency Act* in February of 1995 to target "obscene, lewd, lascivious, filthy, or indecent electronic communications". That aim to protect the individual Internet user from online obscenity was later found unconstitutional by the US Supreme Court; similarly no was the impact of section 230 of the Act that

---

[44] LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.O, 1-8 (2000) (Code).

[45] This paragraph is informed by *The Internet,* Encyclopedia.Com, http://www.encyclopedia.com/topic/the_Internet.aspx.

[46] *See further* Gina Marie Stevens & Charles Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping,* Report of the Congressional Research Service of Congress (3 Dec. 2009), http://www.au.af.mil/au/awc/awcgate/crs/98-326.pdf (detailing US legislative efforts to keep up with electronic communications innovation since the 1928 *Olmstead* wiretapping decision).

[47] *Electronic Communications Privacy Act* 18 U.S.C.A. § 2701ff [1996] (ECPA).

determined operators of Internet services were not to be construed as publishers and hence not legally liable for the words of third parties who use their services. That exemption would eventually transform into the widest possible exemption from liability for Internet Service Providers (ISP)s regarding illegal or socially objectionable material it disseminated over the Internet.[48]

It is important to point out that Internet regulation addresses two components: the content that is transmitted, and the infrastructure *on which* content is transmitted. The above legislation addresses the former and provides the subject of this dissertation while a separate and relatively complex system of telecommunications law addresses the latter and will not be covered herein. As suggested by one scholar of EU Internet law, there is a conceptual difference between the regulatory environment which applies to the wires as opposed to that which applies to the content and, although other media, such as television or radio, share many features with the Internet, they are "non-interactive and distributed from the centre to the periphery and therefore subject to different principles."[49]

Lawmaking within the EU took a more administratively uniform and less derivative route to Internet regulation than that of the US. Rather than applying "inherited concepts to the digital world", EU lawmakers showed recognition of the need for "new rules, a new language and a new social context which do not easily lend themselves to traditional legal classification."[50] The result of those intentions is a rich compendium of directives and national laws that address many aspects of electronic communications. That compendium is nonetheless confusing: "instruments are numerous, policies difficult to distinguish, court decisions conflicting" and official statements contradictory and often incoherent.[51] While the larger political and economic framework is focused on a single market phenomenon, harmonization policies are pursued within the EU not out of fear that disparity in laws between Member States

[48] Section 230, discussed in more detail in Chapter 5 *infra*.
[49] Savin, Internet, *supra* fn 32 at x.
[50] *Id*. at viii.
[51] *Id*. at x.

would slow economic development of the whole union but rather to achieve a coherent vision to steer policy development.[52]

The Internet today is a very different space than that envisioned by its creators and scholars – more regulated, more complex, and more integrated into our daily interactions. In fact, the Internet has become so crucial to our knowledge-based economy that "its preservation and operation is now an issue through which we see our political, social and economic freedoms."[53] Dual expectations of unfiltered content and security are high: as members of western democratic states, we look to our legal systems for unrestricted Internet access and simultaneously for protection of every private detail.

Efforts to produce a single worldwide Internet policy to address those risks have not met with resounding success. Internet policy is comprised of myriad political and economic interests that respond to local, national and international pressures.[54] In the real world, it is highly unlikely that Internet activities can be subjected to a single policy framework across geopolitical boundaries. The EU has played a crucial part in Internet regulation in Member states, however, and maintains a quasi-federal status and so could potentially play a unique role if global regulation becomes the model.

The interests of individual users cannot always compete with those of industry or other sectors. That fact is illustrated in the uneven progress of the US Congress and the Federal Communications Commission (FCC) to enact laws addressing privacy and Do Not Track mechanisms that would unite all states in a uniform, centralized response to threats to individual online privacy.[55] As well, US federal policies do not flow from one source but receive input and pressure, for example, from offline mass media (print

---

[52] Savin points out, nonetheless, that the European Commission often cites Article 114 of the *Treaty on the Functioning of the European Union (TFEU)* as legal basis for regulating the Internet (ix).

[53] Andrej Savin, *How Europe formulates internet policy,* 3 INT. POL. REV. (26 Feb. 2014), http://policyreview.info/articles/analysis/how-europe-formulates-internet-policy.

[54] For an examination of the pitfalls of modern policy making in the UK, *see* Michael Hallsworth *et al., Policy Making In The Real World: Evidence And Analysis,* Report of the Institute For Government (Apr. 2011) (urging the construction of "a *resilient* process that can handle such challenges and pressures. Such a process would be realistic enough to have a chance of being followed in practice. In contrast, the current processes are too brittle – they break rather than bend when put to the test.")

[55] *See further* Ch. 5 *infra.* In general, the FCC oversees Internet infrastructure while the FTC regulates content. There is some confusion of roles when dealing with net neutrality.

or broadcast) as well as utilities (telecoms, radio, cable and satellite). That fact is also in evidence within the EU, where "different policy making efforts have taken place at different directorates" within each member state.[56] While recent harmonization agenda in Europe are prioritizing Internet protections and data privacy, such efforts have historically proceeded with little coordination. For both the US and Member States of the EU, then, while changes to Internet technology and uses are rapid, policy changes require political consensus and hence move at a slower and more cautious pace.

1.3 Law's Purpose in Online Societies

Law in the service of Internet activity currently serves many purposes, from pre-emptive action (perpetuating the status quo, standardizing industrial practices, or protecting cultural norms) to *post facto* objectives (penal sanctions, remediation, or ending high risk practices). The principal new question this dissertation asks is in what way can law assist our reputational integrity *as individuals* regarding online activity. In other words, as we enter an era of human-machine interconnectivity, what can law contribute to our need for reputational privacy? While not all intrusions of privacy will result in harm to our reputations, much of the activities involved in data collection and use have to potential to reveal aspects of our private life that could diminish our future opportunities if they are revealed. Within that frame, I ask two more specific questions: 1) in what ways do current legal systems respond to reputational risks; and 2) how can we best engage the law and extra-legal mechanisms in maintaining our control over our reputational privacy as we enter the era of the Internet of Things? I pursue two lines of inquiry in order to establish where this dissertation might make a meaningful contribution: 1) I review academic literature that builds a conceptual basis for the interlinked notions of reputation, privacy, and memory; and 2) I examine policy statements and memoranda, the text of specific laws, government debates, traditional and new media accounts and analyses, empirical studies commissioned by governments or privately conducted, and case studies (both in law reports and as discussed in new media) that reveal doctrinal and legal reasoning as well as judicial decision-making at the international, regional, and national levels.

[56] *Id.*

The key values that comprise the focus of my investigation – reputation, privacy, memory – are social constructs, like law, and hence mu and in some state of flux. So, too, is the technological infrastructure of new media whose rate of development is frequently described as "exponential". In fact, Internet technology might be outstripping its own rules in terms of the pace of innovation and change.[57] As much as possible, then, I have selected observations and opinions that describe more general trends than particular technological advancements. That treatment of the subject matter results in coverage that is more inclusive than comprehensive. In other words, this research casts its net of inquiry quite wide for contributions and possible influences rather than delving more deeply into a smaller range of technologies or opinions.

1.4 Limits to the Study: Of Apples and Oranges

It is important at this juncture to establish what this inquiry is *not*. Its unit of study is the individual: reputations of corporations, institutions, and state and government entities are not the primary focus. Their activities are included, however, in the context of their impact on an individual's reputation and primarily through their misuse of personally identifiable data. This dissertation also does not deal extensively with state surveillance, but only as those activities constitute a backdrop to institutional incursions on personal reputational privacy. This dissertation does not provide a detailed analysis of the current status of Internet governance, although its infrequent consideration is important to an understanding of the complexity of Internet regulation.

Further, this is not a major comparative study of two legal and political models: one American and the other from the EU. While both models involve liberal democracies with the largest stakes in the digital economy, and hence represent important examples of different cultural approaches to reputation and Internet privacy issues, they are not comparable in terms of political structures, constitutional make-up, or legal systems. The US is a federal democracy, with power divided between a central

[57] The reference is to the observation of Intel Corporation co-founder Gordon E. Moore that, over the course of development of computer hardware, the number of transistors in a dense integrated circuit would double approximately every two years (Moore's Law). That prediction has been interpreted in the non-scientific community as reflecting the general progress in capacity of computer technology. *See further* Gordon E. Moore, *Cramming more components onto integrated circuits*, ELECTRONICS MAGAZINE, 4 (1965).

or national government and 50 States in the Union.[58] It was established in 1789 as a participatory democracy with a common law system and federal constitution. It has a bicameral legislature comprised of the House of Representatives (Congress) and the Senate.[59] A similar system is engaged within each state (Lower House or Chamber and State Senate). Each state has its own legal system, judicial system, and case law as mandated by the US Constitution. Judicial decisions from the highest court level in each state can be appealed to the US Supreme Court; those rulings are binding on lower courts regarding federal laws, such as the US Constitution.[60] Although laws of Congress can be overridden by executive order of the President, they seldom are.[61] Federal laws address trans-state issues within the country such as transportation and communications, but states exercise considerable autonomy to implement their own laws covering the same subject matter. As will be seen, that extra layer of legislative action provides citizens with additional recourse if their first attempt at a federal bill is defeated.[62]

Politically and constitutionally, the EU is more complex. It was created in the aftermath of the Second World War to foster economic cooperation, primarily by pooling coal and steel resources, and to reduce political conflict between nations within Europe. It evolved from the European Economic Community (EEC) of 1958, with six founding member states: Belgium, France, West Germany, Italy Luxembourg, and the Netherlands. Those states were known as the 'inner six' to distinguish them from the 'outer seven' states who formed the European Free Trade Association rather than engage in supranational European integration: Austria, Denmark, Norway, Portugal, Sweden, Switzerland, and the United Kingdom. The EU emerged from that arrangement in 1993 as an organization sharing policy development on a variety of issues from justice to the environment. It is now a political and economic union of 28 countries (excluding Norway and Switzerland) each with its own constitution. It is not a

[58] There are also five territories and one Federal District (Columbia).
[59] *The Legislative Process,* United States House of Representatives, http://www.house.gov/content/learn/legislative_process/.
[60] For greater clarity, US Supreme Court decisions are binding on federal and state courts, only regarding federal laws.
[61] The US President has ten days to sign or veto a bill. See further *The Legislative Process, supra* fn 59.
[62] As will be seen in California's implementation of Kids Do Not Track laws when similar national laws failed to pass in Congress.

federation in the strictest sense, but not just a free-trade association either. The EU has certain attributes of an independent nation: its own flag, currency for most members, and lawmaking structures. It also enjoys diplomatic representation and a common foreign policy when dealing with states external to the EU.[63] The EU operates through a system of supranational institutions and intergovernmental negotiated decisions by the Member States. Within the EU, many policies are formulated as directives that serve as guidelines for national laws. Regulations, such as the proposed European General Data Protection Regulation (EUDR)[64] are mandatory in law and are formally incorporated into national law in each Member State without the need for debate or ratification within those states.

The EU is based on the rule of law and created by statute.[65] It is foremost an economic union (hence the 'euro zone' of 19 EU member states that have adopted the euro (€) as their common currency and sole legal tender). It has created its own Central Bank. It harmonizes national laws in areas of business, free trade, and the security of EU citizens, but has so far been unsuccessful in harmonizing private laws, particularly in the areas of contract, family, and property rights. Although both European and national legislators share the legislative responsibilities, neither of those bodies has final responsibility for the whole. There is no superior political authority which has the final say on who is responsible for what, that is, no overarching authority over the European

---

[63] *The World Factbook: European Union,* Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/geos/ee.html. 'Associated States' lacking full EU membership include: Albania, Bosnia & Herzegovina, Faeroe Islands, Iceland, Israel, Liechtenstein, Montenegro, Norway, Republic of Moldova, Switzerland, the Former Yugoslav Republic of Macedonia, Serbia and Turkey.

[64] J. P. Albrecht, *Report On The Proposal For A Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML+COMPARL+PE-501.927+04+DOC+PDF+V0%2F%2FEN .

[65] The Maastricht Treaty (formally the Treaty on European Union) created the European Union on Feb. 3 1992; an amended version was signed into effect on 1 Nov. 1993 due to the need for a referendum (Denmark) and confidence vote in the UK parliament. The Treaty also created a central banking system for EU members, paved the way for the adoption of the Euro as the common currency strengthened the EU's influence regarding foreign policies of its members. Euro Zone members include: Austria, Belgium, Cyprus, Estonia, Finland, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Slovakia, Slovenia, and Spain. Four countries have formal agreements to use the euro as their official currency: Andorra, Monaco, San Marino, and Vatican City. Kosovo and Montenegro have adopted the euro unilaterally. There is no statutory exit provision.

and national legislators. The European Court of Justice may, however, determine the extent of harmonization when determining cases.[66] The EU passes regulations that substitute European law for some national laws.[67] The legal system might be under common law or civil law system. If the latter, precedent is not binding but case law is taken into account by the courts. The Court of Justice of the European Union (CJEU) is located in Luxembourg and interprets EU treaty law to make sure it is applied in the same way in all EU Member States.[68] It also settles legal disputes between EU governments and EU institutions. Individuals, companies or organizations can bring cases before the Court if they feel their rights have been infringed by a EU institution. The bench is comprised of one Judge per Member State and eight Advocates-General.

Two other courts are located in Europe but are not EU courts. The European Court of Human Rights (ECtHR) located in Strasbourg, France is an international court set up under the Council of Europe that currently has 47 Member States. The Court enforces the European Convention on Human Rights. The International Court of Justice (ICJ), located in The Hague in the Netherlands, was founded in 1945 by United Nations Charter. Its main functions are to settle legal disputes submitted to it by states and to provide advisory opinions on legal questions submitted to it by authorized international branches, agencies, and the UN General Assembly. Its jurisdiction includes questions relating to the UN Charter, the interpretation of international treaties, questions of international law, and the nature and extent of compensation in the event of a violation of an obligation under international law. Only states can be parties in cases before the Court. The US withdrew from compulsory jurisdiction of the court in 1986 after the court ruled its covert war against Nicaragua violated international law. The US now accepts the court's jurisdiction only on a case-by-case basis. The ICJ is not a supreme court for appellate decisions from national courts; it does not act as a court of last resort for individuals. Nor is it an appeal court for any international tribunal. The court has no true compulsory jurisdiction, a matter that is

---

[66] *See further* Martijn Hesselink, *The Ideal of Codification and the Dynamics of Europeanisation: The Dutch Experience,* in STEFAN VOGENAUER AND STEPHEN WEATHERILL (eds), THE HARMONIZATION OF EUROPEAN CONTRACT LAW: IMPLICATIONS FOR EUROPEAN PRIVATE LAWS, BUSINESS AND LEGAL PRACTICE (2006).

[67] *The legal system of the European Union,* Europedia, http://www.europedia.moussis.eu/books/Book_2/2/3/3/index.tkl .

[68] Its court of first instance is the General Court of the European Union.

often challenged by respondents. Enforcement is by the UN Security Council but weak in that its five members can veto enforcement.

There are four institutional components to the EU. The Council of the European Union (the Council) is called the Council of Ministers and is the central legislative and decision-making body in the EU (comprised of one representative at ministerial level from each Member State with the authority to commit their government, a composition that varies depending on the subject on the agenda). In contrast, the European Council consists of the Heads of State or Government of the Member States, its President, the President of the Commission, and the High Representative of the Union for Foreign Affairs and Security Policy. It has no law-making powers but sets the EU's broad priorities through national and EU-level leaders. The European Parliament represents all European citizens through elected members. The European Commission addresses the interests of the EU as a whole through members appointed by national governments.[69] Any regulation, such as the EUDR, must have the approval of the European Parliament, the European Commission, and the Council in order to become law. In principle, the Commission proposes new laws, and the Parliament and Council decide on their adoption. The Commission and the member countries then implement them, and the Commission ensures that the laws are properly applied and implemented.

1.5 Methodology

Through a review of international and domestic[70] legislation, jurisprudence, and policy initiatives, as well as news accounts, studies, and current legal practices, this dissertation explores the extent of control held by the individual over her reputational privacy. This is an exploratory study in that it involves a search of an array of sources dealing with reputation and Internet activities. It examines two emerging regulatory models, the EUDR, and American Do Not Track (DNT) policies to assess the improvements and challenges they pose over current legal responses. In order to stay current with the pressing issues regarding individual reputation affected by new media, I examine unmediated sources such as blogs, videoblogs, and other online peer

[69] *EU Institutions and Other Bodies,* Europa.eu, http://europa.eu/about-eu/institutions-bodies/index_en.htm.

[70] 'Domestic law' is used herein to indicate the laws of a country or member state of the EU or, in the US context, federal laws in contrast to state laws.

contributions by a range of contributors from Internet scholars to professional journalists to law firms to private citizens. Secondary sources include books and journal articles, case commentary and book reviews, as well as online sources of traditional news reportage and opinion, and online dictionaries and encyclopedia. To support particular points I employ government, non-governmental (NGO), institutional and commercial empirical study results, often in chart and graphic form as primarily contained in the Appendices.

Since case law analysis forms an essential component of this inquiry, I will use defamation and privacy cases decided by courts of all levels in EU Member States and the US (both state and federal levels). Given the impossibility of covering all cases that address harms to reputational privacy within the US and in Member States of the EU, I will select where available decisions of the US Supreme Court and the CJEU, the highest appellate court for EU member countries.[71] I will make my case selection based on two methods: an online law report search of cases featuring "defamation", "reputation", and the "Internet", followed by a review of high profile cases suggested by traditional press and new media. Those cases will, in turn, refer me back to an online law report search. That broad base of research method will produce a wider range of cases that fit within the research agenda. In analyzing the cases, I will test those selected for what they tell us about jurisprudential principles in the digital environment, keeping in mind the balance judges must seek between legal tradition that affirms law's legitimacy and the "incrementalism" with which they approach new legal concepts.[72] My analysis will lead to an exploration of emergent legal proposals, such as the EUDR and DNT models I choose to analyze with closer scrutiny in Ch 4.[73]

I hope to discover information on how Internet companies make decisions on takedown requests of subscribers in relation to the guidelines suggested by such

[71] *See further* Ch. 5 herein and *Court of Justice of the European Union,* Europa.Ca, http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm.

[72] "Incrementalism" is used here to indicate the gradual expansion of legal principles from one case to the next. It does not suggest the taking of each case solely on its own merits without consideration for similar cases that have preceded it. *See further* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law,* University of San Diego School of Law, Public Law and Legal Theory Research Paper 55, 34 (June 2003).

[73] Proposal For A Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation) 2012/0011 (COD) (1 Jan. 2013) (EUDR).

decisions as the CJEU's influential *Google Spain* ruling. I also anticipate, from current news accounts of European reaction to behavioral advertising and online harassment and luring of underage Internet users, a cross-cultural and transnational receptivity to the DNT legislative prototype that is attracting considerable institutional attention within the EU. Finally, I consider extralegal solutions to reputational privacy issues and evaluate whether those remedies can assist us in handling the reputational privacy paradox as we enter the Web 3.0 era of interconnectivity.

1.6 Scope and Outline

The subject scope of this dissertation with respect to technology and to legal principles and practices is what is extant midway through the second decade of the 21st century. The unit of study is the individual;[74] the "society" I study can be our real time community or our online collection of peers, anyone who has significant influence over the esteem in which we are held regarding our future opportunities. Similarly, I leave open the possibility that we might have many reputations, one for each society within which we function. I remain mindful, as privacy scholar Julie Cohen has noted, of the socially constructed self "who is the real subject of privacy law- and policy-making…emerging gradually from a preexisting cultural and relational substrate".[75] My principal interest is in how our social presentation of self, as negotiated through language, dress, and other cultural symbols within our personal control, becomes vulnerable to the plasticity and tentative nature of online society.[76] I am therefore focusing on the individual who is tasked with balancing the new demands of an age of technological interoperability with the need for personal control over the delicate balance of self-imaging. My inquiry considers to what extent that control is forfeited to a global, faceless, unknowable public whose impersonal curiosity and collective judgment define our social significance. That question is later reframed within the emerging world of "the Internet of Things", man-machine collaborations where integrated form and function complicates presentation of self as never before. When

[74] For a broadly based introduction to the reputation of nations within international law commitments, *see* George W. Downs & Michael A. Jones, *Reputation, Compliance, and International Law,* 32 J. L. STUDIES, S95 (2002), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=302031

[75] Julie Cohen, *What Privacy is For,* 126 HARV. L. REV. 2 (2013).

[76] *See further* Ch 2, 2.1.

that codependency goes awry, and exposes our more private self to public scrutiny, I question whether law can play a useful role in its reordering. I consider that occurrence, to some extent, in legal systems in Asia, South America, and Canada but primarily focus on the United States and select state members of the European Union.

This dissertation proceeds in six parts: Chapter 1 provides background on the evolution of the computer from a compendium of readable electronic documents (Web 1.0) to an interactive space of peer-generated contributions (Web 2.0) to a network of human-machine interoperable systems (Web 3.0); Chapter 2 reviews the interdisciplinary literature that conceptualizes reputation, privacy, and memory, calling on contributions from disciplines as diverse as anthropology, urban geography, legal informatics, legal theory, computer science, information systems, behavioral psychology, and cultural studies; Chapter 3 provides an inventory of technical methods and extreme online behavior by which our reputations can be harmed on the Internet and the personal and professional cost of such invasive actions. I analyze two cases, the Mosley case in Europe and the Martin case within the US, to personalize the ways that legal systems respond to disclosures and exposure of personal information. I aim to discover any differences in principles and practice shown in the different jurisdictions. I also examine procedural considerations in choosing jurisdiction and law systems for such cases. Chapter 4 provides a more in-depth and methodical examination of legal responses at the international and national level, utilizing private and public law. It considers less universally accepted responses, such as criminal defamation and insult laws employed in non-democratic regimes, and employs a variety of cases to animate particular legal principles or practices and their effect on individual suffering. In that chapter I introduce the possibility of a discrete law of digital speech and non-legal responses. In Chapter 5 the US Do Not Track model and the European Union Data Protection model are analyzed more thoroughly for what they convey about preferred policies and cultural-legal norms, focusing on unique mechanisms such as rights of erasure and notice-and-choice self regulation. I consider what a new digital law would look like in theory and practice, and pose new non-legal responses that are already in use in some jurisdictions. In Chapter 6, I consider the emerging era of man-machine inter-operability, as currently observable in technologies that are wearable and that enhance human biophysical, sensory, and cognitive functioning. I suggest future

research that examines computer enhancement as it relates to the societal presentation of the individual. I conclude by considering whether the tyranny of the reputational paradox needs to continue into a future of digital communications where public and private are embedded, inter-operative, and collaborative.

1.7 Importance of the Study

This study is important for the individual because reputation is the grease in the wheels of social acceptance and professional opportunity. We also accept its measure as our self worth. It is important for our society of peers because, when it is gone, they suffer the loss of trust they have invested in us. While reputation engages considerable study within the corporate and international relations fields, individual reputation as it relates to law receives less attention from academic thinkers, and individual reputation in the digital world even less so. Its study is pursued somewhat obliquely within the context of law and technology, defamation law, communications, computer design, and privacy. This is not to say there is not a burgeoning academic literature on a wealth of imaginable aspects of the digital environment and new technologies, whose contributions are most no in their inter-disciplinarity.

This work differs from preceding academic literature in its *combination* of topics around individual reputation and the Internet. Those topics include: a conceptual study of reputation as it relates to memory and privacy; a consideration of new and extra-legal mechanisms to address novel forms of speech existing in social media spaces; and the contextualization of reputational privacy within the man-machine interconnectivity emerging as the Internet of Things.

CHAPTER 2 LITERATURE REVIEW

2.0 Introduction

In this chapter I review the literature on the conceptualization of three interlinked entities: reputation, memory, and privacy. I will integrate into this review a brief historical account of the societal values upon which reputation used to be measured, first against the overreaching curiosity of one's community members and secondly regarding the non-consensual probing of the state into private affairs in the name of security and sovereignty. My review of literature indicates that, while America was familiar with the idea from France and Germany that a person had a right of personality that the law could legitimate, Americans generally took a more proprietary view of one's name as an intangible but marketable commodity. As a result, the legal systems in European states and in America to enable that process were quite different, as was the jurisprudence that emerged. As well, the role of the state in recognizing such rights was disparate from one side of the Atlantic to the other.

2.1 Theorizing Reputation

> Character is much easier kept than recovered.[77]
>
> ***
>
> O, I have lost my reputation! I have lost the immortal part of myself and what remains is bestial.[78]
>
> ***
>
> You are what Google says you are.[79]

Those who deliberate on the nature of reputation often comment on its contingent quality. For Shakespeare's Othello, for example, a good name was all that stood between our human endeavours and the soulless morass of our baser natures. For contemporary author Michael Iapoce, reputation is "character minus what you've been caught doing," – or what is left of your good name after society has caught you in all

---

[77] THOMAS PAINE, THE POLITICAL WRITINGS OF THOMAS PAINE, vol. 1 (available online from General Books LLC, 1870).
[78] OTHELLO, *supra* fn 1 at Act II, Scene III, ll 265-7.
[79] Megan Angelo, *You Are What Google Says You Are,* WIRED (2 Nov. 2009). http://www.wired.com/business/2009/02/you-are-what-go/.

your indiscretions.[80] Recognition of reputation as a social construct dates back at least to the early Greek philosopher Socrates who is reputed to have advised, "The way to a good reputation is to endeavor to be what you desire to appear."[81] In a similar vein, George Washington has been attributed with the advice that it is better to be alone than found in bad company. A good reputation, then, can turn bad if secrets of our baser natures emerge, our usual discretion fails, our public mask slips, or our companions prove unsavory to public opinion.

Most factors that shape reputations are external to the individual: societal perceptions, moral judgments of our peers, and public challenges to our honour and dignity. The paradox or "mysterious thing"[82] about reputation is that, as a social entity, its worth to the holder resides in the estimation of others. It is that external element of control that argues against treating reputation as personal property. We possess it, and are ultimately responsible for its nature, but its creation and destruction can be instigated without our consent or even knowledge. We might spend a lifetime, therefore, striving to structure our behaviors according to certain externally determined standards, only to have its ultimate shaping change course in an instant, leaving us defenceless. Reputation can be a social good in that we emulate those noble attributes assigned to us by others; it can also be subject to vicious and annihilating commentary that, if untrue, moves us to legal action and other vindications.[83] Additionally, the sting we suffer is not only a sense of injustice and privacy deprivation but also our painful *awareness* of all we have lost in social or moral status.[84] To witness the diminution of our

---

[80] MICHAEL IAPOCE, A FUNNY THING HAPPENED ON THE WAY TO THE BOARDROOM: USING HUMOR IN BUSINESS SPEAKING, 129 (1988).

[81] EDWARD PARSONS DAY, DAY'S COLLACON: AN ENCYCLOPEDIA OF PROSE QUOTATIONS, (1884) as reproduced by Digital Commons, http://digitalcommons.butler.edu/cgi/viewcontent.cgi?article=2009&context=wordways.

[82] Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution, 74* CAL. L. REV. 691, 692 (1986).

[83] The preferred legal recourse is an action in defamation, defined by Black's Law Dictionary as "The taking from one's reputation; the offense of injuring a person's character, fame, or reputation by false and malicious statements." Criminal libel does not recognize a defence of truth and comprises a controversial area of law in various jurisdictions. *See infra* CH IV sections 4.2 and 4.3.

[84] Julian Sanchez, *Book Review*: *The Future of Reputation: Gossip, Rumor, and Privacy Online by D. Solove*, ARS TECHNICA (6 Oct. 2008), http://arstechnica.com/tech-policy/2008/10/future-of-reputation/.

own esteem in the eyes of our significant peers can provoke the ultimate social isolation.[85]

Our awareness of our need for a good reputation shapes our presentation of self within that society. American social theorists George Herbert Mead and Erving Goffman contribute to our understanding of the sociological underpinnings of reputation. For Mead, the mind and self emerges out of the social process of significant communication.[86] A man's society exists *a priori:* the man emerges from that society, not the other way round. "In that way, the development of the individual's self, and of his self-consciousness within the field of his experience" is preeminently social and cannot be understood outside of that social context.[87] According to Mead, our significant communication is achieved through gestures (unconscious communications) and language (conscious) wherein we can change the attitudes and positions of another. Our role is not passive: we play the game *in light of* the attitudes of others.[88] We maintain control to the extent that the indeterminacy of others' responses "gives the sense of freedom, of initiative."[89]

To Goffman, our face-to-face interactions are theatrical performances wherein we negotiate our control over the impressions others have of us. We accomplish this through our choice of setting, appearance, and manners.[90] We live out our more personal, idiosyncratic tendencies backstage. On stage, we keep "face", that is, the positive social value we claim for ourselves that shapes our roles during a particular

---

[85] As expressed by the wife of disgraced NFL football star Ray Rice upon the release of a video revealing he knocked her unconscious: "If your intentions were to hurt us, embarrass us, make us feel alone, take all happiness away, you've succeeded on so many levels." *See Wife defends disgraced NFL star Rice after brutal video,* Yahoo! Sports (9 Sept 2014), http://sports.yahoo.com/news/knockout-victim-wife-defends-rice-firing-214526513--nfl.html

[86] Defined by Mead as the comprehension by the individual of the *meaning* of her gestures and her ability to evoke an appreciation of that meaning in those to whom she speaks. *See further, George Herbert Mead (1863-1931)* Internet Encyclopedia Of Philosophy, http://www.iep.utm.edu/mead/ - 5h3a.

[87] GEORGE HERBERT MEAD, MIND, SELF AND SOCIETY, 42, 43 (1934), comprised of students' transcriptions of Mead's lectures at the University of Chicago).

[88] *Id.* at 160. Mead identifies our society as comprised of the 'generalized other' who assist in our self realization by observing our role-playing. They use social control to bring our acts into alignment with their societal objectives.

[89] *Id.* at 177.

[90] Goffman, Presentation, *supra* fn 8.

contact.[91] Our dramaturgical decisions comprise our performance that others see, just as similar choices by others form *their* front stage presentation of self. Together, we agree on the social limits of our performances and agency, and do our best to avoid embarrassment. Goffman's stigma arises from our inability to meet social standards, something outside of each of us. We could say that Mead and Goffman believe we are who we think other people think we are.

As we migrate online, elements from our backstage move to front stage, blurring the limits of our public/private selves. In the absence of face-to-face communications and immediacy of responses, our sense of social interaction is dulled. For example, in the real world a social visit might include the sharing of conversation and a cup of coffee simultaneously. It is generally clear that "the 'point' of the interaction is the discussion, not the coffee making."[92] Online exchanges lose that element of richness and caring that the mundane task of coffee making provides. We need to find other cues or gestures (Mead) whereby we give off an impression (Goffman) of our sociality while online.

Psychology professor Hugh Miller of Nottingham Trent University suggested as early as 1995 that there is liberation that comes with online communications, a crossing of status lines allowing entry to "power bases" that might not be available to us offline.[93] Writing in an era that predated social media, he noted that access comes with email and the creation of our own web pages, the latter being open for anyone's browsing. Our online interactions, however, might involve more circumspect 'backstage' preparations for self-presentation through our increased access to information on our contact person's institution, department, special knowledge, or hobby interests.[94] We are also less aware of any rebuffs to our invitations to interact; we are also less likely to have anyone correct the gaffes we make in our online communications. In that way, Miller notes, "It is easy to make a fool of yourself on the Web" but "doing it will cause you little pain" because you are not routinely aware of who is accessing your webpage.[95]

---

[91] ERVING GOFFMAN, INTERACTION RITUAL: ESSAYS ON FACE-TO-FACE BEHAVIOR, 5 (1982).
[92] Hugh Miller, *The Presentation of Self in Electronic Life: Goffman on the Internet,* Paper for Embodied Knowledge And Virtual Space Conference, University of London (June 1995).
[93] *Id.* Ethan Zuckerman, the creator of Facebook, makes a similar claim. *See infra* fn 440.
[94] *Id.* at 1.
[95] *Id.* at 3.

Reputation – good reputation – depends on our compliance with social or moral norms that are never static in any complex society. So while legal, religious or social institutions are instruments to protect the status quo, the existing order works best for the wealthy, Miller's "power base", whose values are perpetuated through those institutions. As Lawrence Friedman summarizes, "The status quo freezes a certain distribution of wealth and influence, of standing, reputation, and social capital."[96] Digital communications are liberating us, through the particularities of their architecture, from some of those social constraints.

Daniel Solove of George Washington University Law School has written widely on reputation within the legal context. He offers the oft-quoted distinction, "a man's *character* is what he is, while a man's *reputation* is what other people may imagine him to be."[97] That assessment has also been attributed to Lord Denning of England's Court of Appeal. It is telling of the present day confusion over what constitutes reputation that, in his 2007 text *The Future of Reputation*, Solove does not offer his own definition.[98] The author emphasizes that much rests on a good name: one false rumour can prove deadly, as seen in the European witch hunts between the 14th and 17th centuries where over 500,000 people, mostly women, were burned at the stake on the hearsay of their neighbours. Our efforts at reputational control are limited, argues Solove, as we are jousting with innuendo, "a bundle of half-truths and incomplete tales."[99]

Solove has observed the permanence of access that the Internet lends to personal information, transforming it from something "forget and localized within small local groups" into details of our private lives that are "becoming widespread, permanent and searchable."[100] Historically reputation has been assailable in three principal ways: through our own actions or revelations, by surveillance, and by third party disclosure of concealed information. Those behaviors persist into the Web environment. In the end,

---

[96] LAWRENCE FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY, 15 (2007).

[97] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR AND PRIVACY ON THE INTERNET, (2007) (FUTURE). The author, in turn, attributes the quotation to Theodore Tilton whose wife, Elizabeth Tilton, had a scandalous extramarital affair with the preacher Henry Ward Beecher in the 19th century as contained in Richard Wightman Fox, Trials Of Intimacy: Love And Loss In The Beecher-Tilton Scandal, 33 (1999).

[98] Solove, *id.* at 4, 11.

[99] *Id.* at 189.

[100] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, 8 (2004).

the personal damage is the same: inhibition, further self-censorship, embarrassment, and a profound sense of lost self worth.

In theorizing reputation with a legal lens, we need to consider the nature of the interest that we ask the law to protect.[101] The European law on the rights of personality provides a conceptual starting point for how the law has dealt with the increasing societal pressures to protect one's good name. Concepts suggested by the terms 'inviolate personality', the 'rights of reputation' and 'rights to privacy' all capture the idea of individual and societal pressures on the law to recognize such interests as of right. In this section Roscoe Pound and Robert Post provide much of the groundwork on reputational theory as it began in Europe and influenced privacy law in America. In this section, the contributions of Lawrence McNamara and Giovanni Sartor bring a historical perspective to how reputation has been treated by law in European nations, and Internet scholars Viktor Mayer-Schoenberg and dana boyd analyze how those ideas have transformed with the migration online of many social communications. Those authors represent an emergent literature on the interconnectedness of Internet reputations and changing perceptions of the public/private divide. The ideas of Stijn Smet and Laura E. Heymann are introduced for their questioning of that link between reputation and privacy, a relationship that the Internet has recalibrated in light of the widely expanded online audience to our communications.

Former Harvard Law Dean Roscoe Pound's 1915 article *Interests of Personality* can be considered one of the earliest serious investigations of reputation in the American legal tradition.[102] It examines not the law itself, but the interests around reputation that the law seeks to protect. Pound, like his Harvard contemporaries Louis Brandeis and Samuel Warren, looks for inspiration to the principles of law on reputation and privacy long developed within the European tradition. He concludes, however, that each society translates into law very different interests it considers most worthy of protection.

---

[101] Black's Law Dictionary Online (2nd) (defining reputation of a person as "the estimate in which he is held by the public in the place in which he is known" as first pronounced in *Cooper v. Greeley,* 1 Denio 347, 358 (N.Y.Sup.Ct.1845) or as a "person's credit, honor, character, good name." Reputation is identified as a personal right that can be injured through defamatory and malicious words, libels, and malicious indictments or prosecutions.)

[102] Roscoe Pound, *Interests Of Personality*, (parts 1, 2) 28 HARV. L. REV. 343 (1915).

The safeguarding of man from direct or indirect physical injury has historically been one of law's primary interests. In those situations, law is designed to ward off harm and to maintain social order.[103] Where individual, rather than societal, interest is involved, Pound notes that the intangible quality of honour is the primary interest of man: the "standing among brave men regardful of their honor" is an interest for law that supersedes mere physical integrity.[104] Pound suggests individual rights of privacy were the first in western history to be recognized by law, primarily through the personal interests of the sovereign.[105] That concept became somewhat muddled in European countries, Pound notes, when the sovereign simultaneously juggled individual interests and societal interests as a regime head. Pound reminds us that recognition of individual rights, which originated in *ius natural* or the natural law of classical Rome, formed only the first step in protecting a societal interest in security of the person. Up to the end of the eighteenth century, the whole course of the law had been to disentangle individual interests from group or societal interests and to use the law to secure those rights. Pound stresses that a bill of rights formalizes the assertion of individual rights against those of the state and defines societal rights. [106]

Natural rights are interests Pound feels the law should protect. But how, he asks, do we construct a law that will protect the natural rights of honour or personality? Here Pound calls on the German law's concept of *persönlichkeitsrechten* that can be translated variously as individual rights, rights of personhood, personal freedom, right to personal privacy, or personality rights.[107] The judiciary in Germany has played a prominent or active role in the development of the law of personality. That development has been the envy of, and inspiration for, some America legal thinkers.[108] An examination of decisions of the Federal Supreme Court and the Federal Constitutional Court, both of Germany, shows a most critical role in the development of a right of

[103] *Id.* at 356.
[104] *Id.* at 357.
[105] Harvard Law Dean Prosser would later distinguish social interests, public interests and individual interests as rights to personality that the law addresses.
[106] Pound, *supra* fn 102 at 349.
[107] Harry D. Krause, *The Right to Privacy in Germany – Pointers for American Legislation?* DUKE L. J., 481 (1965).
[108] Paul M. Schwartz and Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?* 98 CAL. L. REV. 1925, 1947 (2010).

personality through their interpretations of the Basic Law[109] and the Civil Code. We will develop that comparison more fully in Chapter 4 *infra*.

The thoughts on personhood and personal dignity as presented by Immanuel Kant (1724-1804) have had a key influence on the German, and wider European, concept of *persönlichkeitsrechten*. Briefly, as a disciple of humanism, Kant believed that every rational creature exists as a goal onto himself, not as a "means for optional use by this or that volition."[110] Kant conceived of what he called a Kingdom of Ends where all inhabitants are treated as their own end, rather than as at the whim of other people's expectations or desires. That process is a rational one. Within the Kingdom of Ends, Kant suggested, people could be treated with respect regarding their personhood and dignity, and always as an end in themselves.[111]

Kant's conceptualization of personhood or *persönlichkeitsrechten* found favour with Brandeis and Warren in late 19th century America.[112] In attempting to find a right, beyond a proprietary one, that would forestall publication of personal secrets, the authors promoted the principle of an inviolate personality.[113] They argued such a right already existed in the common law as a right of privacy, "as a part of the more general right of immunity of the person – the right to one's personality."[114] Those ideas found renewed favour with legal thinkers in the aftermath of the Second World War in the context of the horrors to human dignity perpetrated by Hitler's regime and the holocaust. As stated by German's Federal Constitutional Court, citizens cannot be made the mere object of the state, for "the intrinsic dignity of the person consists in recognition of him as an independent personality".[115]

---

[109] *Burgerliches Gesetzbuch* (BGB).

[110] IMMANUEL KANT, THE GROUNDWORK OF THE METAPHYSIC OF MORALS, (Grundlegung Zur Metaphysik Der Sitten,) (1785) as reproduced and edited by Thomas E. Hill, *et al.* and translated by Arnulf Sweig (2002).

[111] *Id.* This paragraph is informed by the Kant text.

[112] Louis Brandeis and Samuel Warren, *The Right to Private Property*, 4 HARV. L. REV. 193.

[113] *Id.* at 205. "The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality."

[114] *Id.* at 207.

[115] Federal Constitutional Court BVerfGE 45, 187, 228, finding unconstitutional a life sentence without any chance for parole. *See further* Schwartz and Peifer, *supra* fn 108 at 1948-1950 (proposing that such a concept is more egalitarian than the racially based right of personality of the German people or V*olk* as promoted by the National Socialist Party during the Third Reich.)

Pound's *Interests of Personality* was published during the first World War, however, and a right of privacy was not codified in America until 1974. Pound found ways to subsume privacy rights in other causes of action. He separated interests in honour or personality from what he called interests in substance or property. For example, if an author uses real names and actual details about a third person in his work of fiction, that third person has two interests: the personality interest in not having his intimate life detailed in a work of fiction (related to honour or personality) and the proprietary interest in the use of his name (substance or reputation).[116] Pound recommended the first set of rights be asserted through the emerging law of torts, following the recommendation of Warren and Brandeis, in order to protect the privacy of man's inviolate personality, and the latter rights through laws of property.[117]

Pound reminds us that American law, unlike European legal tradition, was slow to recognize wrongs against one's sensibilities, what in Roman law was termed *contumelia* or injury to honour through insult. In the very early European tradition,

> …the beginnings of [defamation] law measured composition not by the extent of injury to the body, but the extent of injury to honor and the extent of desire for vengeance thus aroused, since the interest secured is really the social interest in preserving the peace. [118]

Thus were linked the individual and societal interests in reputation. The law was also protective of individuals suffering coercive actions that forced their will. One could be coerced, for example, by having his honour tested, in which case he would be forced to act out of revenge to recover that honour. The law of equity arose to deal with what the Romans called *metus* or duress on the human will imposed by such coercive action.

As early as 1826 in England, lawyer and jurist Thomas Starkie challenged the idea that law should confine itself to tangible property. He argued that reputation, as an object of injury, owes its existence and importance to the various "artificial relationships" that are created as society evolves.[119] Attacks on reputation could thereby create causes of action for injury within the professional sense, what Post identified as any endeavor involving talent or industrious will. That theme was repeated in America

[116] Pound, *supra* fn 102 at 358.
[117] *Id at* 344.
[118] *Id* at 357.
[119] As discussed in Post *supra* fn 82 at 693.

by pastor Joel Hawes in his 1828 address to the young men of Hartford and New Haven. He proposed that character is not inherited from parents nor is it a "necessary appendage of birth, or wealth, or talents, or station; but the results of one's own endeavors." [120] Armed with "good principles" as revealed through virtuous and honourable action, men's character can be viewed as a form of capital that builds societal worth for garnering "patronage and support".[121]

By Pound's time in America, the early 20th century, legal recognition of intangible harm was not formalized. In order to be recognized in law, such harm had to be appended to actions for physical injury. Pound continued to promote reputational rights when he spoke of having an interest in preventing "private personal affairs…laid bare to the world".[122] For Pound, "a man's feelings are as much a part of his personality as his limbs" [123] and equity law should step in to safeguard feelings, primarily through the granting of injunctions.

Throughout the 20th century, European efforts to protect reputation produced a more uniform body of law than in America.[124] The persistent influence over the ages of the Roman principle of *ius natural* (natural justice) and laws on (insult) can be seen as an enduring theme in the harmonization of laws requisite for the formation of the European Union. Today, Europeans continue to look to statute law to protect their fundamental privacy interests.[125]

In America, by contrast, the US Constitution does not directly address either rights to privacy or reputation, although some state constitutions do. Reputational privacy is dealt with through a more sector-by-sector and industry-specific body of consumer laws, what co-authors Meg Ambrose and Jef Ausloos have called "situational regulations".[126] As a result, reputational privacy is addressed through the tort of defamation that deals with untrue statements and the later emerging privacy torts of

---

[120] JOEL HAWES, ADDRESS TO THE YOUNG MEN OF HARTFORD AND NEW HAVEN, Lecture 4, *Formation And Importance Of Character* 91 as reproduced by Princeton University Library (1828).
[121] *Id.*
[122] *Id* at 362.
[123] *Id* at 364.
[124] Schwartz & Peifer, *supra* fn 108 at 2010.
[125] We will examine those instruments in detail in Ch. 4 *infra.*
[126] Meg Leta Ambrose and Jef Ausloos, *The Right to be Forgotten Across the Pond,* 3 J. INF. POL. 1, 8 (2013).

false light, public disclosure of private facts, intrusion upon seclusion and misappropriation.[127]

Yale Law Dean Robert C. Post recognizes the proprietary aspect of reputation as one of three categories addressed by the law of defamation. The other two are reputation as honour and as dignity.[128] Reputation has rarely been defined at common law and Robert Post suggests it resides in the "social apprehension we have of each other."[129] Post advises that we can come closer to a definition by examining the nature of the injuries that defamation law is meant to redress as well as the nature of the social relationship that reputation is meant to uphold.

Reputation as *property* encompasses the notion of one's name as a marketable commodity, what Post defines as "intangible property akin to goodwill".[130] Such favourable reputation is usually gained through manifestation of particular skills or abilities and is developed through one's efforts and labours.[131] The conceptualization of reputation as property was first explored at English common law in *Gee v. Pritchard*, a case involving a threat of exposure by a son of his mother's private letters.[132] The case stood for the proposition that there was relief in property, but not in equity, for injury to personality. The court of Chancery granted the mother an injunction against their publication.

Today, according to Post, reputation as property is based on the belief that community members are linked to each other through the workings of the market. The market determines the value of each person's talents or labours. To untruthfully attack another's reputation within that context is to unjustly destroy the marketable worth of one's labour.[133] Within that economic construct, Post points out that one can always create a new reputation, given that our good name is our own creation in the first place.

---

[127] As discussed further in Ch. 4.
[128] Post, *supra* fn 82 at 691.
[129] *Id.* at 692.
[130] *Id.* at 693.
[131] *Id. at* 693-4.
[132] *Gee v. Pritchard* (1818) 36 ER 670 (Chancery Ct). An injunction was sought by the plaintiff against her illegitimate son who was angered at being left out of the will of his adoptive father, Lord Gee. The son had threatened to expose to public view letters sent to him by his mother, the plaintiff, allegedly describing the far from idyllic condition of her marriage to Lord Gee. The decision was that the action must be based in property, not on wounded feelings or a violation of trust.
[133] Post, *supra* fn 82 at 694.

The making of reputation via the market is open to all; the evaluation of one's reputation on the market determines who shines, whose worth is more or less, and whose name is devalued. Compensation is due directly to the person offended, but only to the extent that the injury to reputation can be measured by market standards.

By contrast, reputation as *honour* captures the idea that our value is determined by our personal identification with the normative characteristics of a particular societal role. In return, we personally receive from others the regard, status, and estimation that society accords to that role.[134] We are not all equal under this scheme, unlike in the reputation-as-property construct. Our reputation becomes tied to institutional roles society assigns to us and is, therefore, not capable of change at our own hands. Our value cannot be converted into a medium of exchange. Further, injury to one's honour creates injury to our societal status and thus to our entire social system.[135] Post analogizes that to challenge one's honour through accusations is akin to defaming the honour of the King that, at early common law, would have been viewed as an attack on the entire government and on the relationship the monarch held with his subjects.[136] Just as we cannot create our own societal worth, it is not in our hands to alter it singlehandedly. Society has just as significant a stake in keeping our reputation unsullied as we do as individuals.[137] Post criticizes the judiciary for focusing, not on pecuniary compensation, but on restoring our honour through apologies, retractions and the publicity generated by the court decisions themselves. Most such activities have been redressed in criminal courts "where the truth of the statement is immaterial and the plaintiff's redress is vindication" imposed through incarceration or hefty fines.[138]

Reputation as *dignity* focuses on the relationship between our public and private selves, in Post's view.[139] As we connect socially to our communities, we internalize those relationships to build our private selves. Public and private dignities are thereby intertwined. Under the reputation-as-dignity construct, defamation law is the right tool to address reputational damage, unlike in the honour scenarios. In the face of attacks on our dignity, the law of defamation aims to (1) keep our dignity intact to maintain a

---

[134] *Id* at 700.
[135] *Id.* at 701.
[136] *Id.* at 702.
[137] *Id.* at 820.
[138] *Id.*
[139] *Id.* at 703.

positive personal identity while (2) protecting society's communal identity.[140] In that respect, reputation as honour and reputation as dignity are similar, although the former is framed as a social good and focuses on the individual's contributing role to his society while reputation-as-dignity is all about the individual's inherent membership in the community. Dignity in Post's lexicon is not viewed as an acquisitive concept but inherent or 'intrinsic in every human being'.[141] Compensation for defaming our dignity must be of the rehabilitative kind, therefore, of giving back what we have always had. That can be achieved legally through a declaratory judgment, to confirm our membership within our community.[142]

Post also reminds us of the crucial role played by the 1964 US Supreme Court judgment in *New York Times Co. v. Sullivan* as the first to bring defamation within the wider framework of the First Amendment right of free speech.[143] Defamation litigation has been dominated by considerations of basic expressive freedoms ever since.[144] *Sullivan* had the potential to change the course of defamation law because the trial judge instructed the jury that such statements were "libelous *per se*", that legal injury could be implied without proof of actual damages, and that compensatory damages could be awarded because malice was presumed if unsavory statements were found to have been published by the defendant relating to a public figure. The US Supreme Court disagreed, however, holding that actual malice or knowledge that the statements are false or a reckless disregard of the truth, must be proven to establish a case of defamation.

According to media rights scholar Lawrence McNamara of Reading University, any development of the law of reputation is hampered by a lack of "sufficient attention paid to the nature of reputation or to the relationship between reputation and defamation."[145] How can the law protect what it has not defined? He focuses not only on

---

[140] Alice E. Marwick *et al., Youth, Privacy and Reputation (Literature Review)* Berkman Center Research Publication, 10-29. (2010).
[141] Post *supra,* fn 82 at 712.
[142] *See also* Amiram Yehudai, *Informational Blackmail: Survived by Technicality*, 92 MARQ. L. REV., 779, 821 (2009).
[143] *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).
[144] Post *supra* fn 82 at 693. Sullivan, an elected public official in Montgomery, Alabama, included in his duties the supervision of the police. He brought suit against the defendant news service for libel contained in an advertisement in the newspaper with information, some true and some not, that police under Sullivan's control had attacked students and a civil rights leader involved in a civil rights demonstration.
[145] LAWRENCE MCNAMARA, REPUTATION AND DEFAMATION, 1 (2007).

the legal tests as a means to that definition but also on the moral challenge such inquiry sets. Regarding the former, a defamatory statement was determined at common law to be one "calculated to injure the reputation of another by exposing him to hatred, contempt, or ridicule."[146] Into the twentieth century, the House of Lords modified the severity of that test to a requirement that the plaintiff be lowered "in the estimation of right-thinking members of society generally."[147] McNamara would agree with Post that reputation is "intimately related to the concept of community" but focuses on the moral values by that community.[148] He reminds us of the more vernacular tone of the test in Australia, that of the "ordinary decent or 'right-thinking' folk" who influence our reputation depending on whether our statements or image would make them think the less of us as a person.[149]

McNamara offers the following definition of reputation: a social judgment of the person based upon facts that are considered relevant by a community.[150] Unlike other definitions that he believes focus on either property or personality, McNamara stresses four components: *judgment* indicates a communal evaluation of the person; a focus on *facts* encompasses both implications of something a person has done (such as taking a bribe) or a characteristic they possess (such as sexuality); a reputation is *social* because it is a product of association; and those facts must be considered relevant by a *community*. McNamara reminds us that, prior to the age of Enlightenment of the 18th century, knowledge about how one ought to live "the good life" was derived from traditional institutions, most notably those focusing on religion.[151] Moral judgments, and hence reputation, were tied into how closely one aligned her daily life and deeds with the precepts of the prevailing creed. The Enlightenment moved the fundamental source of knowledge about the physical world to reason, with its emphasis on independent and critical thought. People began to pursue individual freedoms of thought and action that, in turn, reshaped their relationship with their communities. In practical terms, that

[146] *Parmiter v Coupland* (1840) 6 M&W 105, 108, Exch.
[147] *Sim v. Stretch* [1936] 2 All ER 1237, 1240 (Lord Atkin) HL.
[148] McNamara, *supra* fn 145 at 19 (noting the paucity of legal scholarship on libel law, especially in the UK, a situation remedied regarding historical background by Jill Cottrell, "What does 'Defamatory' Mean? Reflections on *Berkoff v. Berchill"* TORT L. REV. 149 (1998).)
[149] McNamara holds that the distinction has not been adequately made in English case law.
[150] McNamara *supra* fn 145 at 21.
[151] *Id.* at 23.

pursuit led some to found the democratic community of early America, based on the pursuit of human liberties and an escape from the older moral and societal tethers of traditional Europe. Underscoring that transition was the technological advances that re-defined working and socializing on both sides of the Atlantic. Looked at from McNamara's perspective, modernity was "an advance in the project of human freedom."[152]

McNamara suggests that moral judgment and the composition of community is still crucial to our reputations because morals become visible when norms are contested. Employing the example of homosexuality,[153] socially transmitted diseases,[154] and sexual assault,[155] he illustrates that values are not uniform from one community to another. When comments are made or images created that raise allegations of defamation, a court must form a view about who are the decent, right -thinking people who can serve as a legal standard in that community. He rejects the older legal tests of defamation that measured how a person's actions caused his community to shun and avoid him, or to ridicule him because those tests lack a moral component. The law can therefore only protect reputation if it exists in a genuine moral community. The problem with late modern life in western societies is that there exist competing moral taxonomies to reflect moral diversity. Based on that shift, McNamara approves of the American approach that a statement is defamatory if it would tend to prejudice the plaintiff in the eyes of a substantial and respectable minority."[156]

McNamara has developed his theories of reputation within the digital age; it is significant to the import of his analysis, therefore, that his primary work, *Reputation and Defamation*, published in 2007, makes no direct reference to the Internet community or online social networks. He might be making oblique reference to online communities when he concludes:

---

[152] *Id.*
[153] *Id.* at 34.
[154] *Id.* at 83-5
[155] *Id.* at 144ff.
[156] WILLIAM PROSSER, SECOND RESTATEMENT OF THE LAW OF TORTS, §559 (4th ed. 1971).

> …the courts are required to form a sense of how the jurisdiction forms a community. This may not be straightforward because contemporary Western jurisdictions are not easily seen as sharing a commitment to common values. …*They are not self-evidently 'communities'*. [157] [emphasis added]

Within the digital communications environment, reputation is integrally linked to trust, according to Giovanni Sartor, Professor of Legal Informatics at European University Institute. He finds an interesting, nurturing relationship between the two; trust is necessary because social rules online are weak, especially between parties who are distant in space and culture.[158] Sartor defines reputation as "the evaluative opinion people have of us, and the social mechanism that produces such an opinion".[159] Due to the superficial nature of online conversations, and the fact that contacts are often not likely to be repeated, we seek a rational basis for reliance on such contacts. That comes from information about the individual counterpart, particularly reference to his or her social consideration, that is, to reputation. Reputation emerges from shared beliefs that, as McNamara warned above, are increasingly rare in the moral sphere of postmodern life. Sartor advises we particularly need to rely on such reputational information as specific attitudes and capacities (such as technical competence of a professional) and the person's propensity to act in a certain way, through indications of prior cooperation, reciprocity, respect for existing conventions, and of other people's interests. By relying on an individual's reputation, we gain a cognitive basis for our decisions to trust that individual, and we induce that person to behave in a certain way, and to do so consistently, so we can rely on his continued participation.

Sartor enters the robust debate about online rights of erasure by arguing against an absolute right of the data subject to determine which data is made public. If a person has an absolute right to self-determination over her data, that could "impair the correct formation of reputation" by blocking the circulation of any negative information regarding her, thereby making "reliable reputation unavailable". Those who become aware of the filtering of personal details will tend not to develop trust in her as a resource of accurate information.

---

[157] *Id.* at 229.
[158] Giovanni Sartor, *Privacy, Reputation, and Trust: Some Implications for Data Protection*, Eur. U. Inst. Working Paper No. 2006/04, 4 (2006) http://ssrn.com/abstract=891123.
[159] *Id* at 5. Sartor's ideas are presented here as set out in pp. 3-7.

Sartor cites US Court of Appeal Justice Richard Posner who views informational privacy as an inappropriate subject of legal protection because, by allowing the data subject to pick and choose the personal information about her that is released to others, it encourages a type of self censoring that projects a false or incomplete reputation and hence engenders fraud. That would amount, in Posner's view, to a right to privacy giving legal protection to deception. Further, it would lead to an erosion of trust and would assert a paternalistic intervention that threatens the autonomous functioning of the markets in a free market system. Sartor agrees: he sees a "double noxious effect" of self-censoring: on the one hand it permits a person to manipulate his personal image, and on the other it impedes the "autonomous formation of social opinion" that shapes reputation.

Sartor admits that favouring privacy-as-data control protects certain important legal values, such as freedom, intimacy and dignity. As well, it ensures the possibility that one can change and that keeping certain personal information private can prevent discrimination. The latter is particularly important for avoiding stigmatization, a shunning that can influence others to discriminate, often based on erroneous information. As well, Sartor sees virtue in controlling the revelation of certain data about oneself to people who are able to put them into context. On the other hand, too much context is the online norm when we just use a cursory search to familiarize ourselves with a person and their deeds. With an overabundance of information available, what Thierer recognizes as "an increasingly intractable information control problem",[160] we tend to settle for just a few search entries that might give an incomplete, biased or even false representation. More information might put those impressions in context but it might, just as well, confuse or further bias the reader. Without individual data control, warns Sartor, the sheer barrage of information overwhelms us or demands too much time to sort through, so we revert to accepting the first few 'facts' and descriptions to come to an assessment of a stranger's reputation.

Internet scholar Mayer-Schonberger focuses on the negative effects brought to reputation by the heightened visibility of the Internet. "Consider that in the analog age,

[160] Adam D. Thierer, "The Pursuit of Privacy in a World Where Information Control is Failing." 36 HARV. J. L. & PUB. POL. 410 (2013). (Pursuit Of Privacy)

if one had a dark side, he could hide it".[161] He agrees with author and legal historian Lawrence Friedman's aphorism "if you can't be good, be careful"[162] to point out the enhanced transparency offered by the Internet. That has societal benefits for learning more about each other and reducing people's inclination to hide their dark sides. Mayer-Schonberger proceeds to show, however, that deception and creating a false reputation is just as easy online as offline. Although digital memory is static and constant, and so perpetuates any errors about our histories, we can easily manipulate our reputation by selecting what information about us we post online in the first place.[163] We therefore retain some control over our public selves, although we lose the power balance when it comes to the unilateral data collection by governments and corporations.

Reputation management has emerged as one solution to that control dilemma.[164] As anyone exposed to digital natives will quickly affirm, "major aspects of their lives – social interactions, friendships, civic activities – are mediated by digital technologies."[165] John Palfrey and Urs Gasser distinguish between a person's *personal* identity and *social* identity. Within the life of a 16 year-old girl, her personal identity might be controllable, through her self-expression and interests. Her social identity, however, is primarily beyond her control. Her social identity is visible to onlookers at any moment from associations she makes on Facebook, MySpace and other social networking spaces or links in blogs that become links in other people's blogs. In turn, "the actions of her friends, and their shifting reputations, can affect her identity and reputation in ways that third parties can observe."[166]

While messaging, posting and other user-generated activities have, to date, come with little cost or apparent supervision, Internet scholars complain of one's loss of control of online identity. As social image-making migrates to the Internet, gossip and shaming are shifting dimension. Particularly influenced are young Internet users who rarely distinguish "the online and offline versions of themselves" when thinking about

---

[161] VIKTOR MAYER-SCHONBERGER, DELETE – THE VIRTUE OF FORGETTING IN THE DIGITAL AGE, 19 (2009).
[162] Friedman, *supra* fn 96.
[163] Mayer-Schonberger, *supra* fn 161 at 107.
[164] JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).
[165] *Id.* at 2.
[166] *Id.* at 19.

peer opinion of their identities.[167] Coupled with the instantaneous and worldwide accessibility offered by digital media, the functional fluidity between real world and virtual presentation of self creates new kinds of opportunities for youth to "connect, communicate and develop their public identities".[168] Mizuko Ito *et al.* studied young Americans under 25 over a 3-year period to learn how they were integrating new media into their everyday agenda and practices, and how that changed their negotiations with adults over literacy, learning and authoritative knowledge.[169] They found online socializing connected peers through niche interests, but also afforded opportunities to publicize themselves through their creative work, hence gaining new forms of visibility and reputation.

Marwick *et al.*, in their literature review of *Youth, Privacy, and Reputation*, found young people were quite sensitized to reputational risks from marketers, online predators, identity thieves, and future employers. They seemed less aware that their private data could be manipulated or transferred from one source to another. While acknowledging that young people go online to seek validation by their peers, they also crave new spaces for socialization, exploration and experimentation. Those objectives pose high reputational risks. Marwick *et al.* noted that youth's perception of online space, unlike that of their parents and other adults, is of a private social space; they regard Facebook and other net platforms as virtual corners to hang out, engage in personal talk and gossip, flirt, share secrets, and conduct all the other social behaviors that they engage in offline. They therefore view any attempts at access or oversight by those adults as a clear invasion of their private space. Palfrey and Gasser worry about youth's inability to distinguish between "the online and offline versions of themselves" as they

---

[167] Marwick, *supra* fn 140 at 51.

[168] Mizuko Ito *et al.*, Living And Learning With New Media: Summary Of Findings From The Digital Youth Project, John D and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, 9-10 (2008), https://mitpress.mit.edu/sites/default/files/titles/free_download/9780262513654_Living_and_Learning.pdf .

[169] *Id.* at 1 (The ethnographic study focused on various geographical sites and research methods, ranging from questionnaires, surveys, semi-structured interviews, diary studies, observation, and content analyses of media sites, profiles, videos, and other materials. Collectively, the research team conducted 659 semi-structured interviews and collected 10,468 profiles of subscribers to sites such as MySpace, Facebook and Neopets, 15 online discussion group forums, and more than 389 videos.)

establish and communicate their identities simultaneously in the physical and digital worlds."[170]

Social media scholar dana boyd points out that online networking is based on the profile system, a use of the individual home page that allows users to create a persona they choose to present publicly. Those data include a referential list of friends and ample opportunity to comment on others' profiles, friends, opinions, images and other components of reputation building. The significance of those aspects of online interaction is that they are very public in nature: "friends are publicly articulated, profiles are publicly viewed, and comments are publicly visible."[171] The result is that, in all cultures where Internet access is possible, every user has the potential to be a celebrity. Consider the few who gained such fame or notoriety in Brandeis' day: one had to be significantly in the public eye through professional achievements, or the vicissitudes of fame and notoriety. Only those few were gossiped about in any significant public way: today all of us are learning to expect the scrutiny that was once reserved for the "famous and infamous".[172] "You have movie-star issues," commented one such social media user, "and you're just a person." The sobering cultural impact of such unprecedented voyeurism, exhibitionism and inadvertent publicity is that the Internet's constant remembering threatens, "at an almost existential level", our ability to reinvent ourselves and overcome our miscues of the past.[173]

Laura E. Heymann notes that beyond plaintiff and defendant, another interested party in the matter of reputation is the audience or society whose judgments mold those reputations.[174] She observes that society holds a responsibility for the stability of reputations and for encouraging community cohesion or in curbing the flow of false or hyperbolic information. In Heymann's words, "an audience-focused theory helps explain the importance of truth to the construction of reputation."[175] It is socially problematic for a society's members to be generating false information about themselves or other

---

[170] Palfrey & Gasser, *supra* fn 164 at 20.
[171] dana boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics,* in D. BUCKINGHAM, ED YOUTH, IDENTITY AND DIGITAL MEDIA, 126 (2007).
[172] Jeffrey Rosen, *The Web Means the End of Forgetting,* NYTIMES (21 July 2010) http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?...all
[173] *Id.*
[174] Laura E. Heymann, *The Law of Reputation and the Interest of the Audience,* 52 B. C. L. REV. 1342 (2011).
[175] *Id.* at 1419.

members. Society also plays a role in fine tuning what speech it will tolerate in order not to chill democratic participation: mere opinion, satire, and defamatory statements about public figures will be tolerated to the extent they are not done with malice or they do not incite violence.[176]

Finally, the ideas of Stijn Smet regarding the relationship between free speech and individual reputation are important for what they reveal about adjudicating opposing fundamental rights. Smet gives the example of the European Convention on Human Rights (ECHR) that guarantees both the right of free expression[177] and the right to protection of one's reputation.[178] That information is important for the clarity it can bring to judicial reasoning when both rights are recognized as having value. Smet proposes a three-step model: first, determine whether the case presents a "false conflict".[179] Such a situation might occur when, for example, one party is under procedural pressure that compromises his ability to adequately present his case. The necessity to bring an action within a reasonable time might be represent such pressure. A judge in that case can show some latitude in the procedural rules, thereby averting a false conflict. Secondly, determine whether a compromise is available that will keep both rights intact as much as possible.[180] If no compromise exists, a judge must compare the rights according to the following criteria: 1) which right, if denied, would create the most serious impact; 2) does the infringement affect a core or periphery aspect of the right; 3) are there additional rights in the balance for either party; 4) does either right involve a general interest shared by other members of society; 5) is either right to be exercised in a manner that is contrary to the very aim it is designed to achieve; and 6) are both rights being exercised responsibly.[181] Those concepts illuminate the values a court would assign to reputation and free expression when faced with their conflict.

---

[176] A testing of those limits could be observed in the January 2015 murders of journalists at the Paris satire magazine Charlie Hebdo.
[177] Article 10, para 1.
[178] *Id.* at para 2.
[179] Stijn Smet, *Freedom of Expression and the Right to Reputation: Human Rights in Conflict,* 26 AM. U. INT'L REV., 183, 184 (2010).
[180] The German Constitutional Court recognizes that doctrine as the *Praktische Konkordanz, id* at 189.
[181] Smet, *supra* fn 179 at 191.

2.2 Theorizing Memory

> Has it ever struck you, Connie, that life is all memory, except for the one present moment that goes by you so quick you hardly catch it going?[182]
>
> ***
>
> The beauty of the human mind and human forgetting is that, as we forget, we're able to generalize, to abstract, to see the forest rather than the individual tree.[183]

In this section we call on various theorists of memory, from both the individual and collective perspective, to build an appreciation of the new face of memory in the digital terrain. First, we consider the creative process involved in memory as set out by British psychologist Reginald Bartlett in the early 20th century and how that process reaches dramatic results in the 21st century with the activities that produce false memory. Next, legal historian Inga Markovits develops a theory that our memories, particularly as they recreate prominent people and events, are shaped and manipulated by the powerful and political. Gary Fine, as behavioral scientist, illustrates how moral entrepreneurs can manufacture disparate reputational fates for two historical figures who, by all accounts, are very similar in make-up, experience and abilities. Jonathan Zittrain shows how video images can distort memory and perpetuate embarrassing or false stories that are best left unexposed. The work of Liam Bannon discusses how both memory and forgetting are necessary to avoid the banality introduced into our lives by man-machine interactivities. Perfect remembering is a concept addressed by Internet scholar Viktor Mayer-Schonberger who emphasizes the tasks required of online functioning that call on a healthy dose of daily forgetting. For Canadian scholar Patrick Macklem, law is memory, as exemplified by the struggles of the Brok family to gain restitution for property they owned in pre-war Prague. What these various accounts tell us is that the way we remember might be as significant to reputation as what we remember.

Liam Bannon admonishes us as individual Internet users for not fully appreciating the beneficial necessity of forgetting. His studies focus on social and cultural nuances that could keep our highly technologically-infused lives in the future from a banal and barren pre-occupation with machines. Bannon suggests that we can

---

[182] TENNESSEE WILLIAMS, THE MILK TRAIN DOESN'T STOP HERE ANYMORE, 36 (1963).
[183] Mayer-Schonberger, *supra* fn 161 at 16.

fight such banality by grasping "the duality of human memory," the equal importance of forgetting and remembering.[184] As a balance to the information processing skills that we have all been taught since the arrival of the computer, Bannon sees a dire need for a "judicious forgetting" that can ease our immersion into a future world where human intervention in the interconnectivity of machines will be negotiated on a daily basis.[185]

Bannon frames his considerations of forgetting as a positive feature of present and future life, not a default mechanism within the emerging technologies of ambient intelligence and ubiquitous computing. The latter advances in communications technology have the potential to enable most of our future functioning in society via machines talking to machines, ideally in our service but without much human intervention. That development, argues Bannon, has us thinking that forgetting is a passive activity, something that occurs when there is a default in our abilities to amass and remember unquantifiable amounts of information. Forgetting, Bannon argues, is an active pursuit, not a mechanical erasure or failure to retrieve.[186] He presents, as support, the commentary of early 20th century British psychologist Sir Frederick Bartlett on the less-than-perfect virtues of human remembering:

> Remembering is not the re-excitation of innumerable fixed, lifeless and fragmentary traces. It is an imaginative reconstruction, or construction, built out of the relation of our attitude towards a whole active mass of organized past reactions or experience, and to a little outstanding detail which commonly appears in image or in language form. It is thus hardly ever really exact, even in the most rudimentary form of rote recapitulation, and it is not at all important that it should be so. [187]

Bartlett's thesis is that not only is human remembering imperfect but it is not a full-package experience stored in the brain. It is comprised of various images that are constructed in the moment. Remembering is a creative act, seldom a "fixed, lifeless" copy of the original experience as was earlier thought.

Bannon concludes that forgetting is good for human well-being as it overcomes the stultifying and paralytic effects of amassing so much accurately retained data. He

---

[184] Liam Bannon, *Forgetting as a Feature, not a Bug: the Duality of Memory and Implication for Ubiquitous Computing"* 2 CODESIGN, 3-15 (2006).
[185] *Id.* at 6.
[186] *Id.* at 5.
[187] FREDERICK BARTLETT, REMEMBERING: A STUDY IN EXPERIMENTAL SOCIAL PSYCHOLOGY, 205 (1932).

recommends several technical solutions that will help Internet users to forget: marking private emails and messages so that permission is required before anyone can pass them on; constructing digital shelters within our community where electronic signals are blocked within the shelter and people can gain some reprieve from always being plugged in;[188] creating personal sweeper technologies that would hinder the pickup of meaningful signals from particular sites, akin to military jamming technologies; and electronic tagging of information with 'sell-by' dates, after which the information would self-destruct. Bannon is most insistent that, whatever our choice of technology to take us away from total remembering, our ability to live in the moment indicates our comfort with submitting to temporary oblivion which he holds as having positive benefits to our social and economic lives.

Peter Fleischer, Chief Privacy officer for Google, suggests that seeking a clean digital slate marks an attempt to let people "wash away digital muck", or to "delete the embarrassing stuff".[189] He plays down claims to a right to oblivion as a mere fashion, what he calls the "new black of censorship fashion". From his corporate perspective, Fleischer sees privacy being used as a screen to justify online censorship or, in the case of journalists and the First Amendment right, what used to be achieved by crying libel or defamation. He warns that recognition of the right to censor opens up the floodgates to Internet regulation, a possibility that the public have, to this point, ardently rejected as repressing free speech.

False remembering is another facet of memory that draws suspicion and distrust, and can be catastrophic for reputations. In the alternative, it can be met with understanding or a willingness to explore further the processes of memory.[190] Similar experiences of two American public figures make the case. NBC Nightly News anchor Brian Williams "misremembered" actual events when he reported being on a Chinook helicopter in Iraq in 2003 that was forced to land under enemy fire. Further

---

[188] Bannon attributes that idea to Peter Sepulveda-Sandoval, *Digital shelters*, Presented as a Poster at CAST01: Living in Mixed Realities, a conference on artistic, cultural and scientific aspects of experimental media spaces, 21-22 September 2001, Bonn Germany.

[189] Peter Fleischer, *Foggy Thinking about the Right to Oblivion*, Blog (9 Mar. 2011) http://peterfleischer.blogspot.ca/2011/03/foggy-thinking-about-right-to-oblivion.html.

[190] Vinay Menon, *Give Williams the benefit of the doubt: Menon,* TORONTO STAR (9 Feb. 2015), http://www.thestar.com/entertainment/2015/02/09/give-williams-the-benefit-of-the-doubt-menon.html.

investigation in 2015 reveals Williams was on another helicopter that arrived one hour after the event.[191] Similar claims of having a different memory than the official story were made by then-US First Lady Hillary Clinton in 2007. She stated she had been the victim of sniper fire while disembarking from a plane in Bosnia; videos of the event show no such disturbance.[192] When faced with widespread journalistic accusations of filing a false report[193] or "concocting war stories"[194] (in Williams' case) or of "mischaracterizing" or "overstating" her foreign political experiences (in Clinton's),[195]both public figures admitted to telling and retelling the story over the years to the point of believing their false accounts.

Similar observations were made of President Ronald Reagan who, according to biographers, gave others the impression that he had been at Normandy and at the liberation of the Nazi death camps when he had, in fact, spent the war making movies in Hollywood. Reagan reportedly later told an associate, "Maybe I had seen too many war movies, the heroics of which I sometimes confused with real life."[196] While Brian William's employers speak of his "inexcusable" behavior and distance themselves from his story by placing him under a period of suspension, Williams speaks of the incident as where "we were all I think - scared…and it all became a fog of getting down on the ground." Regarding his false story, he stated, "I don't know what screwed up in my mind that caused me to conflate one aircraft from the other [*sic*]"[197]

---

[191] Pamela Enger, *Brian Williams explains how he 'misremembered' the Iraq helicopter incident,* BUSINESS INSIDER (19 Feb. 2015), http://www.businessinsider.com/brian-williams-explains-how-he-misremembered-the-iraq-helicopter-incident-2015-2.

[192] Jeff Mason, *Hillary Clinton calls Bosnia snipe story a mistake,* REUTERS (25 Mar. 2008), http://www.reuters.com/article/2008/03/26/us-usa-politics-clinton-idUSN2540811420080326.

[193] Tom McCarthy, *Brian Williams' reports on Katrina called into question by New Orleans residents,* GUARDIAN (6 Feb. 2015), http://www.theguardian.com/world/2015/feb/06/brian-williams-hurricane-katrina-new-orleans-residents (speaking of "revelations earlier this week that he had peddled a false story".)

[194] Eliana Johnson, *Is Brian Williams Invincible?* NATIONAL REVIEW ONLINE (6 Feb. 20150, http://www.nationalreview.com/article/398118/brian-williams-invincible-eliana-johnson.

[195] Suzanne Smalley, *Hillary: Made-Up Memories?* NEWSWEEK (24 Mar. 2008), (reporting that Clinton had told the story "for many years, gradually adding embellishment and changing details. Perhaps she may have actually come to believe it.")

[196] *Id.*

[197] Travis J. Tritten, *In his words: Brian Williams' interview with Stars and Stripes,* Stripes.com (9 Feb. 2015), http://www.stripes.com/news/us/in-his-words-brian-williams-interview-with-stars-and-stripes-1.328590 - .VNkOaJw3TBo.twitter.

Clinton defends her recreated memory of the Bosnia event by stating she was merely mistaken and subject to human error.[198] Both explanations, if true, support Frederick Bartlett's assertion that memories are dynamic and mu reconstructions of disruptive events, not static copies of their elements. Proof is elusive, however, as memories can only be communicated through the holder's recall, a process that is little understood by medical science. Cognitive psychologist Christopher Chabris of Union University in New York explains how memory distortion occurs: "each time you are telling a story you are not pushing play on a cd player but reconstructing the event" and the "information is assembled from different sources. You insert that into your story."[199] So you lose the ability to tell which part is false. The lesson overall is that memory is less reliable than we think.

Julia Shaw, professor of forensics at the UK University of Bedfordshire agrees that memory is constructive and might not signify an attempt to deceive or behave in a way that is less trustworthy.[200] Shaw and Stephen Porter of the University of British Columbia have implanted complex false memories of committing crimes into subjects through guided imagery. In a recent experiment, they determined that of 30 participants who were falsely told they had committed a crime as a teenager 21 (71%) were classified as having developed a false memory of the crime.

False memory research has contributed in some respects to our understanding of our memory recreation processes. We are learning, for example that memory is greatly affected by the choice of wording used by another when he questions our version of events,[201] and that false conclusions can be convincingly implanted for an event that

---

[198] Daniel Nasaw, *Tale of coming under sniper fire mistaken, Clinton admits,* GUARDIAN (25 Mar. 2008), http://www.theguardian.com/world/2008/mar/25/uselections2008.hillaryclinton.

[199] Christopher Chabris, *The Current with Anna Marie Tremonte,* CBC Radio Podcast (11 Feb. 2015), http://www.cbc.ca/radio/thecurrent/malleable-memory-hearing-aids-and-death-threats-from-the-kremlin-1.2962410/memories-are-malleable-looking-for-truth-behind-false-memory-1.2962457

[200] Julie Shaw and Stephen Porter, *Constructing Rich False Memories of Committing Crime,* PSYCH. SCI. (14 Jan. 2014).

[201] Elizabeth F. Loftus, *Reconstruction of automobile destruction – Example of interaction between language and memory,* 13 J. VERBAL LEARNING & VERBAL BEH., 585 (1974) (explaining that using the word 'smashed' rather than 'hit' when asking about an automobile accident was more likely to evoke a false memory of broken glass at the scene).

never happened.[202] The implications of such massaging of memories are profound for our reputations and careers. Further research might help ease public suspicions of memory that is inconsistent with the original event, such as learning that a good mood is more likely to colour memory than sadness,[203] or that false memory can be triggered by sleep deprivation.[204] For now, our understanding as a western society of the psycho-chemistry of memory, like the sociality of reputation, is disappointingly rudimentary.

Mayer-Schönberger posits that the difference between how humans remember and how the Internet remembers is deep and fundamental: humans forget, or remember selectively, while the Internet remembers everything in perpetuity.[205] He points to time and money as the factors that, in the pre-digital age, discouraged the storage of large masses of information. With the arrival of digital acquisition and cloud computing, storage of limitless amounts of data is possible. In the pre-digital era, storage of analog information meant costly physical space, and costly retrieval. All of those objections have been met by digital technology that compresses data infinitesimally, and makes accessing that information far easier.

Mayer-Schönberger comments on the sheer bilge of online data that has accumulated as a result: "now we are steeped, not just in knowledge, but in memory".[206] That development comes with problems of its own; primarily the difficulty of achieving any systematic, depersonalized retrieval or analysis of such Big Data. Mayer-Schönberger highlights what we have lost in the progression to digital memory. Human forgetting, he reminds us, both on the individual and societal level, allowed us to act and think in the present rather than being tethered to an ever-more-comprehensive past.

For legal historian Inga Markovits, we can have private memories and public memories. The law plays an important role in how we remember. It shapes our

---

[202] Elizabeth F. Loftus & Jacqueline E. Pickrell, *The formation of false memories*. 25 PSYCH. ANNALS, 720-725 (1995) (implanting memories in a 14-year-old of being lost in a mall as a child).
[203] Justin Storbeck & Gerald L. Clore, *With Sadness Comes Accuracy; With Happiness, False Memory Mood and the False Memory Effect,* 16 PSYCH. SCI., 785-791 (2005).
[204] Steven J. Frenda, *et al., Sleep Deprivation and False Memories,* PSYCH. SCI. (2014) (false memory was noted where encoding occurred after a prolonged period of no sleep, not before).
[205] Mayer-Schonberger, *supra* fn 161 at 32.
[206] *Id* at 12.

recollections of the past to fit those who dominate the present.[207] She points out that, as individuals, we have no control over our memories. "We forget what we would like to remember, remember what we would like to forget", have memories triggered by what we smell and taste, and must accept that "events become important because we remember them".[208] For private, individual memory the past rules the present. With Markovits' public memory, however, the converse rules: the present rules the past. Powerful public figures in each era determine which names and events survive as worthy of remembrance. She gives the example of public monuments, which are chosen by the political elite and strategically placed to perpetuate the public memory of a particular individual and his/her particular deeds. No society prefers to memorialize its bad deeds (slavery in the US) or people (holocaust perpetrators in Germany). Those acts are excised as mistakes of history. In that respect, public memory legitimates selective past acts and personalities.[209]

Law seems a likely candidate to assist with memory, argues Markovits. It has a lot to do with legitimacy and it proto-typifies model citizens, such as the 'prudent' or 'reasonable' man and the 'reckless' driver. Informed by our likes, dislikes, moral wishes and concepts of the norm, the law validates those past events of which we approve, and punishes those we do not. Law, therefore, has developed rules on how to investigate the past by discriminating what is legally 'reliable' from what is not.[210] Law accomplishes that objective by setting requirements for standards of proof, burdens of proof, fictional ideals such as the 'reasonable man' or 'right thinking person', theories of the case and stringent legal tests. Law has highly influential filtering powers when it comes to memory. As such, it is an important medium for defining our past.

Markovits suggests that East Germany's role in the holocaust is an apt example of how collective memory can reshape history and dictate how we remember and forget. There has been much recent talk in Germany about the *Aufarbeitung*, or 'working over' of past events of the Nazi regime. That word has become synonymous in modern Germany with coming to terms with the past, or rethinking events that portray

---

[207] Inga Markovits, *Selective Memory: How the Law Affects what we forget and remember about the past: the Case of East Germany,* 35 LAW & SOC. REV. 513, 513.
[208] *Id.*
[209] *Id.* at 314.
[210] Diane Martin first introduced such concepts to this author during "Persuasion and Proof", an LL.M. course at Osgoode in 2005.

Germans in a negative light. Such an act calls on selective forgetting and remembering that remakes the German national character like making old garments into new.[211] In other words, the past that Germany is trying to come to terms with has already been preemptively construed by those in positions of influence.

Jonathan Zittrain notes, like Markovits, that it is the higher rung on the socio-political ladder that most influences what is retained and 'remembered' on the Internet.[212] He asks, what about historical events that, in retrospect, turn out to be untrue; when an Internet user logs on twenty years after the posting of the inaccuracy and there is no overriding notice that the account is in error? It is presented as if it just occurred, and in a false light or with factual inaccuracies. The erroneous event has been archived online in perpetuity, without any reference to its inaccuracy or misrepresentation.

Zittrain gives as example a series of YouTube video stills portraying a bombing in the Middle East that were photo-shopped to deceive the viewer; many years later they persist online with no corrections or other indication that the representations are inaccurate. The video stills show a rescuer, in a baseball cap, pulling the injured victims of a bombing out of a rubble site. A second video still shows the same rescuer, himself now a fatality, being lifted out of a similar pile of rubble. Through close examination, Zittrain determines that the latter video was taken *before* the first still. In other words, the photo of his removal from the rubble has been altered by photo finishing software; it is a false portrayal of what happened. One detail that gives the duplicity away is that the baseball cap, in the photo of the rescuer as a dead victim, is under the man's arm and quite obviously tightly pressed to his side. That erroneous series was posted and distributed by Reuters, a reputable news service. Zittrain shows how, shortly after the posting on YouTube, the fake series of images were removed from view, but are still present in the online video archives and thereby, with a little work for the viewer, accessible to the public. Zittrain concludes that, if it is privacy or accuracy we seek, the Internet is not the place to find it. Even so, the offending or erroneous images persist online into the future.

---

[211] Markovits, *supra* fn 207 at 513.

[212] Jonathan Zittrain, *Build Internet Communitarian Memory"* Open Democracy Online, https://www.opendemocracy.net/jonathan-zittrain-tony-curzon-price/build-internet-communitarian-memory.

Northeastern University behavioral scientist Gary Fine speaks of "reputational entrepreneurs", that powerful elite that are able to control public memory of historical figures using their narrative facility and institutional placement.[213] Fine compares Warren Harding and John F. Kennedy, both American presidents: the former was rated the lowest in the estimation of historians and the public for his presidential abilities, the latter rated near the top. Political opponents and the press set that agenda, Fine insists, while neither colleagues nor public have risen to defend Harding. Both men were outgoing, personally charming, popular in their roles as US Senators prior to their terms as president, accused of sexual improprieties while in the White House, and viewed as too close to their Attorneys General who were therefore considered political liabilities. Both died during the third year of their presidencies. History judges Kennedy as one of the best presidents in terms of civil rights record and overall popularity, although Harding was equally so viewed during his tenure. In hindsight, however, Harding is maligned as a failed president, the worst chief executive in US history.[214]

Fine reminds us of Durkheim's principle at work here: that images of a highly successful or a deeply flawed leader rallies social cohesion and communal solidarity. The nature of that image is shaped by what Fine terms "reputational politics". Reputations are grounded in a social construction of character, subsequently generalized to policy and thence to the character of the society itself.[215] What politicians, competitors and journalists determine to be the prevailing reputation of a public figure is generally the persona adopted by historians and therefore by the public for succeeding generations. Such manipulation constitutes collective memory.

Fine also speaks of *moral* entrepreneurs, those arbiters of social mores that determine whether a historical figure has promoted or defiled the values that their community holds dear. Over time, the evaluation of the moral worth of our leaders rests less on their individual attributes or triumphs and more on the causes of their successes or failures. To be recognized as a failure suggests the absence of supporters who would propose a historical justification for a positive reputation. "[T]hus the figure is an

[213] Gary Fine, *Reputational Entrepreneurs and the Memory of Incompetence: Melting Supporters, Partisan Warriors, and Images of President Harding,"* 101 AMER. J. SOC. 1159-1193 (1996).
[214] *Id* at 1160.
[215] *Id* at 1161.

'orphan', scorned by rivals and neglected by ostensible allies".[216] The prevailing impression of Harding was that he was an unintelligent man, too trusting of his cronies, a passive leader, indifferent to corruption, and passive in execution of his duties when the nation needed active leadership during the post World War I period. That perception is achieved by attacking Harding's agenda through his character, and by controlling memories of Harding through those in command of public, collective memory.

For Patrick Macklem of the University of Toronto, law is memory. He has studied the struggles of the Brok family to gain restitution for property they owned in the old city of Prague, Czechoslovakia prior to the communist takeover during the 1930s.[217] The Broks owned the building and operated a textile business out of the ground floor. They lived in a spacious apartment within the building and rented out the remaining apartments to employees. As the Nazis began their 'reconfiguration of Europe' in the 1930s, they confiscated the Brok property at Rybna 9 and transferred title to a Slovakian company. The Broks emigrated to Canada, except for one son who remained in the building as a tenant. After the war, Rybna 9 was treated as state property by the Czechoslovak Socialist Republic and, in 1990, sold as part of the post-communist, liberal democratic reforms, to an offshore holding company. One of those reforms included an initiative to return property, taken by the Nazi and Communist regimes, to their original owners.[218]

In contemporary Europe, post war restitution claims can be brought either before the ECtHR or the United Nations Human Rights Committee ('the Committee'). The Brok family took the Czech government to court and their case was eventually settled by the Committee in their favour under the guarantees of equality enshrined in the International Covenant on Civil and Political Rights. Macklem's conclusion after reviewing several restitution cases that have been decided by either fora is that the ECtHR approaches its cases with "a modernist impulse to repudiate history" because it refuses to entertain any equality claim under the European Convention on Human

---

[216] *Id.*
[217] Patrick Macklem, *Rybna 9, Praha 1: Restitution and Memory in International Human Rights Law,* University of Toronto Public Law Research Paper No. 04-12. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=617022
[218] *Id* at 4.

Rights (ECHR) regarding restitution rights in post-Communist Europe. The Committee, however, is willing to "remember certain pasts as a matter of equality".[219]

Macklem observes through the Brok case that international human rights law is beginning to "construct legal spaces for the expression of collective memory".[220] Law has the capacity to memorialize shared memories, a role that takes on particular significance when a minority community is under pressure to put aside the social, political and economic pressures of its shared past. In that sense law is "dialogical, exercising an active and ongoing engagement with the past". That role can justify minority rights and prompt the larger community to respect a minority's collective past and present identity.[221]

In contrast, the ECtHR guarantees non-discriminatory enjoyment of rights and freedoms as enshrined in Article 14 of the ECHR. The Court has long taken the narrow view that, in order for judicial recognition as an equality right, claims must address only those rights contained within the four corners of the Convention. By denying restitution claims for the confiscation of property by the Nazi regime, the ECtHR has shown "a modern impulse to repudiate Europe's burden of the past"[222] and a willingness to forget. Macklem points out the danger in such forgetfulness: that the burden of Europe will become heavier as it becomes "cloaked in darkness", to the point where Europeans might forget who they are.

In summary, the foregoing academic sources illustrate the intricate correlation between the concepts of reputation and memory, whether within the context of a community's opinions that shape our individual good name or the societal and political pressures to either remember or forget our collective pasts in order to address the stigma created by a dark history. The significance of that symbiotic exchange is that memory can be determinative of reputation, whether of an individual or a collective. If those memories are complimentary, we tend to favour perpetuating them; if unfavourable, we might seek forgetfulness or the right of erasure. In the next section,

---

[219] *Id. at* 5.

[220] Maurice Halbwach, *On Collective Memory* in ON COLLECTIVE MEMORY, L.A. Coser (ed & trans.) (1992) (introducing the concept of collective memory to signify shared memories that form part of the fabric of a community's beliefs).

[221] Maclem *supra* fn 217 at 16.

[222] *Id.* at 17.

we explore literature that defines the role of law in protecting our privacy interest by choosing those to whom we would reveal our personal identities and memories. We begin with the efforts of Harvard law alumni Brandeis and Warren to import into America the European right of privacy, with significant implications that endure into the digital age.

2.3 Theorizing Privacy

> Now the right to life has come to mean the right to enjoy life,
> - the right to be left alone.[223]
>
> ***
>
> Privacy is shorthand for breathing room to engage in the processes
> of boundary management that enable and constitute self-development.
> So understood, privacy is fundamentally dynamic.[224]

There is a considerable lack of clarity within American legal and philosophical discourse regarding how to define privacy. American jurist Richard Posner noted in 1977 that the concept is "elusive and ill-defined".[225] Academics continue to disagree over whether privacy is an instrumental term designed to protect core values or whether there is something intrinsic in the concept itself that needs to be respected.[226] To add to the confusion, privacy as an academic consideration is often included under the rubric of security, justice, liberty, or human rights.

The disparity in perceptions of the place of privacy in our lives is further revealed by juxtaposing the above quotations, the first made in *fin de siècle* America by Harvard law colleagues Louis Brandeis and Samuel Warren, showing hopeful determination that one can reap the full enjoyment of life by closing one's doors to prying intrusions of press and government. The second quotation reveals the post-modern angst and nihilistic realism around the subject of privacy as provoked by our entry into the digital age. Julie Cohen, in the third excerpt, is more hopeful as she present privacy as a subjective entity we can manage and mold. In the simpler world of

---

[223] Brandeis and Warren, *supra* fn 112.
[224] Cohen, *supra* fn 75.
[225] Richard A. Posner, *The Right of Privacy,* 12 GEO. L. REV. 393, 393 (1977).
[226] *See further* Amitai Etzioni, *The Limits of Privacy* (1999); Charles Fried, *Privacy, 77* YALE L. J., 475-493 (1968).

Brandeis and Warren, there is a clear public/private divide; in the 21st century view that divide has collapsed or been eroded by technological gains in online communications. Cohen speaks for the more cosmopolitan view[227] that privacy is ours to define but also to safeguard.

This section will examine that development, commencing with the seminal contributions of Brandeis and Warren, of privacy as a legal right in America. We will then move to Harvard Law Dean William Prosser in codifying those principles into tort law. Prosser's formulation will then be compared to the European, more unified approach as exemplified in the German concept of personality rights. James Q. Whitman will explain that comparison as the difference between a European respect for personal dignity and the American safeguarding of personal liberty. Daniel Solove and Lawrence Friedman comment on observable transitions between the analog and digital worlds and the privacy challenges they pose. Helen Nissenbaum worries that the digital world has erased context, a factor also incorporated into Jeffery Rosen's discussion about how one must jeopardize more of one's privacy by revealing sufficient information to contextualize inaccuracies that affront reputation. Dana boyd reveals a personal digital experiment with her DNA that unwittingly exposes her extended family, including the unborn, to unnecessary reputational invasion. She asks whether privacy is an outdated concept that has no currency in an age of dystopian excess. Canadian surveillance scholar David Lyon picks up that query and toys with the concept of turning the state's probing eye back on itself. He warns that surveillance is no longer perceived as the horror we previously envisioned: for willing purveyors of others' secrets, it is at worst an annoyance that has to be negotiated.

Any thorough conceptualization of privacy as a fundamental right within the American tradition begins with two seminal articles: the first by American jurist Louis Brandeis and journalist Samuel Warren, who urged in 1890 that privacy be cherished as an individual civil right and its breach be a recognizable cause of action through US tort law; and a comparative piece in 2004 by James Q. Whitman of Yale University whose thesis is that cultural differences account for widely divergent views of privacy on each side of the Atlantic. While American's perception of the privacy right was founded on a

[227] 'Cosmopolitan' is used in the Stoic sense that we are all citizens of the world and hence its stewards.

culture of liberty, privacy advocates in Europe focus on the right to retain one's dignity.[228] In Whitman's words:

> What is at stake are two different core sets of values: On the one hand, a European interest in personal dignity, threatened primarily by the mass media; on the other hand, an American interest in liberty, threatened primarily by government.[229]

Those cultural distinctions define two very different expectations of privacy. Brandeis and Warren remind us that the framers of the US Constitution introduced the Fourth Amendment to protect individuals from unreasonable searches and the unwarranted intrusion of the state into citizens' property and private effects.[230] To the early framers of the constitution, such protection provided liberty. Those rights could not be infringed by the state without a judicial warrant and probable cause, a constitutional reminder that governors served at the will of the people. The roots of privacy needs in colonial America began with conceptualizing the family home as "a heaven for solitude and intimacy", a barrier against the intrusion of unwanted outsiders, including the state.[231]

In the early days of the American republic, expectations of privacy outside the home were not high. With the mails as the primary communication method in the new colony, citizens had dim hopes that their mail would arrive unopened. As first colonial postmaster, Benjamin Franklin insisted on mail carriers swearing on oath not to open the mails.[232] Franklin's replacement, however, in the face of the rising revolutionary tide of 1776, warned that all mails were subject to inspection by ministerial mandate if treason was suspected. Hence a system of Warrants of Assistance was implemented that gave the young government wide powers of search and seizure. It was those excesses that gave rise to the constitutional entrenchment of the Fourth Amendment and the impetus for defining a 'reasonable expectation of privacy' for the private citizen.

---

[228] James Q. Whitman, *The Two Western Cultures Of Privacy: Dignity Versus Liberty*, 113 YALE L. J., 1151.
[229] *Id* at 1219.
[230] The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[231] DAVID FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND, 36 (1967).
[232] ROBERT E. SMITH, BEN FRANKLIN'S WEBSITE: PRIVACY AND CURIOSITY FROM COLONIAL AMERICA TO THE INTERNET, 4 (2000).

Through common law challenges, the public/private line has progressively blurred over the intervening years to the point that, with the 21st century invention of wearable technologies such as Google Glass, we can spy on each other with immunity, adopting "participatory surveillance" that could render moot any privacy questions we might have.[233]

Free speech, as protected by the First Amendment, provides the most formidable challenge to privacy rights in America. Its development over the nineteenth and twentieth centuries has occurred primarily through the common law. Laws have lagged behind the development of institutional ways to access our private affairs, to the point where technological advancement leaves our expectations acutely compromised, most prominently by government and commercial institutions. That right is expanded by the interpretation by American courts of the First Amendment as extending to entrepreneurial rights as commercial free speech.

Another impediment to recognition of a right to privacy in American law was the fact that privacy is an intangible, inchoate privilege, without physical attributes like property, what Brandeis and Warren called the "products and processes of the mind".[234] The authors spoke of a growing desire for "the right to be left alone" from the prying lens of photography and reportage of the news media. They had a particular aversion to misuse of the photographic image; they were well aware of the ability of such images in the wrong hands to foment gossip and defamatory statements. They justified their increased need for solitude by reference to "the intensity and complexity of life, attendant upon an advancing civilization".[235]

Brandeis and Warren proceed to establish that the law of defamation, focused as it is on a person's interrelations with his community, proves an effective legal instrument to address injuries to reputation as a property claim, but insufficient to shield a person whose feelings for privacy have been offended and who therefore seeks to be left alone.[236] They maintain that the common law protects a person's right to

---

[233] Anders Albrechtslund, *Online Social Networking as Participatory Surveillance,* 13 FIRST MONDAY, (3 Mar. 2008), http://firstmonday.org/article/view/2142/1949; Matthew Braga, *Google Glass raises significant privacy issues,* FIN. POST (19 June, 2013) FP11. The Glass device enables the wearer to record other people in video and audio without their permission.
[234] Brandeis & Warren, *supra* fn 112 at 194. *Id* for all quotations in this paragraph.
[235] *Id.* at 197.
[236] *Id.* at 195, n 1.

determine when or if they wish to communicate their private thoughts and to whom.[237] They insist such rights are distinct from copyright law and property law and allow for a person to refuse publication or publicity and enjoy the "peace of mind or the relief afforded by the ability to prevent any publication at all".[238] Brandeis and Warren call that allowance the right of "inviolate personality" and equate it to the "right to the immunity of the person" or the German-based "right to personality".[239]

Brandeis and Warren's article is generally regarded as the impetus behind the creation of the four privacy torts as set out in Dean Prosser's Restatement of Tort.[240] They envisioned tort law as the appropriate mechanism for asserting those rights because the victim in a tort action could gain some satisfaction with remedies like injunctions or monetary compensation through damage awards, unless the matter was found to be so trivial that the court showed a preference for honouring free speech.

The interesting subtext of the article is that a seminal right to be forgotten is being recognized and encouraged by an American jurist and a journalist as early as 1890, even if couched in the proprietary aphorism that a man's home is his castle, a place of respite from the public eye of the state and the media. To this day, the heart of American privacy rights resides in protecting the sanctity of the home.

By the 1960s, Prosser had organized over 300 tort law decisions into four discrete causes of action for breach of privacy, built upon the work of Brandeis and Warren: 1) intrusion upon seclusion, 2) appropriation of the name or likeness of another, 3) public disclosure of private facts "not of legitimate concern to the public", and 4) disclosure of private facts that portray the victim in a false light.[241] Prosser concluded that privacy law in America was best founded upon:

> ...four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff…"to be let alone."[242]

That observation determined that the course of privacy law would be through four

---

[237] *Id.* at 198.
[238] *Id.* at 200.
[239] *Id.* at 207.
[240] Benjamin E. Bratman, *Brandeis and Warren's the Right to Privacy and the birth of the Right to Privacy,* 69 TENN. L. REV., 623 at fn. 10 (2002).
[241] Prosser, *supra* fn 156, §652B.
[242] William L. Prosser, *Privacy,* 48 CAL. L. REV. 383, 389 (1960).

disparate actions under tort law, not tightly bound to each other through any single concept.

In commenting on Prosser's achievement in clarifying privacy law, author Samuel J. Hofstadter noted that, "the doctrine has had a checkered career".[243] Prior to Prosser's text, states differed not only in their view of the scope of the right of privacy but even with respect to its existence. Prosser's classification proved "extraordinarily persuasive for wavering state courts and legislatures".[244]

Daniel Solove has been considered the modem heir to Prosser's deliberations.[245] In *Understanding Privacy*,[246] he conceives of information privacy, a broader field than tort privacy, in terms similar to Prosser's approach but incorporating "a plurality of different things" as inspired by interactions on the Internet and social media. [247] Unlike Prosser, who imposed a pre-conceived framework of privacy principles on different fact situations, Solove starts from the ground up, identifying the range of harmful actions perpetuated online and arranging them into a taxonomy comprising four privacy concepts: (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion. Each of those groups leads in turn to "different related subgroups of harmful activities."[248] For example, subcategories of harm relating to information collection are (1) surveillance, and (2) interrogation. Solove holds the belief, shared with Prosser, that privacy law concerns a range of interests to be protected, only some of which overlap and only in certain ways.[249]

With the assistance of Brandeis and Warren's historical perspective, the first tort above, intrusion upon seclusion, tells of a right to be free from unreasonable search and seizure (as encoded in the Fourth Amendment); the second tort, the appropriation of the name or likeness of another, suggests data appropriation that offends a right to oblivion; the third tort, public disclosure of private facts is the clearest statement of a civil right to privacy; and the fourth grounds, disclosure of private facts that portray the

---

[243] SAMUEL H. HOFSTADTER, THE DEVELOPMENT OF THE RIGHT OF PRIVACY IN NEW YORK, 53 (1954).
[244] *Id.*
[245] Schwartz & Peifer, *supra* fn 108 at 1941.
[246] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).
[247] *Id at* 101.
[248] *Id* at 103.
[249] Schwartz & Peifer, *supra* fn 108 at 2010.

victim in a false light, suggests potential grounds for civil defamation suits and could provide grounds for a right to be forgotten. Those actions are based in private law, however, and are not actions against the state. Americans are therefore still left with no definitive legal protection against challenges to personal privacy conducted by government action. [250]

James Whitman observes that continental European ideas of privacy even today "are just not much at home in American legal culture".[251] While he views the Brandeis and Warren article as an attempt to transplant a continental-style privacy law into the American context, Whitman judges it a failure because the culture of privacy, and the systems of law, rest on disparate principles on each side of the Atlantic. Such discrepancies impede efforts to arrive at a definition of privacy that would be acceptable on both continents.

Whitman reveals that the impetus for Brandeis and Warren's article was a report by the "yellow press" in its gossip column of a private party at the Warrens' house, media coverage that the authors found very intrusive.[252] He suggests that Brandeis and Warren, frustrated by the lack of protections in the extant American common law for such intrusions on their privacy, researched the law then in vogue in Europe and learned how it defined similar intrusions as insults to honour in French and German law and provided grounds for offences against personality.

According to Whitman, Brandeis and Warren were aware that continental laws could not be incorporated directly into America's laws due to the different common law and civil law traditions but, aware that privacy laws were not abundant in America,[253] they nonetheless suggested that affronts to personality, artistic feelings and sensibilities, like affronts and insults to one's honour on the continent, justified actions for injury to privacy. Tort law was the preferred forum, due to the growing reference in courts to emotional and moral harms.[254]

---

[250] Elizabeth Gaffin, Friending *Brandeis: Privacy And Government Surveillance In The Era Of Social Media*, MA Thesis, Naval Post-Graduate School (2008).
[251] Whitman, *supra* fn 228 at 1202.
[252] *Id.* at 1205.
[253] By 2004, according to James Q. Whitman, less than a third of American states had privacy laws (1203).
[254] Whitman, *supra* fn 228 at 1208.

Whitman's basic thesis is that American and European efforts to enact a transnational law of "privacy" is deeply hampered by the deep-routed differences in how privacy is perceived: in European culture it is based on a societal reverence for a person's dignity, closely tied to honour and addressed historically through the law of insult, while in America privacy's limits extend to one's liberty and the public right to know, as reinforced in the constitutional devotion to "life, liberty and the pursuit of happiness" and reflected in the common law and the First Amendment claims of free expression.

Whitman points out that the cultural difference can be seen in something as seemingly benign as the propensity of Americans to share trivial details of their private lives to complete strangers. He cites as example the Monica Lewinski affair wherein the most graphic details of then-American President Clinton's extra-marital sexual activities were front-page news. In Europe, such indiscretions by state leaders are treated as private and not open to media exposure, unless criminal behavior is alleged.[255]

A more recent example that underscores Euro-American cultural differences regarding the boundaries of private actions can be seen in the European reaction to the New York arrest of Dominique Strauss-Kahn for sexual assault on a Sofitel domestic worker.[256] Responding to the television coverage of his arrest in handcuffs and his parading in front of the press, Strauss-Kahn commented, "Beyond the fantastic - and therefore incorrect - nature of this story, this is a despicable affront to my private life and dignity".[257] To Strauss-Kahn, his reputation is tied into his dignity and honour, matters directly connected to his private life.

A journalist for *Le Nouvel Observateur*, Laurent Joffrin, comments on the added tension in France between a person's right to privacy and the public's right to know.[258] That right to privacy instills in journalists not just a passive obligation to avoid stories

---

[255] *Id.* at 1155.

[256] Dominique Strauss-Kahn was head of the 178-member International Monetary Fund, former Minister of the Economy under then-President Mitterrand and poised to announce his candidacy for the Presidency of France as leader of the Socialist Party. Although he was indicted by a grand jury, Strauss-Kahn's charges were later withdrawn due to the lack of credibility of the victim.

[257] *French writer details Strauss-Kahn Affair*, AGENCE FRENCH PRESSE-IN-PARIS (23 Feb. 2013), http://www.chinadaily.com.cn/cndy/2013-02/23/content_16250243.htm.

[258] Celestine Bohlen, *Drawing the Line on Privacy*, NYTIMES, Europe Ed. (15 Mar. 2013), http://www.nytimes.com/2013/03/16/world/europe/16iht-letter16.html

that intrude on one's privacy but an active responsibility to "protect people's private lives". Strauss-Kahn was targeted by the press, not because of his sexual indiscretion or even his alleged criminal intentions, but because his attitude toward sex and women "smacked of a kind of '*droit du seigneur*', a license for powerful men to have their way."[259] The line is crossed, Joffrin emphasizes, when an editor tells a journalist "to go investigate a private life." In America, by contrast, digging into the deepest recesses of a public figure's personal history for a story is just considered competent journalism.

In a similar vein, Whitman notes that Europeans perceive as crass and outspoken the propensity of Americans to speak openly about money: salaries, property values, business investments, to persons they have just met. The practice of reporting credit information of private citizens to credit agencies particularly rankles the European sense of propriety and privacy. Talking about money, and showing a willingness to reveal very intimate information to people on the first encounter, shows the reverence with which Americans hold rights of free speech and the primacy they award to free enterprise and the public's right to know, the latter usually with respect to public figures. And yet, Americans seem deeply offended by nudity on public beaches, a practice Europeans have taken for granted for generations. [260]

In his conclusions, Whitman summarizes that Europeans value personal dignity above all else, an intangible quality severely threatened by today's mass media, while Americans treasure liberty, threatened primarily by their government. Whitman cautions that those values are neither absolute nor mutually exclusive. Nothing prohibits safeguarding how we present ourselves while inhibiting the investigative and regulatory excesses of the state.

Concepts of privacy continue to differ on each side of the Atlantic, however: that might be because privacy law is the product of local anxieties and ideals. In America, those anxieties focus on the police and other authorities who are viewed as the enemies of personal liberty; in Europe, "they focus on the ambition to guarantee everyone's position in society, to guarantee everyone's honor", a fact about the Continent as true today as it was in the time of the French Revolution. Whitman cautions that, whatever position we support, we must urge jurists and lawmakers to move beyond the "shallow

[259] *Id.*
[260] Whitman, *supra* fn 228 at 1155.

intuitionism" of decrying every invasion of privacy as "evil or horrible". [261] In order for law to function *as law*, it must work to protect what social tradition tells it is worth safeguarding. That tradition simply does not recognize personal dignity in America nor anti-statism in Europe.

The Internet activity of citizens of both jurisdictions does not alter those basic values, but intensifies the opportunities for defying them through indiscriminate voyeurism. As Solove states:

> When it comes to gossip and rumor on the Internet, the culprit is ourselves. We're invading each other's privacy, and we're also even invading our own privacy by exposures of information we later regret. [262]

UCLA author Lawrence Friedman would agree that traditional patterns of communication and hierarchies of control are no longer. As early as 1999, he observed the passing of traditional societies, typified by European states, whose relationships were strongly *vertical* and whose identity was fixed by one's birth or social position.[263] In its place was what he saw as a "horizontal society" with flattened relationships between authority and the rest of society, and between the former titular and functional tiers in society. People were feeling freer to choose who they are and to form relationships on a plane of equality, choices that relate to the former identity determinants such as race, gender, ethnicity, and religion and that affect one's relations to politics, social structure, and the law. Over time, Friedman has noticed an intensification of that horizontal reshaping of traditional life due to the Internet and the social media networking it affords. As individuals now connect with like-minded others across barriers of space and time, claims Friedman, global mass culture is redefining community and replacing old loyalties and allegiances.

Similarly David Flaherty points out the linguistic complexity of thinking about privacy in the digital age and calls for a semantic distinction between privacy protection (a 'broad, all-encompassing concept that envelopes a whole range of human concerns) and data protection (a legal concern for our personal identifying data, such as birthdate,

---

[261] *Id.*
[262] Solove, Future, *supra* fn 97 at vii.
[263] LAWRENCE FRIEDMAN, THE HORIZONTAL SOCIETY, 45 (1999).

social insurance number, passport or credit card numbers, for example).[264] With respect to the latter, Flaherty has conducted a comprehensive study of five western democratic states regarding the efforts of public sector institutions to protect individual privacy from "the massive surveillance capacities of governments and corporations".[265] Countries were chosen for their leading approach to privacy protection. He concluded that, despite having the oldest national data protection laws, Sweden is the prototype of the surveillance state; Germany has the most effective national privacy laws of the five countries on the subject; Canada has the most developed system of data protection in North America while America's various privacy legislation is seen as practically toothless in protecting individuals from growing personal data collection.

Privacy, Flaherty concludes, is a major human concern and people want to be left alone with their secrets but, paradoxically, do not seem particularly vigilant in exercising due care to protect them. Throughout the 1990s, privacy activists grew increasingly concerned about the security of online transactional data available through web browsing, credit-card use and intelligent highways. Today privacy scholars are calling for a total reconsideration of the concept of privacy to reflect the increasing technological impossibility of closing down all online platforms to the peering eyes of corporations and the state in the name of enterprise or national security.[266]

The question of whether privacy matters anymore in the era of online image management is tackled by a new breed of media scholars, well-represented by former Microsoft researcher dana boyd. She has decided to test the limits of her networked world "where boundaries are not so coherently defined and where entities are not so easily articulated".[267] In a recent experiment, she provided a saliva sample for DNA analysis. A digital reading of boyd's DNA indicated some of her forebears probably had origins "distinct from the family narrative", that is, were secretly integrated into the

---

[264] David H. Flaherty, *Controlling Surveillance: Can Privacy Protection be made Effective?* In P.E. AGRE AND M. ROTENBERG (EDS), TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, xiii (1998).

[265] Included were France, Federal Republic of Germany, Sweden, Canada and the United States.

[266] For more on our move from pop culture to 'peep' culture *see* HAL NIEDZVIECKI, THE PEEP DIARIES (2009) (crediting our voyeuristic appetite with "baring all in the name of entertainment, self-betterment, and instantaneous recognition", for reinventing mass culture as a continuous peep show.)

[267] Dana boyd, *Debate: Networked Privacy*, SURV. & SOC., 348 (2013).

family tree and contributed to the familial gene pool through extra-marital, unacknowledged births. Biological indicators also told of disease probabilities that made family medical stories either inaccurate or "statistically curious".

In the process, boyd realized that her methodology compromised the privacy of a large contingent of her family. By subjecting her DNA to laboratory scrutiny, she had put not only herself under the microscope but the medical and other personal data of all members of her extended family including children she had yet to produce. As her biomedical data were part of the mega data aggregation that is archived within public data collections, she had unwittingly exposed people she had never met to the prying eyes of the curious. As boyd concluded, "[I]n doing so, I learned information about them that they may not wish to know and may not wish me to know".[268]

Boyd's DNA experiment shows the heightened networked character of our decisions and actions and the permanency of their results in the digital age. It illustrates that pre-Internet concepts of privacy belong irrevocably in the past. As boyd notes about personal links, "sometimes, as with DNA testing, we are linked by immu factors" while other connections are social or locational.[269]The latter suggests we have a choice in the matter, but boyd insists choices are long gone now that third parties can access, copy, transfer or otherwise manipulate our data. "Learning algorithms" or programs that carry out binary sorting without human prompting can collect and collate digital information about us that can predict our tastes, habits and decisions about friends and purchases and create our online personae. "How machines see us depends on how our data connects to others," boyd advises.[270]

Boyd warns that any model of privacy that depends on the individual's control of information will fail, because in current online environments users do not have enough information of online interconnectivity to decide which data should be shared with whom and when. Users also are aware that Internet companies like Google and Facebook have limitless ways to share data without our approval. As well, given the prevalence of data leakages and the architectural tendencies of the Internet to arbitrarily link one piece of datum with others, absolute control is not possible. It is as futile as trying to contain the poisonous ink from an octopus as it infuses surrounding

[268] *Id.* at 349.
[269] *Id.* at 348.
[270] *Id.*

waters. "Expecting that people can assert individual control when their lives are so interconnected is farcical," boyd asserts.[271] The DNA experiment shows how people who are not even born can be affected by online data creation. Social media is particularly vulnerable to unconsented sharing, profile creation and aggregated linkage of the sender with non-intended recipients.

Today's privacy can best be approached by stepping outside of our obsession with the individual as the appropriate unit of analysis in any privacy discussion. Of far greater import on the Internet are groups, communities, relationships and networks. According to boyd, only through the collective lens can we begin to model, and to advise, with whom we wish to share and to understand how to share without jeopardizing the privacy of others.[272]

Helen Nissenbaum of New York University agrees that the contours of our privacy rights in the digital age are quite different from what we have come to expect of our communications when offline.[273] She characterizes our new right to privacy neither as a right to control information nor a right to have its access restricted but the qualified right to have our expectations about the flow of information met. The issue is no longer should we share, because the architecture of the Internet and its governing algorithms dictate that sharing is inevitable. Nissenbaum tells us that the direction of sharing is guided by "key organizing principles of our social lives, including moral and political ones".[274] It will be guided, not by our static expectations of privacy, nor by societal norms, but by contextual norms. She invokes us to insist on "contextual integrity", the right to know in what context our data will be disseminated and re-sent, so that we can request correction when that context misrepresents our image or other personal data. She rejects the public/private divide of past times as a basis for what should be kept private; old standards of what should be categorized as "sensitive information demanding special consideration" have been swept aside by our need to share openly online.[275]

Nissenbaum's insistence on the critical importance of contextualization finds a

---

[271] *Id.* at 350.
[272] *Id.*
[273] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRATION OF SOCIAL LIFE (2009).
[274] *Id.*
[275] *Id.* at 232.

precursor in the 2001 debate on the relationship between privacy and context among Professors Robert C. Post, Lawrence Lessig and Jeffrey Rosen as sponsored by Georgetown University School of Law.[276] Both Post and Lessig propose that using another's private information out of context, and thereby misrepresenting some aspect of another person's character or personality, does not lead to an invasion of privacy, just a misunderstanding on the facts as presented. They suggest, as corrective, adding further information about the subject to enlarge the context and no harm is done. They give the example of a requirement by the United States Supreme Court that journalists who wish to cover trials must stay for the entirety of the trial so as not to misrepresent the narrative, the parties or witnesses by cherry-picking certain information for their publications.

Jeffrey Rosen counters that the only way to correct misrepresentation of another person through a public account based on private information is to provide *more* private information in order to create a broader context, to enlarge what the public knows about a person's life or circumstance.[277] In that way, the harm of the original exposure and misrepresentation is compounded by the addition of yet further information that the subject would prefer to keep private and that creates harm to that person's dignity and sense of autonomy. One's autonomy is involved because the subject is forced to lose control over another piece of his private life in order to set straight the mistaken perception created by the first revelation. In Rosen's words, privacy as autonomy presumes a "self-actualized individual self" as defined by its differences from, rather than its similarities to, the relevant community. The injury to privacy is thereby compounded by adding further context and that is contingent on more personal revelations.

Privacy, to Rosen, becomes the control of personal information we do not wish others to know. The violation to privacy is the involuntary wrenching of that information and dropping it into another context of information that might paint it in a more accurate light. That offends the subject's dignity, autonomy and wish to be understood.[278] Rosen defines autonomy as the private right to act outside of social norms. He gives the example of President Clinton's public display of infidelity while in office *via* the Monica Lewinsky affair. Had the Clintons been allowed to resolve the

[276] Jeffrey Rosen, *The Purposes of Privacy: A Response,* 89 GEO. L. J. 2117 (2001).
[277] *Id.* at 2121.
[278] *Id.* at 2118.

matter outside the public eye, any range of solution could have been exercised. The President's publicists insisted, however, on the production of a video of the Clintons dancing on a beach, in order to air the apparent resolve of the couple to work things out. In addition, Hillary Clinton was booked on talk show circuits to discuss her decision to stand by her husband. By playing out those choices in public, the Clintons were forced to discuss the possibility of divorce in order to satisfy the public that they were contemplating the normative solution to marital infidelity. A respect for their privacy would have allowed them to structure their most intimate relations out of the confines of social norms in a way that gave them autonomy over their reputations and public image.[279] Rosen argues that such exposure constitutes an offence against liberal freedom in that it does not respect public/private boundaries.[280]

Canadian surveillance researcher David Lyon of Queens University joins the conversation about changes to the public/private divide by agreeing with boyd's assertion that digital architecture is an uncompromising arbiter of how our online identities are identified. Lyon reminds us that the starting point must be our assumption that state and corporate surveillance is constant and all pervasive.[281] Data are aggregated, he explains, to compare populations, to sort people so they can be treated differently. State and corporate profiling is a given, in the name of free enterprise and national security. "So in a sense you are already a suspect," Professor Lyon said. He marvels that most people seem enthusiastic about submitting themselves to those surveillance regimes, from personal updates online to customer loyalty programs. "We're going through a cultural change," he notes, where "big surveillance is still there, but we need to be aware of our own responses and our participation in surveillance." He says further, "The social calculus is in flux…and the boundary between accep and intrusive surveillance is fluid and dynamic".[282]

---

[279] *Id.* at 2119.
[280] *Id.*
[280] *Id.* at 2120.
[281] David Lyon as quoted *in* J. Brean, *'You are already a suspect': Surveillance becoming 'routine' as it evolves into a social media pastime,* NAT. POST, (4 June 2013).
[282] *Id.*

Lyon also addresses what he calls the "fun surveillance" of social media, what Mann *et al.* saw as the more fanciful aim of sousveillance.[283] The surveillant opportunities afforded through the workings of social digital messaging can "domesticate" other more nefarious forms of state monitoring of its citizens that we might want to challenge on civil liberties grounds. We are thereby lulled, says Lyon, into that erroneous aphorism that we have nothing to hide and therefore nothing to fear. Lyon is critical of the blasé attitude many assume regarding government surveillance: "For many people…surveillance is at worst an annoyance that has to be negotiated," he says.[284] In the next section, we explore how a in very different culture, that in the People's Republic of China (PRC), individual Internet users are beginning to respond to the intensifying prying by the state into online activities.

2.4 Privacy as a Social Construct

If you don't want anyone to know, don't do it.[285]

A reputable text on Chinese architecture advises that concepts of privacy, or *yinsi*, have been part of discourse in China from the earliest recorded times to the present, with varying functions and values.[286] Such discourse has found little reflection, however, in the laws of China until very recently.[287] The term '*yinsi*' carries treasonous or criminal overtones, indicating undesirable behavior such as the harbouring of illicit secrets or selfish and conspiratorial actions. Such connotations suggest that the concept of privacy has long been suspect in China.[288]

In a practical comparison of Western and Chinese concepts of privacy, someone from the US or Europe might be offended at practices at Chinese public lavatories that

---

[283] Steve Mann *et al., Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments,* 1 SURV. & SOC. 1, 331-355 (2003), http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3344.
[284] *Id.*
[285] Chinese proverb as spoken by Eric Schmidt, *Google CEO Eric Schmidt on privacy,* YouTube, https://www.YouTube.com/watch?v=3tNpYpcU5s4.
[286] BONNIE S. MCDOUGALL & ANDERS HANSSON, EDS, CHINESE CONCEPTS OF PRIVACY (2002).
[287] The term 'China' is used herein to indicate the country in more general terms and as observed by external eyes: the 'PRC' connotes the political or economic entity.
[288] *The Long March to Privacy*, ECONOMIST (12 Jan. 2006), http://www.economist.com/node/5389362.

are "open-plan affairs" where locals unconsciously squat elbow-to-elbow. Similarly with Chinese hospital treatments that are carried out amid crowds of observers; people think nothing of asking strangers about myriad details from their incomes to their weight that in Western societies are perceived as no one's concern.

With rapid commercial and residential development and hence with the proliferation of intrusive employers, data-mining marketers and invasive surveillance cameras, modern China is witnessing invasion of privacy Western-style. Stories are legend of state use of Yahoo! and other Internet companies for censorship activities and for delivering up people sought for criticizing the state. US Internet company Google became aware of such state intrusion on individual Internet users in the PRC when Chinese officials requested the US company hand over information on individual social media communications; Google subsequently withdrew its holdings from the PRC to Hong Kong in April of 2010.[289]

State spying enjoys a long history in the PRC: when Communist leaders first came to power in 1949, they exercised limitless prying into civilian affairs. State intrusions that would never have been acceptable in the West were commonplace: for example, women of childbearing age had their menstrual cycles recorded by state authorities to monitor whether they were getting pregnant without state permission. This became particularly critical during implementation of the one-family-one-child state policy. More recently, police have come under particular regulatory scrutiny in cities like Nanjing where a municipal law requires that they report when they marry, divorce, travel outside the country, purchase a car or invest in property.[290]

The PRC also must deal with the socio-economic pressures of a population growth that outstrips all other countries in the world, challenging all aspects of state rule, from feeding its people to maintaining a probing eye on all citizen actions that reveal even a whiff of individual dissidence.[291] Massacres at Tiananmen Square signaled the winds of political dissidence in the PRC and its iconic message is not lost on privacy

---

[289] Miguel Helft, & David Barbosa, *Google Shuts China Site in Dispute over Censorship*, NYTIMES (22 Mar. 2010), http://www.nytimes.com/2010/03/23/technology/23google.html?_r=0.
[290] Long March, *supra* fn 288.
[291] The PRC population in 2012 was calculated at 1,316,562,729, including mainland China plus Hong Kong and Macau, excluding Taiwan, World Population View (2013), http://www.prb.org/Publications/Datasheets/2013/2013-world-population-data-sheet/world-map.aspx.

and human rights advocates around the rest of the world. Throughout its comparatively long history, the PRC has shown only brief interludes of open foreign policy that have afforded western eyes a glimpse of the intense authoritarian practices and iron rule of the PRC.

Chinese individuals increasingly express their concern that privacy rights enjoy only the flimsiest of legal protections in their country. Privacy is mentioned little in China's constitution, labour law or medical law, and the few provisions are vaguely worded and are all subject to the "notoriously arbitrary workings of the Chinese legal system". [292] Under government pressure, employers continue to monitor their employee's activities on the Internet and marketers document potential customers' buying preferences and credit ratings. In response, individual citizens are voicing their displeasure.

Surveillance is both an internal practice and a trans-state activity in China. In imitation of Britain's prodigious use of surveillance cameras, China is installing security and traffic-monitoring cameras on all its main streets. Most Beijing cameras have night-vision capabilities that can track speeding drivers and notify them of their infractions via text messages sent to their mobile phones. China's practice of hacking foreign computer systems was recently documented by surveillance scholar Ron Deibert, former director of University of Toronto's Citizen Lab. He conducted studies into the Stuxnet virus that crippled Iran's nuclear program and temporarily disabled State data collection functions in several countries including Canada.[293] Deibert traced the massive hacking activities to a location in rural China.[294]

Kenneth Farrell of the University of Pennsylvania's Communications faculty tackles the "dynamic interrelationship between American and Chinese cultural and legal approaches to privacy".[295] Global privacy, he insists, is under threat, but simply equating the English "privacy" with the Chinese *yinsi* restricts dialogue between the two

---

[292] Long March, *supra* fn 288.
[293] Ron Deibert, *The Growing Dark Side of Cyberspace (…and what to do about it)*, 1 PENN ST. J. L. & INTL. AFF. 260 (2012).
[294] Ron Deibert, Shadows In The Cloud: Investigating Cyber Espionage 2.0, Information Warfare Monitor and Shadow Server Foundation (2010) http://deibert.citizenlab.org/publications/.
[295] Kenneth Farrell, *Global Privacy in Flux: Illuminating Privacy across Cultures in China and the US*, 2 INTL J. COMM., 993-1030 (2008).

cultures.[296] Much more meaningful is to examine cross-cultural differences regarding individual expectations of privacy and discrepancies between the public/private divide.[297]

Differences in public/private concepts of privacy can be culturally determined as we see with semantics. For example, unlike the "public square" implications of the word *public* in English speaking cultures, the equivalent *gong* in Chinese refers to shared societal interests, a difference that might indicate a more shared privacy interest in the PRC.[298] Farrell cites the concern amongst Chinese citizens about unauthorized transference of their personal data to authorities and corporations, compounded with the worry about cell phone and Internet spam, as more conducive to fashioning national legal solutions than in America where "business interests have a more direct claim on politics".[299]

In summary, distinctions between perceptions of the public/private divide in the lives of individual Internet users in China and in America can be attributed to cultural expectations and societal conditioning. Despite the ready inclination among pre-Internet Chinese citizens to share what, in the western view, is very private information in public situations Farrell sees such communal openness waning as communications move online. Whether that observation can be linked to the accelerated growth of consumerism and private ownership, or to the growth in new media use, are questions that await further empirical studies.

In America, individual perceptions of privacy are changing as well. In a 2009 academic collaboration between political scientists at the University of Connecticut and the University of Rhode Island, public opinion about state intrusions on personal privacy since 1990 was surveyed and support was found to be in decline, despite a prominent surge around the 9/11 terrorist attacks.[300] Farrell believes there is room for a "common, abstract principle of privacy" that Chinese and American Internet users can

---

[296] On the challenges of comparative translations of terms such as 'privacy' and 'yinsi', Farrell notes, "It is certainly true that in terms of the broadest possible mapping of Chinese and Western inter-discursive structure, we can say that the translation for privacy is *yinsi*" (p. 995). He also reports, "concise definitions are elusive and ultimately impossible" (999).
[297] Farrell, *supra* fn 295 at 995.
[298] *Id.* at 1022.
[299] *Id.*
[300] S.J. Best, B.S. Krueger and J. Ladewig, *The Polls Trends: Privacy in the Information Age*, 70 PUB. OPIN. Q., 375, 377 (Fall 2006).

share, but it must continuously negotiate the tension in personal privacy versus the need for information. As more Chinese gain affluence and thus access to physical property, the possible expansion of an expectation of privacy to include that tangible space is very real. Americans, in contrast, have seen concepts of real space diminish as perceptions of virtual space grow in what Farrell describes as an "intensifying rupture" between territorial and informational privacy.[301]

2.5 Gaining Oblivion: The Right to be Forgotten

> Spirits they are, to whom second bodies are owed by Fate, and at the water of Lethe's stream they drink the soothing draught and long forgetfulness.[302]

In Virgil's mythical world set out in the Aeneid, souls of the dead are led through a cleansing of memories of the present world prior to their entry into the next. They readily drink of the waters of Lethe to wash clean the memory slate of past cares. In a striking example of life imitating art, the concept of forgetfulness has arisen in legal drafting circles as a solution to the alleged permanence of our digital footprints.[303] There is an emergent literature that debates the contours of a right to be forgotten and a corollary right to oblivion. The concept of a human right to disassociate oneself from past mistakes or misrepresentations can be seen as both "intuitive and appealing" in Europe;[304] so too in America, given that the possibility of second chances was an ethos from which the new nation was forged.[305] The legal form that forgetfulness will take, however, and its practical implications, are issues currently under vigorous debate by governments, Internet companies, and academics on both sides of the Atlantic.[306] Such

---

[301] *Id.* at 1023. Those observations tie into Whitman's comments *supra* fn 228.
[302] VIRGIL, AENEID, Book VI as trans. by H.R. Fairclough, at para 703, http://www.theoi.com/Text/VirgilAeneid6.html.
[303] *See further* Oscar Wilde, *The Decay of Lying,* INTENTIONS (1889) reproduced as an ebook by Gutenberg.org at http://www.gutenberg.org/ebooks/887 (proposing the anti-mimetic idea that life should imitate art, not the other way round).
[304] Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice'* 8 SCRIPTed, 229-256 (2011), http://dx.doi.org/10.2139/ssrn.1986719.
[305] Friedman, *supra* fn 96 at 1921.
[306] In this section 'forgetfulness' is used to collectively signify the right to be forgotten, the right to forget, the right to oblivion, the right to erasure, and *le droit a l'oubli*. Such use reflects the debate in English that focuses on the EUDR preparations.

activity has been spurred by the proposal to update existing European law on data retention practices in light of the emergence of the Internet and other new media. Those revisions are highlighting the differences in US and EU concepts of privacy and free speech and their interaction, particularly online. Any meeting of the minds promises to have profound consequences on the American participation in the digital economy and, on the individual level, on the reputational risks to which we are exposed when online. I will now outline the conceptual background of forgetfulness and then detail its practical application and criticisms.

The French concept *droit à l'oubli* has a longer history than its English counterpart,[307] as does the Italian notion of reinventing oneself or *il diritto all'oblio*. At its most basic, forgetfulness allows us to revise our past in light of present knowledge or perceptions. Promotion of the concept of forgetfulness appeared in law and technology literature as far back as the 1990s in what David Flaherty called "one of the admirable products of European thinking and lawmaking".[308] Those who write of Internet regulation, however, are not in accord as to whether forgetfulness should be a "right, interest or value".[309] The conceptual distinctions between the 'right to be forgotten' and the 'right of oblivion' have also not been clarified nor related to the right of personality or the right of reputation. Pere Simon Castellano suggests the important distinction that will influence any law of forgetfulness is that Europeans tie the right to the issue of consent to use one's personal data while Americans focus on the societal entitlement to second chances.[310] Nor does there even appear to be a satisfactory English translation of *le droit à l'oubli*.[311] Ausloos suggests that the French term encompasses both forgetting and oblivion into the notion of 'forgetfulness'. In summary, it is not clear whether any of the foregoing concepts exist in law (*de lege lata*) or whether they are best debated as a future right (*de lege ferenda* or the law as it should/could be).[312]

The debate about the legal status of the right to be forgotten and the right to

[307] The debate in English, focused on the EUDR preparations, also uses terms such as the right of erasure, the right to delete, and the right to forget.
[308] Flaherty, *supra* fn 264.
[309] Robert Kirk Walker, *Note: The Right to be Forgotten"* 64 HAST. L. J. 257 (2012).
[310] Pere Simon Castellano, *The Right to be Forgotten under European law: a Constitutional Debate*' 6 LEX ELECTRONICA, 1 (2012).
[311] Fleischer, *supra* fn 189.
[312] Jeff Ausloos, *The Right to be Forgotten - Worth Remembering?* 28 CLSR, 143-152.

oblivion is quite active, driven perhaps by a considerable lack of legal clarity around the concepts. Is it a natural right, inchoate but recognized, or a legitimate interest, an ethical aim or social value[313] or a virtue or policy objective? All that is certain is that the concept has not crystallized as a generally accepted legal principle in either the American or the European legal tradition.[314]

As early as 1972 and long before the introduction of the PC, Alan Westin and Michael Baker of the University of Michigan recognized that the American value of allowing a fresh start was under siege because of the immense and accelerating storage capacities of computers.[315] They observed that anyone seeking to reform their lives for "religious, humanistic and psychiatric" reasons would be "barred by their past mistakes" because of the indelible memory of computers.[316] "The computer is assumed not to lose records," they observed, "to forward them efficiently to new places and organizations" and to "create an appetite in organizations for historically complete records."[317] It is those organizations' voracious appetite for our personal facts, then, and their institutional preference to "preserve and evaluate" that poses the major threat to any forgiveness principle.[318] In hindsight, as became clear in the analysis of the intelligence failure around the 9/11 terrorist attacks, the evaluation or analysis function fell victim to the sheer bulk of preserved data by the NSA and other authorities.

In a 1998 policy paper on forgetfulness, American science and technology scholars Jean-Francois Blanchette and Deborah Johnson presented the issue as one involving the obligation of the state to deliver social goods.[319] They identified the principal social goods that needed balancing against individual rights of privacy as the efficiency that computerized data collection brought to law enforcement, government service, and national security. Blanchette and Johnson conclude there is a general consensus in America that "too little is being done to stop the onslaught of personal

---

[313] Martin Dodge, & Robert Kitchin, *Code, objects and home spaces*, 41 ENVIRONMENT AND PLANNING 41, 1344-1365.
[314] The Martin case from Connecticut, as examined in Ch 3.3, provides an exception to that general trend.
[315] ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY (1972).
[316] *Id.* at 267.
[317] *Id.*
[318] *Id. at* 268.
[319] Jean-Francois Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 4 ACM Policy '98 Conference, London School of Economics.

data collection" and that privacy protection policy has been *ad hoc* and piecemeal. It is the act of retention, not the ubiquity of surveillance, they worry about, the social implications of a lack of institutional forgetfulness. They note that if a cost benefit analysis were conducted of personal privacy versus national security, institutional needs, law enforcement or government efficiency, privacy would be the loser.[320]

Police scholar Gary Marx takes a more cultural-historical perspective. He has noted that 'starting over' or moving to a new frontier is a powerful concept in American culture, given the history of the nation's founding.[321] "The beliefs that once a debt has been paid to society it is forgotten and that people can change are important American traditions." [322] He worries that surveillance information obtained via computers transcends time in that "it is available for analysis many years after the fact, and in totally different interpretive contexts."[323] With the "mass of easily accessible files, one's past is always present" and that undesirable permanence applies to erroneous or sabotaged data, as well as debts that have been paid.[324] Marx warns that such hoarding of data can create a class of permanently stigmatized persons within society.

The practical urgency in understanding the precise parameters of the forgetfulness right is that, as Jeffrey Rosen warns,

> Unless the right is defined more precisely when it is promulgated over the next year or so, it could precipitate a dramatic clash between European and American conceptions of the proper balance between privacy and free speech, leading to a far less open Internet.[325]

Georgetown University Professor of Law Franz Werro perhaps comes closest to linking forgetfulness with reputation when he considers such a right to be encompassed within the more general right to personality, to demand the erasure of archived data by authorities once they are not longer of legitimate use in order to "keep their activity trails private".[326]

---

[320] *Id.*
[321] GARY MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (1988).
[322] *Id* at 223.
[323] Gary Marx, *The Iron Fist and the Velvet Glove: Totalitarian potential within democratic structures. In* J.F. SHORT (ED.) THE SOCIAL FABRIC: DIMENSIONS AND ISSUES, 135 -161.
[324] *Id.*
[325] Jeffrey Rosen, Forgetting, *supra* fn 172.
[326] Franz Werro *The Right to Inform Versus the Right to be Forgotten: A TransAtlantic Clash,* in A. C. CIACCI, *ET AL.,* (EDS) HAFTUNGSRECHT IM DRITTEN MILLENNIUM (LIABILITY IN THE THIRD MILLENNIUM), (2009).

In terms of the individual user and forgetfulness, authorities in the European Information Commissioner's Office (ICO) worry that privacy advocates' promotion of the concept creates unrealistic expectations in the public of revisionist possibilities. [327] Instead, suggests the ICO, the focus should be on the 'right to object' to how personal data is used, as that emphasis would place the onus on the collector, primarily the corporate and security sectors, to justify their collection and transfer policies regarding citizens' data:

> It is a reversal of the burden of proof system used in the existing process. It will strengthen the person's position but it won't stop people processing their data.[328]

A further objection of the ICO is that the right to be forgotten is currently unworkable given disagreement from one country to the next on how to define *sensitive* personal data, a term used in explanatory literature accompanying the proposed EUDR text.[329] In the area of collective memory, there exists some resistance to revisionism as well.[330]

The interest in forgetfulness has proven to have more currency in Europe than in America, perhaps because "Europeans concede more than Americans to the public realm and look to the state to secure more of their rights and liberties".[331] For example, in a 2004 selection of civil service personnel in Greece, the country's Data Protection Authority recommended to the national selection committee that only the names of successful candidates for appointment to public service positions be publicized, not the names or details of those who were rejected.[332] Specifically, the Authority reasoned that it would be disproportionate to the aim of government transparency to publish exam failures that could come to public notice by pure chance. In addition, the Authority has

---

[327] Alastair Stevenson, *Right to be Forgotten on the web unworkable, argue data watchdogs*, V3.Co.Uk (26 Mar. 2013), http://www.v3.co.uk/v3-uk/news/2257523/right-to-be-forgotten-unworkable-argue-data-watchdogs. ICO officers are government regulators for freedom of information and oversight regarding the protection of personal data. The office often functions as a specialist ombudsman service.
[328] *Id.*
[329] Schwartz & Solove, The PII Problem, *supra* fn 7.
[330] William Dutton, *Programming to Forget*, Review *of* Delete: The Virtue Of Forgetting In The Digital Age By Viktor Mayer-Schonberger, 327 SCIENCE (19 Mar. 2010) 1456.
[331] AUSTIN SARAT, *ET AL.*, (EDS), IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY, Introduction (2012) 10-11.
[332] Greek Data Protection Authority Decision No. 62/2004.

generally recommended a time restriction on the publication via Internet of unfavourable administrative acts such as demotions, suspensions and dismissals.[333]

Another example is the decision by French courts to anonymize their published decisions by deleting reference to the parties and other personally identifying information before it is made public. The CNIL, as oversight authority,[334] has also invoked the violation of the right to be forgotten in the inclusion of litigant's names on a webpage available to the public[335] as well as dissemination of litigants' identification via publicly available legal databases.[336]

The enthusiasm in Europe over the EUDR, and the equally vocal opposition expressed by American observers, (as will be developed further in Chapter V *infra)* indicates that deep-seated cultural differences could delay any meeting of the minds.. Adding to that potential impasse is the paradoxical relationship presented in the twenty-first century between privacy and publicity. In the last century, "the golden age of public relations", publicity and engaging the attention of the press came to be something that many private citizens sought out and even paid for.[337] This has led in present times to an American culture obsessed, at once, with being seen and being hidden, "a world in which the only thing more cherished than privacy is publicity."[338]

Further to certain public policy concerns, forgetfulness is considered not only acceptable and socially useful, but necessary. The prospect of having a criminal record for life provides one example. European criminal law and regulations provide for the erasure or at least a public ban on access to records of minor offences through the regime of pardons. Similarly, American criminal records for youth are routinely abbreviated and accessible only to government officials in some states. In certain EU Member States, such as Germany and France, criminal records are automatically removed from the public record after a pre-set length of time and remain unavailable to prospective employers and credit rating agencies so as not to taint their future

[333] Greek Data Protection Authority Decision No. 1/2010.
[334] The National Commission of Informatics and Freedom (CNIL), the state authority in charge of protecting personal data and citizen privacy.
[335] Decision No. 2011/238.
[336] Decision No. 2001/057.
[337] Jill Lepore, *The Prism: Privacy in an age of publicity*, NEW YORKER (24 June 2013) 32, 36.
[338] *Id.*

success.[339] The rationale is that minor or youthful mistakes should not interfere with one's social and professional opportunities. It offers an escape from "the persecution of the past".[340]

The right to oblivion, in contrast, is known within data retention practices as tied to unwarranted data retention. Conceptually it does not differ from the French *le droit a l'oubli*, according to University of East Anglia Professor Paul Bernal; it relates to the right to silence on past events in life that are not longer occurring, primarily in the criminal sanction context.[341] It is mainstream media, in Bernal's view, that has added a more alarmist interpretation involving historical revisionism, Internet censorship, and the suppression of free speech. The real evil that legislative mechanisms are meant to address is the languishing online of digital evidence of who we are and where we navigate; that information is of immense value to hackers, over-zealous bureaucrats, and others of indifferent or adverse interests.[342] Bernal illustrates how easily such data is accessed: he cites the 2011 mining by a PhD student of personal information of 35 million Google users from its databases, including names, email addresses and biographical details. The mining did not break any of Google's posted rules and was assessed by the student as "completely trivial" in terms of the technological skill required.[343] Shortly thereafter, Google introduced a social networking platform that turns users into gleaners of friends' personal information and compilers of such profiles, all in the search for social "circles" and without the illegal hacking implications.[344]

In light of the unwitting and seemingly benign 'outing' by new media users in search of social connection, the distinctions between various types of forgetfulness fade in significance. More pressing are current hurdles to protection of the individual user:

---

[339] Hans Graux *et al., The Right to be Forgotten in the Internet Era,* ICRI Research Paper No. 11 (2012), http://ssrn.com/abstract=2174896.
[340] Castellano, *supra* fn 310 at 1.
[341] Paul A. Bernal, *A Right To Delete?* 2 EUR. J. L. & TECH. (2011), http://ejlt.org/artiview/75/144.
[342] Zittrain's term for forgetfulness is 'reputation bankruptcy': (Future of Internet, *supra* fn 36 at 228ff); *see further* Rosen, Forgetting, *supra* fn 172; John Hendel, *Why Journalists Shouldn't Fear Europe's 'Right to be Forgotten'",* ATLANTIC (25 Jan. 2012), http://www.theAtlantic.com/technology.archive/2012/01/.
[343] *Id.*
[344] Alexei Oreskovic, *First Look at the Google+ social network: The Top Secret Demo,* REUTERS (28 June 20111), http://blogs.reuters.com/mediafile/2011/06/28/first-look-at-the-google-plus-social-network-the-top-secret-demo/.

the practicalities of acquiring consent, detecting misuse, and enforcing workable privacy standards.

The concept of forgetfulness has some detractors and William Dutton of Oxford University's Oxford Internet Institute expresses the most frequently voiced objections: that "erasing history is not only Orwellian and unfeasible, given the scale of the web, but it will have a chilling effect on freedom of expression," legitimizing government's role in censorship in liberal democratic societies.[345] It will also create a "legal swamp" in the privacy and data protection area that is already fraught with uncertainties. Dutton argues that privacy and data laws already cover any abuse of personal privacy that is the target of right to be forgotten rules. In Dutton's words:

> [Y]ou are asking for a right to purge a service of all information they [service providers] might hold about you. I don't think this policy would or should reach so far.[346]

In practical terms, debates over the nuanced meanings and historical referents of a right to be forgotten have cast a shadow of uncertainty that extends over more altruistic digital activities such as data conservation and digitization projects. Its practical significance to memory and reputation will expand as the EUDR enters force and implements a right to *erasure*, as will be discussed further in Chapter 5.2. The need for forgetfulness to protect reputation and status could become increasingly undermined by the tyranny of online architecture that enables some of the more invasive misuses of the online environment as I discuss next.

[345] William H. Dutton, *The EU's Right to be Forgotten and Why it is Wrong*, OII Online, (2010) http://billdutton.me/2013/04/05/the-eus-right-to-be-forgotten-and-why-it-is-wrong/ .
[346] *Id.*

CHAPTER 3 THE TECHNOLOGY AND SCOPE OF REPUTATIONAL HARM

3.0 Introduction

In this section I examine how our reputations are damaged online – the inner workings of the Internet and the Web that make reputational damage possible. I first consider the idiosyncratic features of new media that achieve the type of harms I will further describe, with legal responses, in chapter 4. Next I canvass various actions, by ourselves and by third parties, that compromise our reputational privacy. I organize those actions into *exposure* harms (involving online personal content) and *disclosure* harms (representing non-consensual data collection and dissemination). This section concludes with two cases, the Mosley case tried in various EU member state jurisdictions and the Martin case in the US. Those cases illustrate the discrepancies between a plaintiff's expectations that extant laws will restore lost status and the legal and personal-life repercussions that fall short of those goals. I incorporate into those considerations a discussion of whether digital speech is a profoundly different method of communication online than off, warranting a different legal or other response as explored in Chapter V.

3.1 Technological Idiosyncrasies of Digital Media

a Reconfiguring of Information Bits

Digital information is aspatial and hence easily transported. That is why material that is stored on a computer on the other side of the world can be accessed as easily as material located next door. Digital information is divided into packets of binary digits ('0's and '1's in computer code) known as 'bits'; packets comprise the smallest unit of transfer, which are disseminated in any order and recombined at the receiving end. That system of transmission facilitates a much speedier conveyance of message than the analogue system that must be sent and received in the same sequence of information. Transmission can also be described as non-rivalrous, meaning that its consumption by one person does not diminish the possibility of its subsequent (or simultaneous) use by

others.[347] Digital transmission also provides easier access to the individual user; one way to measure the effort that we expend to access information on the Internet is to consider its 'ontological friction' or the forces that create resistance to information flow.[348] Analogue means of transmission involves a much higher ontological friction than that for digital information. It has been argued that easier access through a lower ontological friction means increased risks to personal privacy.[349]

As each packet travels through the network, it passes through a series of specialized computers or 'routers' that determine the most direct path for the packet to travel from sender to receiver. Routers must make a copy of each packet in order to read and direct it. The life-span of these copies is limited to a fraction of a second. When we search information, we enter search words into a search engine, such as Google, Yahoo! or Mozilla Firefox. Those Internet service providers (ISPs) have an allocated website with a domain name, such as <http://images.google.ca> that serves as the entry point to information stored on Google as contained on the World Wide Web (www).[350] The Domain name is an alias for a number which is what the computer uses to find the location of the website, such as <www.1acc.com = 207.159.89.66>. Once the website has a domain name it can then be accessed by any user on the World Wide Web (www).

In theory, search results are non-discriminatory: any user should be able to enter the domain name above, type in a search word or phrase, and receive the same search listings in the same order as any other user who enters those search words. The search engine even autocompletes partial entries and suggests the highest-ranked responses to those search words, even those we have not anticipated. Through auto-correction and search order a serendipity factor is introduced into online searches that expand our bank of desired information. Such autonomous architectural features can

---

[347] Michalis Vafopolous, *Being, space, and time on the Web.* 43 METAPHILOSOPHY, 405-425 (2012).
[348] Luciano Floridi, *The Ontological Interpretation of Informational Privacy*, 7 ETH. & INF. TECH. 185 (2005).
[349] *Id.* at 186.
[350] Domain names are used to identify one or more IP addresses. For example, the domain name *85uqueэne85.com* represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL *http://www.pcwebopedia.com/index.html,* the domain name is *pcwebopedia.com. See further* 'Domain Name', Webopedia, http://www.webopedia.com/TERM/D/domain_name.html.

have dire consequences, however, for individuals who are misrepresented in web searches, as will be discussed further under Chapters 3 and 4.[351]

Access is augmented within the digital world for audio and video information stored online because it can be stored in greatly compressed files on a user's hard drive. When using file-sharing hardware such as Napster or Netflix, an audio or video file can be 'virally' shared with unlimited users within seconds.[352] Once downloaded, those files can be 'burned' onto blank CDs or DVDs for offline use, for redistribution, or illegal sale. Unlike real time sales, digital products can be offered in a wider selection because storage is cheaper and of much increased capacity than when dealing with physical storage space in the offline world. Content can be kept temporarily or permanently, or be accessed when the user is mobile through mobile devices or por flash drives (USB keys) to be accessed through other devices, either wired or wireless. Users may also choose to stream audio or video offerings without storing them at all. Streaming services can also be interactive, allowing the receiver to choose which audio or video streams she wishes. All of those affordances illustrate the growing ease of distribution of content from one source to many, a key factor in the dissemination of prejudicial, secret, or defamatory content. In that way, the same technologies that enable wide accumulation, access, and distribution are the ones that service the viral dissemination of content the data subject would find objectionable.

With the amount of traffic generated by steady growth in Internet use worldwide,[353] network breakdown is avoided through the technique of 'caching' or the automatic storage of material searched by a user.[354] When a user first accesses a webpage offered by a server, key elements of that page are retained and more easily

---

[351] Ch. 3 under Lingering Data, Autocorrection, and the Power of Internet Companies, and Ch. 4 under ISP Liability.

[352] Michael A. Einhorn, *Bits, Bots, and Crackups: Life on the Information Superhighway'*, (11 Oct. 2002), http://ssrn.com/abstract=332700. Stored bits must be converted from digital to analogue signals before they can be heard through speakers.

[353] Almost 3 billion users by the end of 2014, according to the United Nations ITU: the number of mobile phone users will reach almost 7 billion within the same time span. *See further Number of Internet Users Worldwide Approaching 3 Billion*, Voice Of America News (6 May 2014) http://www.voanews.com/content/number-of-internet-users-worldwide-approaching-3-billion/1908968.html.

[354] This paragraph is informed by *Internet Technology Explained: Hosting, Caching, and Mirroring,* Eurim.org.uk Background Paper How Data is transmitted over the Internet, Network Governance Working Party, https://www.yumpu.com/en/document/view/34086341/how-data-is-transmitted-over-the-internet-eurim.

produced the next time the user requests the same information. On the second try, it is not necessary to transmit the data packets all the way from the original hosting computer, and very little demand is placed therefore on capacity in the core network. Caching can be managed through the use of metatags, inserted into a document's URL[355] that describe its attributes and which can create a set of instructions for a search engine or Web server on retrieving the desired content. Meta tags can also be used to mark a document as uncache-able, so that a web server will not save or archive the document, or will cache it for a specified period of time, so it is not used when it is too old. It has been suggested that Internet companies could meet obligations under the EUDR principle of the right to be forgotten through expiry dates set on cached data.[356] Generally, data subjects should have concern over online data that has been 'de-contextualized, distorted, outdated, no longer truthful (but not necessarily false)'.[357]

b Cloud Storage, Anonymity, and Attribution

Digital data is capable of cloud computing, a concept with three components: storage on a location independent of the device from which it is generated; sharing of that storage as a fungible resource[358] with other customers; and charging for access based on resources used.[359] Responding to user demand often involves an overlay of those services, a process not always known to that user. For example, a user might subscribe to the data storage services of Dropbox that, behind the scenes, uses Amazon's infrastructure or those of other commercial service providers. The user herself might combine services, such as when involved in analytics monitoring or cloud-

[355] A URL (Uniform Resource Locator) indicates the location of a file on the web. When you type the address of a web page into your browser, you are typing a URL, such as <http://www.eurim.org.uk/activities/netgov/9911paperinternettech.pdf> used to retrieve the article in the previous footnote (339).
[356] Mayer-Schonberger, *supra* fn 161.
[357] Norberto Nuno Gomes de Andrade, *Oblivion: the Right to be Different from Oneself', Reproposing the Right to Be Forgotten*, in VII International Conference on Internet, Law & Politics, Net Neutrality and other challenges for the future of the Internet, 13 Revista De Internet, Derecho Y Politica, 122, 127.
[358] Goods or elements are fungible when they are capable of being substituted for another.
[359] *See generally* Kuan Hon *et al., The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated?* Cloud Legal Project Paper, Centre for Commercial Law Studies, University of London (2011).

based billing, creating an integration of systems that shows the growing interconnectivity of cloud services. The precise nature of services becomes critical when attempting to define a 'controller' of digital data, as required by both US legislation on data protection and the EUDR.

There are three general types of data that might be involved in cloud computing: anonymized and pseudonymized data, encrypted data, and sharded or fragmented data. Those distinctions will be considered in turn as they are important in determining whether data should be treated in law as 'personal data'.[360]

i Anonymity and Attribution

There are two principal ways in which a user can be identified: through her IP address[361] and through her digital search history. Here is how it is done: a user enters search terms into an Internet search engine, such as Google. The query terms are logged or tracked by the search engine. The log data also includes such items as the type and version of web browser of the user, her IP address, and other information gleaned by cookies that are inserted each time the user conducts a search. That information routinely includes an ID for the computer, the date and time and duration of each site visit, the path to and from the site, the time spent on each page, and the links that are clicked during each visit.[362] Cookies retain that information about previous searches for speedier access each subsequent visit. That information can be combined with other fragments of personally identifying data to arrive at a more accurate profile of the user. Anonymization removes information obtained from cookies as well as from the IP address.

Anonymizing and pseudonymizing processes conceal the data subject's identity. To anonymize a person's identity is to remove sufficient identifiers so that identification

---

[360] *Id.* at 8.

[361] IP address, or Internet Protocol address, is a computer acronym for a set of rules or standards that are used by computers to communicate with each other across a network, such as the Internet. Computer protocols govern the standards used to enable the connection, communication and data transfer. Each computer has a distinct IP address. *See further What does IP address stand for?* English Language Terminology, http://www.englishlanguageterminology.org/acronyms-initials-abbreviations/what-does-ip-stand-for.htm.

[362] Nichoel Forrett, *Cookie Monster: Balancing Internet Privacy with Commerce, Technology and Terrorism*, 20 TOURO L. REV. (2004), http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=1749&context=lawreview

is not possible through discrete bits of information. To pseudonymize an identity is to substitute one ingredient - a name, for instance - with numbers or other characters that can deflect direct identification. Identities are disguised, therefore, not removed. That process is of particular interest to researchers and statisticians, as they are able to collect different information relating to the same individual without having to know her name, thereby complying with privacy laws.

Those processes are conducted before data is stored or otherwise dealt with in the cloud. Data is frequently anonymized or pseudonymized before sharing or selling it to another entity, although much personal data sold to commercial advertisers do not go through such preliminaries. For example, some US companies that sell health related data would anonymize or pseudonymize such personal data prior to selling it to research companies, but others would not. In another example, the EU company HipSnip enables mobile phone users to 'snip' and save offers from consumer product brands, a process that permits owners of those products to trace the consumer due to a lack of anonymizing activity.[363] Often only part of the data is altered or deleted, however, and only some identifiers are disguised or altered by cryptography. Other information, such as a usage trail or test results associated with a name are left intact, a matter of concern to privacy advocates and policymakers. The degree of anonymizing and pseudonymizing becomes a critical factor in determining what is 'personal data', 'personally identified information', or 'personally identifiable information' when constructing privacy or data protection legislation. Those definitions, and hence the type of data that is regulated, differ from one country to the next, a matter of grave concern to privacy scholars like Paul Schwartz and Daniel Solove.[364]

Technology that enables deanonymization, or the reversal of the anonymization and pseudonymization process, is now readily available. That reality has mobilized legislative efforts at data protection. De-anonymization is achieved by assigning sufficient identifiers (numbers or other symbols) that disclosure of an individual is achieved. Identifiers can also be comprised of different pieces of information about a person which, when taken individually, would not lead to her identification. So removing direct identifiers, (such as names, email addresses, IP addresses, or medical

[363] *Id.* at 9. HipSnip's terms of service permit it to 'share, rent, sell, or trade aggregated or anonymized data.' *See* HipSnip's *Legal Statement at* https://angel.co/hipsnip.
[364] Schwartz & Solove, The PII Problem, *supra* fn 7.

device identifiers) might not achieve complete anonymity if indirect identifiers can be collected that, in the aggregate, lead back to identification.

The concept of attribution is simply the determination of user actions online as can be traced to that user. Anonymity and pseudonymity would be used, therefore, to escape our attribution by a third party. Our vulnerability to invasive technology at the hands of the state is accelerating at an alarming pace in the digital era. Through use of deanonymizing technology and the combination of seemingly discrete bits of information,[365] data analysts can pierce the public/private divide we believe we enjoy as citizens of a democratic state. For example, we have been told that our gender and sexual preferences can now be ascertained from a mere examination of our use of the 'like' function on Facebook.[366] Similarly we have been alerted that we are only four mobile phone conversations away from government identification.[367]

ii Encoding, Encryption, and Hashing

The principal function of encoding, encryption and hashing is to transform data into another format. The first two methods are reversible; hashing is not.[368] A user would encode data to ensure its consumption, in a proper and safe format, by a different type of system.[369] The algorithm used is publicly available, so secrecy is not the objective. For example, if you are trying to submit your curriculum vitae in application for a job and the intended recipient asks for the document in ASCII, he is asking for plain text without formatting such as pre-set tabs, bolding, or italics, in order to

---

[365] Daniel J. Solove, *Justice Scalia's Dossier: Interesting Issues about Privacy and Ethics,"* CONCURRING OPINIONS (29 Apr. 2009) http://www.concurringopinions.com/archives/2009/04/justice_scalias_2.html.

[366] Rebecca J. Rosen, *Armed with Facebook 'Likes" Alone, Researchers Can tell Your Race Gender and Sexual Orientation,* ATLANTIC (12 Mar. 2013) http://www.theAtlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-and-sexual-orientation/273963/.

[367] Matt Warman, *Online anonymity: impossible after four phone calls,* TELEGRAPH (25 Mar. 2013), http://www.telegraph.co.uk/technology/news/9952841/Online-anonymity-impossible-after-four-phone-calls.html.

[368]Paulan Korenhoff, *Forgetting in Bits and Pieces: an exploration of the 'right to be forgotten' as implementation of 'forgetting' in online memory processes,* Tilburg Institute For Law, Technology, And Society Working Paper No. 4/2013, 5, Http://Www.Ssrn.Com/Abstract=2326475. *See generally,* Alan Baddeley *et al.,* Memory (2009).

[369] Daniel Miessler, *The Difference Between Encoding, Encryption and Hashing,* Daniel Miessler Blog, https://danielmiessler.com/study/encoding_encryption_hashing/.

smoothly facilitate importing your information into his applications. Encoding does not, as a rule, involve privacy issues and hence does not pose a risk to personal content or reputation.

Encryption, on the other hand, strives for secrecy. Encrypted messages can only be accessed via a de-encryption key and involves the transforming or converting of an entire data set in order to keep it secure from unwanted access. It is achieved by applying an algorithm to the data, which functions as a 'foreign language' that remains inaccessible to those who do not speak that language. The popularity of the BlackBerry mobile phone, for example, particularly within political and corporate sectors, was due in large part to the encryption system that was sourced offshore. Only designated recipients with the de-encryption key could return a message to plaintext. Blowfish is an example of an encryption cipher, available in the public domain; the Advanced Encryption Standard (AES) is another. Encryption malfunctions pose a serious risk to data security and, hence, to reputation.

Hashing is a system that allows detection of any tampering with the integrity of your data. In order to establish that data has not been modified, methods are used to compare data input with data output. The sender performs a 'hash' function by taking a group of characters and mapping it to a value of a certain length, called a 'hash value' that represents that string of characters. The intended recipient uses the same hash function to generate the hash value and compares that to the one received with the message.[370] Hashing is critical in detecting efforts at identity theft, hacking, and nonconsensual surveillance. On an individual level, hashing names or passwords can make theft of passwords more difficult, even for users who employ weak or identical same passwords for several accounts. While the process will not render their database or website any more secure, it offers some damage control in the event of a security breach.

iii Sharded or Fragmented Data

Those terms refer to an automated procedure of breaking up data into fragments for storage in different storage facilities or locations. The procedures depend on the

[370] *What is Hash Function*? Technopedia, http://www.techopedia.com/definition/19744/hash-function.

storage provider's sharding policies; cloud storage providers can usually meet requests for storage within a desired geographic area, such as within continental Europe.[371] Kuan Hon *et al.* raise an issue of interpretation that is critical to the EUDR: if unencrypted data uploaded to the cloud is automatically sharded for distributed storage, can a cloud user who accesses or uploads the personal data, and who might run applications in the cloud that operate on, and change that data, be considered a 'processor' of personal data. The EUDR potentially imposes strict accountability on that user-producer regarding the protection and retention of that data.[372]

c Geo-location and Other Surveillance Capabilities

Keeping in mind that the focus of this dissertation is the individual Internet user and her reputational privacy, I include this section on state surveillance methods to review ways the state can collect and use personal data that creates privacy risks for the individual.

Many of our digitized devices have built-in geo-location mechanisms that autonomously map our usage through the location of our devices. Those capabilities allow benign uses such as device location when we have misplaced our mobile phones or ts, or mapping services to direct our travels from one physical location to another. They also, however, form part of a larger data collection program by state authorities under the rubric of national security. It is known, for example, that since 2011 Apple iPhones and iPads routinely record the position of our devices and save the data in individual files at Apple Inc. storage facilities for the growing circumstances that allow warrantless searches by government.[373] Such accessibility has privacy and personal security implications, as that data is apparently unencrypted and hence unprotected from third party access. That digital disclosure extends to any device with which we synchronize our mobile phones, such as our laptop computers or t devices.

While it is beyond the scope of this dissertation to explore the political agenda behind such activities, we will provide a brief description regarding US government

[371] Kuan Hon, *supra* fn 359 at 11.
[372] *Id.* at 31.
[373] Alasdair Allan & Pete Warden, *Got an iPhone or 3G iPad? Apple is recording your moves'*, O'Reilly Radar Blog (20 Apr. 2011), http://radar.oreilly.com/2011/04/apple-location-tracking.html

surveillance and identification practices involving our digital device communications that has an impact on access to our personal data.

Historically, state surveillance has been concerned with "ascertaining and using" specific information about targeted individuals who are of political or criminal menace to public order or safety.[374] State authorities accomplish that by watching us, through human agents and digital monitoring of our "data doubles", created via the mandatory disclosure of such personal information as our banking activities or use of government services. With the expansion of national security agenda in western states leading up to the new millennium, as expanded by the need for a formalized internal and foreign policy response to the Twin Towers attacks in 2001, governments in the US and EU have taken unprecedented steps to monitor, identify, and profile users of digital communications. That security net has scooped up not only foreign communications transmitted to the US but, within the continental US, communications between and among American citizens. How is that technically accomplished?

Since 2005, the US government has required major telecommunication companies in the country to hand over the call-detail records of their customers.[375] Such data includes customers' names, street addresses, times of calls, and other personal information including "detailed records of calls they made – across town or across the country – to family members, co-workers, business contacts and others."[376] Further, the National Security Agency (NSA) is reported to be in receipt of copies of American citizen's telephone and other communications records.[377] Such surveillance activity is conducted primarily using devices called fiber optic splitters that make copies of all emails, web browsing activity, and other Internet traffic to and from its customers and provides those copies directly to the NSA.[378] This copying includes both domestic and

---

[374] Malcolm Thorburn *Identification, Surveillance, and Profiling: On the Use and Abuse of Citizen Data*, in DENNIS, SULLIVAN ED., PREEMPTING CRIMINAL HARMS, 17, http://ssrn.com/abstract=1991747.

[375] *How The NSA's Domestic Spying Program Works*, Electronic Frontier Foundation, https://www.eff.org/nsa-spying/how-it-works.

[376] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (5 Nov. 2006), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[377] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, NYTIMES (16 Dec. 2005), http://www.pulitzer.org/archives/7037. Such activities are, according to the authors, in violation of the privacy safeguards established by Congress and the US Constitution.

[378] Electronic Frontier Foundation, *supra* fn 375. 'The reports showed – and the government

international Internet activities of phone customers. The disclosures of whistleblower Edward Snowden identify PRISM as an NSA program devised to receive such copies taken from "emails, video clips, photos, voice and video calls, social networking details, logins and other data held by a range of US internet firms."[379] A leaked government PowerPoint presentation identifies the Internet firms as Microsoft and its Skype division; Google and its YouTube division; Yahoo; Facebook, AOL, Apple, and chat service PalTalk.[380]

The British news media reported similar activities by Government Communications Headquarters (GCHQ), based in Cheltenham, through access to the NSA system employed since at least June of 2010. That piggybacking on NSA capabilities reportedly generated 197 UK intelligence reports in 2012 alone.[381] Such access would appear to "allow GCHQ to circumvent the formal legal process required to seek personal material such as emails, photos and videos from an Internet company based outside the UK."[382] Google has denied they provided a back door to governments for surveillance but suggests it has cooperated with legal requests for consumer data. The PowerPoint establishes that the NSA has had access to both stored communications and real-time collection of raw data "'for at least six years, without the knowledge of users, who would assume their correspondence was private.'"[383]

In terms of individual disclosure risk, the British Broadcasting Corporation warns Internet users that when they visit a website their IP address, type of device, and screen size can easily be ascertained.[384] In households with more than one device, it is the IP address of the router, and not the individual device, that is traceable, although law enforcement agents have facilities to trace an individual's geo-location from his IP

---

later admitted - that the government is mass collecting phone metadata of all US customers under the guise of the *Patriot Act*. Moreover, the media reports confirm that the government is collecting and analyzing the content of communications of foreigners talking to persons inside the United States'.

[379] Leo Kelion, *Q&A: NSA's Prism internet surveillance scheme,* BBC News (25 June 2013), http://www.bbc.com/news/technology-23027764

[380] *Id.*

[381] Nick Hopkins, *UK Gathering secret intelligence via covert NSA operation,* GUARDIAN (7 June 2013), http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism.

[382] *Id.*

[383] *Id.*

[384] Tom De Castella & Kayte Rath, *Prism and privacy: What could they know about me?* BBC News Magazine (12 June 2013), http://www.bbc.com/news/magazine-22853432.

address.[385] The website can also see what search term or former website brought users to the current website. An individual's geo-location can be determined by cross-referencing the IP address with other data and, if access was obtained using a work computer, the name of the employer. All those details are automatically identified and recorded. Internet service provider British Telecom suggests that, unlike its American counterparts, it does not keep a record of customers' browsing activity.[386]

After such metadata has been obtained by the NSA or other intelligence agency, it begins to data mine and analyze it for evidence of activities that threaten national security. Data mining involves the search for key words and connections of ideas or persons. According to the Electronic Frontier Foundation, the specific equipment installed at telephone facilities includes a machine called the NARUS Semantic Traffic Analyzer[387], a powerful tool to conduct deep packet inspection (DPI). The latter is a method of information extraction that filters packets of data as they reach inspection points in their transmission. DPI collapses firewall security programs as it searches for breaches of protocol, viruses, spam, or other predetermined criteria and redirects such data for closer inspection.[388] Good uses include cleaning up spam and viruses and helping with traffic disruption. Bad uses include totalitarian-type surveillance by governments, including the copying of data. The NARUS machine forwards such communications to a central location for storage and analysis. The Electronic Frontier Foundation estimates the NSA installs several such storage facilities across America. Author James Bamford estimates a $2 billion running cost for the Utah facility back in 2006 which housed data the NSA has collected for the past decade, including "the complete contents of private emails, cell phone calls, and Google searches" and personal

[385] Michael Horowitz, *What does your IP address say about you?* CNET (15 Sept. 2008) http://www.cnet.com/news/what-does-your-ip-address-say-about-you/.
[386] *Id.*
[387] Public Unredacted Klien Declaration, para 35, (28 Mar. 2006) Electronic Frontier Foundation, https://www.eff.org/node/55051. "[A]s of the mid-2000s—each Narus machine was capable of analyzing 10 gigabits of IP packets, and 2.5 gigabits of web traffic or email, per second. It is likely even more powerful today."
[388] Quinn Norton, *iColumn: The Dangers of Deep Packet Inspection,* Maximumpc (2 May 2013), http://www.maximumpc.com/article/columns/Deep_Packet_Inspection_2013 .

data trails composed of parking receipts, travel itineraries, bookstore purchases and other "digital pocket litter".[389]

It is important when discussing Big Data collection practices of state authorities to distinguish between those used for statistical and demographic purposes (which are helpful to the data subject and research generally) and those employed for citizen profiling (generally perceived as exploitative in the hands of state authorities).[390] The latter function is more worrisome in the breach: analytics are often misapplied or results contain errors that could have grave consequences for the data subject. In the following account of a researcher at Harvard University's Berkman Center for Internet & Society, profile indicators have led to an erroneous 'personalization'.

> Google thinks I'm interested in parenting, superhero movies, and shooter games. The data broker Acxiom thinks I like driving trucks. My data doppelgänger is made up of my browsing history, my status updates, my GPS locations, my responses to marketing mail, my credit card transactions, and my public records. Still, it constantly gets me wrong, often to hilarious effect.[391]

The researcher suggests we all have a data doppelganger somewhere in the digital universe, due to the sheer amount of processing of Big Data that is being conducted day to day. The menacing aspect of that possibility is the data disclosure we undergo continuously at the hands of unknown third party agencies.

d Distinguishing a Processor, Controller & Publisher

Identifying the role of the Internet company becomes crucial when attempting to allocate liability for the placement or carriage of libelous or other damaging reputational content. This area of law is in flux in both the US[392] and EU,[393] generating

---

[389] James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What you Say),* WIRED (15 Mar. 2013), http://www.wired.com/2012/03/ff_nsadatacenter/all/.
[390] Thorburn, *supra* fn 374 at 142.
[391] Sara M. Watson, *Data Doppelgangers and the Uncanny Valley of Personalization,* ATLANTIC (16 June 2014) http://www.theAtlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780/.
[392] Sam Gustin, *Is Broadband Internet Access a Public Utility?* TIME (9 Jan. 2013), http://business.time.com/2013/01/09/is-broadband-internet-access-a-public-utility/ (reviewing Susan Crawford's Captive Audience: The Telecom Industry And Monopoly In The New Gilded Age, a book that recommends the same); *Internet Regulation: Not neutral about net neutrality,* Economist (15 Nov. 2014), http://www.economist.com/news/business/21632511-barack-obama-jumps-debate-about-how-regulate-broadband-not-neutral-about-net (indicating US President Obama supports the public utility idea).

a large body of litigation for the courts and government watchdogs such as the FCC in America and the International Telecommunications Union (ITU) in Europe. US industry leaders maintain either that their role is confined to acting as intermediary between those who post the content (publisher) and the subject of the content (individual user), or that they are data processors under an agency arrangement with the publisher. The EUDR defines a processor as a "separate legal entity with respect to the controller who process [sic] personal data on his behalf";[394] a controller is any body that "determines the purposes and means of the processing of personal data."[395] Those definitions suggest that processors act as agents for controllers who decide what information is processed and how. For example, SNS providers offer online communication platforms that enable individuals to publish and exchange information with other users. In this respect, under the EUDR, it could be argued that they are data controllers because they determine both the purposes and the means of the processing of such information.[396] In a more complex example, a public health authority might work jointly with several hundred agencies to transmit personal health data; in that situation, both agency and authority could be considered joint controllers.[397] The decision-making by controllers would seem to involve more autonomy and hence attract more legal liability. For their part, ISPs and the public health authority could argue they are merely processing information or data that is conveyed to them by data controllers; they do not have an active role in determining the 'purpose and means' of what is published online.

The concept of 'publisher' within the online context is more complex. With Google, for example, the role of an active publisher of online content focuses primarily on active editorial decision-making. In a 2012 White Paper on the issue commissioned

---

[393] Leila Abboud, *France calls for EU to regulate Web giants to counter dominance,* REUTERS (19 Sept. 2013) http://www.reuters.com/article/2013/09/19/us-france-eu-webgiants-idUSBRE98I14E20130919; Mark Scott, *E.U. Debates Which Nation Will regulate Web Privacy,* NYTIMES (26 May 2014), http://www.nytimes.com/2014/05/27/technology/with-european-data-rules-come-a-need-for-a-cop.html?_r=0.

[394] Opinion 1/2010 On The Concepts Of 'Controller' And 'Processor', ARTICLE 29, Data Protection Working Party, Document 169, adopted 16 February 2010, 25 http://ec.europa.eu/justice/data-protection/index_en.htm.

[395] *Id.* at 7.

[396] *Id.* at 21.

[397] *Id.* at 24.

by Google Inc., legal practitioners Volukh and Falk advise that liability can be sidestepped by focusing on the 'mere communicator' role:

> To be protected by Safe Harbor laws, and free from copyright and libel suits, it often works best for Google to be a mere communicator of information, and not responsible for the information people put online.[398]

That characterization might involve disproving that Google's activities involve editorial judgment. We know, however, that Google determines the content and order of search results based on which items most accurately respond to the nature of the search query.[399] Volukh and Falk conclude that Google's exercise of editorial judgment in such cases is analogous to, and could attract liability for, the activities of traditional book and other media publishers.[400]

The CJEU judgment in the 2014 *Google Spain* case indeed identified Google Inc. and its national divisions as controllers under most conditions, subject to liabilities for constructive knowledge of content.[401] That judgment is persuasive, not binding, on the final form that the EUDR will take; it is also not binding on US jurisdictions. It remains to be seen how legal and market pressures around such liability issues raised by Google Spain will affect individual applications for content erasure.

---

[398] Eugene Volokh & Donald L. Falk, *First Amendment Protection for Search Engine Search Results*, White Paper submitted to Google Inc. (20 Apr. 2012) 4, http://www2.law.ucla.edu/volokh/searchengine.pdf

[399] *Id.* See also *Search King, Inc. v. Google Technology, Inc.* No. CIV-02-1457-M, 2003 WL 21464568, at§4 (W.D. Okla. May 27, 2003) where the federal court of Oklahoma concluded that Google's rankings of pages were "subjective result[s]' that constituted 'constitutionally protected opinions" entitled to full constitutional protection.

[400] *Id at* §27.

[401] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González,* Judgment in Case C-131/12, Luxembourg, CJEU Grand Chamber, 13 May 2014 (Google Spain) http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065. The case involved an auction notice for property in Spain regarding an outstanding debt of Mario Costeja Gonzales. Although the debt was paid and the property was not auctioned, Google searches ten years later still brought up the newspaper advertisement. Gonzales sued for its removal, citing damages to reputation that jeopardized his financial, professional, and social opportunities. Google claimed to do so would amount to historical revisionism.

e The Speed and Ambit of Dissemination

The speed and reach of online transmissions provides another unique feature of web-based content, improving on such attributes of telecommunication cables and telephony transmission to an exponential degree.[402]

Internet speed can be measured by megabits per second,[403] information that can be seen in the downloading activities of users. Figure 1 illustrates, under 'speed' in the right hand column, the minimum megabits per second (Mbps) at which emails are downloaded (0.5), content is downloaded from a browser (less than 0.5 to 1), a video is streamed (0.7), a high definition movie is streamed (4), videoconferencing occurs (1), and tele-learning materials can be downloaded (4). Those figures indicate a transmission speed often faster than the time it takes us as humans to find the 'send' key on a particular page. The figures also indicate that the downloading speed for email and government information sites were relatively the same in 2013 and can be accessed in half a second, the fastest access of any shown, except for streaming radio content. The latter function requires uploading time, however, which routinely slows down the transmission. Although those results are contingent on the bandwidth, time within the 24 hour clock, and type of device used, they indicate that gossip, lies, doctored content, and other reputational damage can be disseminated with menacing speed.

Translating those figures into meaningful descriptors of speed can be achieved in a relational sense if we consider the example of the use of Twitter to warn others about impending natural dangers. For example, when examining the transmission of tweets during an Earthquake in Virginia in August of 2011, one author suggested that their speed (200,000 kilometers per second) actually overtook the seismic event and arrived in neighbouring states *before* the earthquake (traveling at 3 to 5 kilometers per second).[404]

---

[402] Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N. C. L. REV. 3 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2024661

[403] A bit is a single numeric value, either 1 or 0, that encodes a single unit of digital information. A byte is a sequence of bits; usually eight bits equal one byte. An Internet Protocol (IP) address contains 32 bits or 4 bytes. The bits encode the network address so that it can be shared on the network. The bytes divide the bits into groups. A megabit, then, equals over one million (1,048,576) bits. *See further* Bradley Mitchell, *What is the difference between bits and bites*, About.Com, http://compnetworking.about.com/cs/basicnetworking/f/bitsandbytes.htm.

[404] Brad Plumer, *Tweets move faster than earthquakes,* WASH. POST (25 Aug. 2011), http://www.washingtonpost.com/blogs/wonkblog/post/tweets-move-faster-than-earthquakes/2011/08/25/gIQA4iWHeJ_blog.html.

Those comparative figures convey the speed of reputational damage that new media offers.

Activity	Minimum Download Speed (Mbps)
Email	0.5
Web browsing	
Job searching, navigating government websites	0.5
Interactive pages and short educational videos	1
Streaming radio	Less than 0.5
Phone calls (VoIP)	Less than 0.5
Watching video	
Standard streaming videos	0.7
Streaming feature movies	1.5
HD-quality streaming movie or university lecture	4
Video conferencing	
Basic video conferencing	1
HD video conference and telelearning	4

Table 1: 2013 Broadband Speed Guide (excerpt)[405]

In addition to the speed at which a defamatory posting can cause injury is the ambit of its reach. At the close of the first quarter of 2014, for example, Facebook was reported to have 1.28 billion monthly active users.[406] Unlike in Brandeis' day,

[405] Source: US Federal Communications Commission (FCC) http://www.fcc.gov/guides/broadband-speed-guide. (Report offer results of rigorous broadband performance testing for 13 of the largest wire line broadband providers that serve well over 80 percent of the U.S. residential market. Tests conducted used automated, direct measurements of service delivered to the homes of thousands of volunteers across the United States.)

[406] *6 New Facts About Facebook,* Pew Research (3 Feb 2014), http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/ (advising Pew Data indicates Facebook is used by 57% of all American adults and 73% of youth ages 12-17, and that adult Facebook use is intensifying. *See also Facebook claims to become 'biggest stadium in the world' for World Cup,* RT (9 June 2014) http://www.facebook.com/fifaworldcup(reporting that although Facebook usage amongst European youth reached 57% penetration of the 17-25 year old market, it is not the

embarrassing or degrading material is not just disseminated to a limited circle of friends or newspaper subscribers: viewers of the *Star Wars Kid* YouTube video, for example, posted in 2002 by rancorous classmates of a 15 year-old awkward teenager, reached over 29 million viewers as of June, 2014.[407]

One of the more prominent examples of the instant interoperability of media in today's event coverage occurred on March 2, 2014 with the Oscar Awards ceremony in Hollywood. A media conversation occurred as 43 million viewers watched the event in person or on television and transmitted and re-transmitted SNS commentary with other viewers using social media accessible on their tablets and smartphones. The discursive level was record-breaking for the secondary transmissions of a public media event: Twitter claimed that 14.7 million tweets mentioned the Oscars during the telecast and Facebook reported 25.4 million interactions overall that mentioned the show. That simultaneous conversation resulted in the highest television ratings for the Oscar event since 2004. In addition, the 'selfie' photograph tweeted by Oscars host Ellen DeGeneres was retweeted within the subsequent twenty-four hour period 2.8 million times.[408] That messaging traffic caused an overload disruption of Twitter service for about 20 minutes, generating even more publicity for the event.[409] The Oscar moment illustrates the high value in the news and entertainment business of interconnected participatory media that can orchestrate simultaneous real time grassroots and networked conversations that are regenerated by journalists and anonymous tweeters within a few hours, with live commentary about the secondary traffic during the event. The speed and ambit of transmissions detailing the event comprise the story as much as what unfolded within the Dolby Theatre in Los Angeles. The event created a "landmark social media moment"[410] with real time observation, by television and SNS users, of a digitally transmitted event going 'viral' through the secondary interactivity of social media

---

most popular SNS for youth overall, eclipsed by Hyves in the Netherlands and SchulerVZ in Germany*)*.

[407] The figure on 9 June 2014 was 29,192,626 as recorded on *Star Wars Kid,* YouTube, www.YouTube.com/watch?v=HPPj6viIBmU.

[408] A reported 254,644 tweets per minute. The previous record was the 810,000 tweets of President Obama kissing his wife upon learning of his election win in 2013.

[409] David Bauder, *Ellen DeGeneres' selfie a landmark social media moment*, ASSOCIATED PRESS & CTV NEWS (4 Mar. 2014), http://www.ctvnews.ca/entertainment/ellen-degeneres-oscar-selfie-a-landmark-social-media-moment-1.1712937.

[410] *Id.*

transmission. While no quantum of viewers is used to define when a video reaches viral status, the term in general use conveys the idea that an event has been viewed by more than a million people in less than a week.[411]

The widespread and immediate implications for personal reputation of viral transmissions are illustrated by a split-second comment: Oscar host DeGeneres made a derogatory quip to guest Liza Minnelli suggesting she looked like a drag queen as a result of recent plastic surgery.[412] That comment was streamed live and subsequently carried on social media, print stories, and video and audio clips, provoking the largest Twitter traffic to date of any public figure.[413] A Google search of 'Liza Minnelli at Oscars' the same evening delivered hundreds of search results of the remark within seconds.[414] Many of those stories characterized DeGeneres' comment as 'transphobic', a pointed reference to the self-identified gay entertainer; other commentators label the remark 'transmisogynist',[415] 'disrespectful',[416] and 'mean-spirited'.[417] The comment, defended by DeGeneres as humourous, illustrates the fragility of reputation, those of *both* DeGeneres and Minnelli, and the unimaginable breadth of potential stigma caused by the out-of-control social media frenzy that reaches millions of viewers in the blink of an eye.

In gauging the ambit of harm, one should also consider the dissemination of insulting or defamatory content accessed through the serendipity of the search function. Search results can offer a wealth of information we did not even know existed and were not looking for, and can provide new insights simply through their random combination.[418]

---

[411] 'Viral', Techterms.Com, http://techterms.com/definition/viral.
[412] Caitlin Dewey, *Internet consensus: DeGeneres' Lisa Minnelli joke 'mean', 'transphobic'*, WASH. POST (3 Mar. 2014), http://www.washingtonpost.com/blogs/style-blog/wp/2014/03/02/.
[413] George Stark, *Ellen DeGeneres 'uquesn 'transphobic' after Oscars joke that suggested Liza Minnelli looked like a drag performer falls flat*. DAILY MAIL (4 Mar. 2014), http://www.dailymail.co.uk/tvshowbiz/article-2573116/.
[414] Results can be viewed at https://www.google.ca/?gfe_rd=ctrl&ei=H7vvUrXrJKuC8QfQkYCIBg&gws_rd=cr - q=liza+minelli+at+oscars
[415] Dewey, *supra* fn 412.
[416] *Id.*
[417] Jason St. Amand, *Was Ellen's Liza Minnelli Joke Transphobic?* EDGE SAN FRANCISCO (3 Mar. 2014), http://www.edgesanfrancisco.com/entertainment/celebrities/news//156105/.
[418] Korenhoff, *supra* fn 368 at 2. *See also* B. Sparrow, *et al., Google Effects on Memory: Cognitive Consequences of Having information at our finger tips*, 333 SCIENCE, 776-778.

f Memory and Durability: the Half Life Debate

The question of how long online content endures is of critical importance to sufferers of a derogatory remark or untrue accusation within new media. Much literature addressing new media communications has us believing that reputation-damaging postings are permanent or at least highly persistent. Hence there is potential for deeper and more enduring harm than offline defamatory statements because of the expanded audience and its protracted access to our data. Internet users, particularly young ones, receive ample warnings of the permanence of online memory from industry, educators, and family. In contrast, among those who study the Internet is a group of digital communications-savvy scholars who maintain that online content is short-lived. Texting and SNS communications as well seem to remain on our smart phones or other devices despite promotion of their perishability.[419] We speak of their evanescence, a feature that "eases the force of the blow" of defamation.[420] It has become, in some circles, the 'half-life' debate of digital communications.

Among proponents of content evanescence is Harvard history scholar Jill Lepore who assesses the Web as ethereal, uns, and unreliable. She cites two studies that empirically establish the transience of online sources. In the first, a 2013 survey of legal policy-related journals identified a near-fifty percent loss in workable URLs over six years.[421] The second study, at Harvard Law School, found over 70% loss of URLs cited in *Harvard Law Review* and other journal articles, as well as a 50% attrition of URLs within US Supreme court opinions. Lepore notes the frequency with which the error message (Page not Found) is the result of our online search efforts and concludes, "[s]ocial media, public records, junk: in the end everything goes."[422] Both of those studies relate half-life to the amount of time that content remains accessible and functionally useful while online. The term does not describe the value of the underlying knowledge conveyed.

Within the contingent of social network scholars who argue that the durability of information via Internet does evaporate over time are Daniel Gomes and Maroi

[419] For a comprehensive review of social networking sites *see* dana boyd & Nicole B. Ellison, *Social network sites: Definition, history, and scholarship,* 13 J. COMP.-MED. COMM. (2007).
[420] Bernstein, *supra* fn 402 at 2.
[421] Jill Lepore, *The Cobweb: Can the Internet be Archived?* NEW YORKER (26 Jan. 2015) 34.
[422] *Id.*

Silvia. Their studies suggest that, in 2006, just over half (55%) of content remained online after one day, 41% after a week, 23% after 100 days, and 15% after a year.[423] Meg Ambrose of Georgetown University in turn suggests that "information is not permanent, no matter the medium" and calls for principled information storage practices.[424] She attributes disappearing content more to technological malfunctions such as media and hardware errors, software failures, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and organizational failures.[425] Interestingly, a search of one of Ambrose's articles posted on her Georgetown University website brings up an error message suggesting its evaporation, or at least disappearance, from a reader's view.[426]

Those observations of disappearing articles, eroding links, and faulty URL address the technical decay of online access. Another view of the half-life debate is the diminishing value or usefulness of knowledge or content over time. The half-life of knowledge can be defined as the time span between its attainment and its obsolescence.[427] Software trainer Cathy Gonzales of the University of Northern Texas pointed out over a decade ago that half of what was known in the world had not been known ten years prior. In other words, the amount of online-accessible knowledge in the world had doubled over those ten years.[428]

Marketing professionals assign another meaning to the half-life of digital communications: the waning of public interest over time in particular technologies or platforms. It is appropriate, in marketing terms, to speak of emails reaching a half-life as a social networking preference as a large percentage of users have migrated to Facebook and other SNSs. Similarly the usefulness of data sets might be described as reaching their half life with time, as possessing only half their scientific usefulness compared to when they were first compiled. As much of learning is now online as a shared activity

---

[423] Daniel Gomes & Mario J. Silvia, *Modeling Information Persistence on the Web*, Proceedings of the 6th International Conference on Web Engineering, 1 (2006).
[424] Angelo, Google, *supra* fn 79 at 23.
[425] *Id.*
[426] Meg Leta Ambrose, *A Digital Dark Age and the Right to be Forgotten*, 17 J. INTERNET L. (2013) 1.
[427] *See, for example,* Cathy Gonzalez, *The role of blended learning in the world of technology* (2004), http://www.unt.edu/benchmarks/archives/2004/september04/eis.htm.
[428] *Reflecting on Learning Theories and Instructing*, Idt2me (23 Apr. 2011), http://idt2me.wordpress.com/2012/04/23/reflecting-on-learning-theories-and-instructing/ - respond.

rather than an internal, individualistic experience in a library stall, the study of the persistent value of knowledge is an important pursuit; knowledge acquisition is altered to some extent every time new tools are utilized and skills developed.

g Is Digital Speech Different?

Who among us has not been alarmed at the bluntness of expression used in the texting or YouTube commentary authored by digital natives? If the compression of words and fragmentation of meaning has you scratching your head, consider this fictional text authored by an adult to suggest how a casualty of the massacre at Bull Run might have communicated to his wife on the evening before his death if texting had been available 60 years ago:

"rly scrd. mite not mk it. luv u. C u on otr side."[429]

As every prosecutor and defence counsel is aware, trial outcomes can turn on the indecipherability of one term or line in a social media message (SMS)[430] that frustrates attempts to successfully link cause and effect. When SMS users suggest that they employ two languages to communicate with their close communities, the truncated, rebus-like form used for social texting and a more grammatically correct form for more professional or academic communications, a recent study supports their claim.[431] Study participants spoke of their ability to speak two languages, to effortlessly move from one to the other depending on the medium. As the study reported,

> students are generally aware of the context in which they are writing and they can switch to the appropriate register or style when writing formally for

[429] Peggy Drexler, *The Importance of being Fluent in the Language of texting,* FORBES (23 June 2014), http://www.forbes.com/sites/peggydrexler/2014/06/23/the-importance-of-being-fluent-in-the-language-of-texting/.

[430] A texting acronym for 'short message service' or the text message itself.

[431] Shazia Aziz *et al., The Impact of Texting/SMS Language on Academic Writing of Students – What do we need to panic about?* 55 ELIXIR LING. & TRANS. J. 12884 (2013), (reporting on 50 undergraduates (42 males and 8 females) in Bachelor of Computer Engineering and Bachelor of Telecommunication Engineering classes in Lahore India. Participants between the ages of 19 and 25 years were asked to write an essay which was analyzed for texting features.)

> academic purposes despite the fact that texting is their common way of communication.[432]

Those results pose the question: might digital language comprise its own form of communication?

In canvassing the harm that we need to prove for legal actions in reputational damage, it is relevant to consider whether new norms should be adopted for characterizing speech on the Internet. Given the democratization of online speech (free, spontaneous, and open cultural expression) it has been suggested we allocate less probative weight and meaning to such utterances.[433] The human sources of communications, so critical to acceptance of traditional media accounts, are often suppressed online. Cues about authority and status can be hidden, as one psychological study of Internet behavior points out,

> Although one's identity in the outside world ultimately may shape power in cyberspace, what mostly determines the influence on others is one's skill in communicating (including writing skills), persistence, the quality of one's ideas, and technical know-how.[434]

With the lack of editorial second thought for bloggers, tweeters, and other participants in virtual reportage and other new media uses, it becomes practically infeasible to read the tone of derisive material. The normative debate usually goes like this: the Internet is a communicative tool with a wireless method of transmission but otherwise of similar purpose and method as offline communications, and so the customary societal norms should apply; on the other hand, Internet content is "located in another time and zone" and therefore not subject to the norms of traditional journalism.[435] Yuval Karniel of IDC Herziliya in Israel takes the position that "an anonymous, instant, unfiltered and unmediated statement" for which there is no source and "which does not make grounded factual claims" should not constitute a cause of action for defamation.[436] He views the role of blogs and other informal journalism as the preliminary flagging of issues that the mainstream offline press later might assess as worthy of more formal investigation, as

---

[432] *Id* at 12889.
[433] Yuval Karniel, *Defamation on the Internet: A New Approach to Libel in Cyberspace,* 2 J. INTL MED. & ENT. 215, 216 -219 (2008).
[434] John Suler, *The Online Disinhibition Effect, 7* CYBERPSYCH. & BEH. 324 (2004).
[435] *Id*. at 218.
[436] *Id*. at 234.

was the case with the Clinton-Lewinski allegations.[437] Such investigations could lead to publication in traditional media, argues Karniel, but are not to be valued as authentic information source in themselves.[438]

A counter position has been taken by Meg Ambrose who suggests that the purpose of self-publishing online is to express opinions and convey news in the language of traditional media but using electronic platforms. That opinion holds that, for the digital author, all online speech maintains a fluidity due to its *ad hoc*, unstudied, and unedited nature and is itself a contributor to our moral autonomy, to our self-presentation. Our expression via online blogs, chats, commentary, and emails affirms our own moral career, and that justifies constraining others 'in their attempts to engineer and directly, or indirectly shape' our identities.[439] Texting, therefore, is its own means of expression, its own language.

Ethan Zuckerman, founder of Facebook, points out that the difference with online comments (within the context of the hate or 'dangerous' speech incited by trolls) can be characterized as one of access: the Internet creates an environment where we are aware of speech we would not hear otherwise. Most of us in pre-online times, he argues, would not have been aware of what speech is shared at a KKK meeting, and many of us would not have heard the sexist jokes that were told in male-dominated locker rooms. Online speech permits a crossing to formerly closed communities.[440] Researcher Susan Benesch of the Berkman Center of Internet & Society at Harvard University defines the online-offline speech discrepancy involved in hate or dangerous speech as one perceived in the effect such speech has on people. With online speech environments we can examine the effect of speech on people through tracking both responses and effects. In offline environments, however, 'it's very hard to measure what reactions dangerous speech leads to'.[441] Zuckerman and Benesch's comments introduce the constitutional

---

[437] *Id.*
[438] *Id.,* p. 237.
[439] Angelo, Google, *supra* fn 79 at 22.
[440] Ethan Zuckerman, *Susan Benesch on dangerous speech and counterspeech,* Blog (2 Mar. 2014) http://www.ethanzuckerman.com/blog/2014/03/25/susan-benesch-on-dangerous-speech-and-counterspeech/.
[441] Susan Benesch, *Troll Wrastling for Beginners: Data-Driven Methods to Decrease Hatred Online,* Video, Berkman Center for Internet & Society (25 Mar. 2014) http://cyber.law.harvard.edu/events/luncheon/2014/03/benesch.

parameters of freedom of expression in more ad hoc forms of online expression, a discussion we shall take up more vigorously in Chapter IV.

3.2 How Harm is Done

a Exposure Harms: the Technology and Case Examples

In terms of how reputational injury can be practically achieved using the Web, I examine three sources that, either through attributed or anonymous postings, inflict shame or ridicule than can be easily ascertained by other members of a virtual community. Those sources include: exposure by other users; exposure by ourselves; and exposure by journalists.[442] My focus continues to be the individual Internet user: reference to corporate, government, or other institutional activity is used to survey the extent of the threat to that user's reputation.

i Exposure by Other Users

The most common, and probatively useful, online activity by other users that damages reputation involves 'flaming', 'outing', tagging, and creation of false 'mirror' social networking sites.[443] Flaming can be defined as the hostile and insulting interaction between Internet users, often expressed through profanity. Flamers subscribe to forums, chatrooms, email, Xbox or PlayStation interactive games and video-sharing sites with the intent of embarrassing other players by revealing their identities and personal information to pierce the anonymity of their chosen pseudonyms or avatars. Flaming is routinely generated by political, religious, or philosophical topics and the objective is to impose emotional and reputational injury for all participants to see.

Some websites create an interactive environment that attracts the participation of flamers or 'trolls',[444] sowers of discord through their deliberate, inflammatory messaging. Such online provocateurs are increasingly the subject of social science

---

[442] Exposure by journalism is a method that is covered more generally throughout this dissertation.

[443] Cyberbullying and cyberstalking are online predatory behaviors that are traditionally addressed by the criminal law and are beyond the scope of this paper.

[444] *The Chambers Dictionary* (12 ed) (2011): to 'flame' is to produce 'an insulting, rude or controversial email message' and to 'troll' is to 'make a conscious attempt to provoke controversy or disagreement on the Internet' more generally.)

research, and developing theories to explain flaming or trolling include deindividuation (a psychological state where inner restraints are lost when individuals are not seen or acknowledged as individuals),[445] and the disinhibition effect (the de-inhibiting of behavior prompted by anonymity resulting in more aggressive or punitive activity).[446] Such behaviors can attack the emotional integrity of others either through individual action or group behaviors. With the latter, individual identity is absorbed by the group, and individual responsibility for actions is diffuse due to the number of actors. One way to reduce deindividuation is to make group members more self-aware by addressing them by name, pointing out the harm they are doing.[447] Another is to report (or self-report) such anonymous attacks online, as this former troll reports:

> After processing what I did, I was disgusted by how I acted and I sent [the victims] a message and talked to them in private. I did apologize … You are proving nothing when you use someone's personal information for your own vandetta.[sic].[448]

Outing originally involved "an act of telling the public that a person is homosexual when that person does not want the public to know"[449] For example, in a survey of studies exploring the low reportage levels in same sex domestic assault cases, the authors determined that threats of 'outing' the victim's sexual orientation is used by the abuser to isolate the victim even further.[450] The threat to go online with such personal information compounds the shame. It could also bring fear of loss of family emotional support or the ability to sustain oneself financially[451]

---

[445] Christina Demetriou & Andrew Silke, *A Criminological Internet 'Sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap*, 43 BRIT. J. CRIM., 213, 214.
[446] Suler, *supra* fn 434 at 322; *see more generally* P. Ellison *et al*. *Anonymity and Aggressive Driving Behavior: A Field Study*, 10 J. SOC. BEH. & PERS., 265 (1995).
[447] *See further* Mike Perry, *Deindividuation*, Living in a Social World, http://www.units.miamioh.edu/psybersite/fans/deindividuation.shtml .
[448] *Gotham City (Gameplay Discussion)*, Sony Online Entertainment (13 Dec. 2013), *see generally* https://forums.station.sony.com/dcuo/index.php?forums/gotham-city-gameplay-discussion.2/page-5 . For further exploration *see* Teo Keipi et al. *Who prefers anonymous self-expression online? A survey-based study of Finns aged 15–30 years*, 18 Inf., Comm. & Soc. (2015) (correlating anonymous Finnish Facebook users with both grandiosity, a component of narcissism, and low self-esteem; users are younger, highly trusting, with few offline friends.
[449] Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/outing.
[450] Hadar Aviram and Annick Persinger, *Perceiving and Reporting Domestic Violence Incidents in Unconventional Settings: A Vignette Survey Study*, 23 HASTINGS WOMEN'S L.J. 159 (2012).
[451] *Id.*

The meaning of 'outing' has been expanded through popular usage. It now conveys the more general idea of exposing undesirable aspects of a person's self or experiences and includes the activities of Anonymous, an international collective of activists and hacktivists,[452] whose rationale is to cause the public exposure of personal secrets or public wrongs. For example, a news article has described as 'outing' the Anonymous identification of the man who taunted Canadian teen Amanda Todd into performing sexually explicit acts on her webcam, ultimately resulting in her suicide.[453] In a show of similar journalistic altruism, the media blog Gawker claimed to be the first to 'out' Toronto mayor Rob Ford's use of crack cocaine by blogging about its viewing of a video showing Ford's indiscretion.[454] The Gawker founder claimed his 'outing' contributed to Ford's confession of illicit drug use.[455] Those examples suggest outers might be motivated by a sense of noble cause, of exposing evil and righting an injustice. Gamer 'outers' give no such impression, however, although their incentives remain relatively unexplored by research.

There appears to be an unwritten social code amongst bloggers that anonymous contributors will not be exposed. The reaction of a science writer to the outing of a fellow writer explains the preference for anonymity:

> There's still a lot of fudging around, figuring out the boundaries of our online interactions. When people play games like outing someone who's using a pseudonym, they're … declaring to the community that "I believe that our community standards should say that this is an appropriate way to deal with conflict".[456]

---

[452] Hacktivism indicates anonymous group action to convey a political message through manipulation of a website.

[453] Sady Doyle, *Outing online sexual predators is a sensationalist stopgap,* GUARDIAN (17 Oct. 2012), http://www.theguardian.com/commentisfree/2012/oct/17/outing-online-sexual-predators-gawker-anonymous.

[454] Gawker is a blog founded by Nick Denton and Elizabeth Spiers and based in New York City that bills itself as 'the source for daily Manhattan media news and gossip'. Founded in 2003, it focuses on celebrities and the media industry. *See Documents: Rob Ford did 'Hezza', Tries to Buy Crack Video with a Car*, Gawker.com (12 Apr. 2013), http://gawker.com/documents-rob-ford-did-hezza-tried-to-buy-crack-vid-1476729771.

[455] *Gawker Ends Hunt for Purported Crack Video*, CBC Radio podcast (18 July 2013), http://www.cbc.ca/news/canada/toronto/gawker-ends-hunt-for-purported-rob-ford-crack-video-1.1370154.

[456] CC Mark, *On outing in the sciblogging community,* Scientopia (21 Jan. 2014) http://scientopia.org/blogs/goodmath/2014/01/21/on-outing-in-the-sciblogging-community/.

In some instances, anonymity is a safety precaution:

> Some people [choose anonymity] to avoid professional retaliation…there are tenure committees at many universities that would hold blogging against a junior faculty; there are companies that don't allow employees to blog under their real names; there are people who blog under a pseudonym in order to protect themselves from physical danger and violence![457]

Within that frame, to expose a fellow participant is to breach an unwritten code of mutual trust and support.

'Tagging' represents another potentially harmful activity. It serves the same function as keyword searches by attaching a word or phrase to a digital object, such as a document or photograph, for easy retrieval. Facebook reported in 2011 that "Every day, people add more than 100 million tags to photos on Facebook."[458] The social networking server (SNS) promotes tagging as "an easy way to share photos and memories" because, unlike photographs that get forgotten in a camera or an unshared album, "tagged photos help you and your friends relive everything."[459] Tagging occurs in two ways: through the identification of individuals in a photograph by a user that is then locked into the memory of networking sites through facial recognition software; and the insertion of single words on a site that provides a link to that photograph. Both methods instantaneously create a tracking system of images. For example, when you post a photograph on your Facebook, MySpace, Instagram or other SNS, and tag persons in the photograph, those tags create a link to your SNS account, in Facebook, for example, through your Facebook Timeline.

You can also tag by creating a status update, letting friends know who you are with at any given moment. That update is conveyed instantaneously and with your implied consent: unless you opt-out of such tagging in your privacy settings, each time you enter a message or image on your FaceBook or other social messaging account, that SNS autonomously sends an alert or update by email to each of the subscribers within your bank of 'friends'. Anyone who sees that update can click on any of your friends' name and go to their Facebook Timeline without invitation, unless your friends have

---

[457] *Id.*
[458] Justin Mitchell, *Making Photo Tagging Easier,* Facebook (30 June 2011) https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130.
[459] *Id.*

indicated in their privacy settings that they do not welcome such access. Facebook does warn against that activity: "if you or a friend tags someone in your post, the post could be visible to the audience you selected plus friends of the tagged person."[460] The friend you have tagged will also receive notice via their Facebook account or email that they have been tagged. And so the depth of their exposure grows.[461] While Facebook architecture provides for reversing tagging of your photographs, it is not at all a straightforward or visible process.[462]

The facial recognition involved in Facebook tagging is controversial for its automatic default. As well, in order to access privacy settings on the SNS to delete your photograph, you must subscribe to that system, a requirement that artificially inflates the subscribership figures *of that SNS* and that assumes a certain technical facility on your part. Another concern is that the facial recognition technology resides in Facebook's servers and not on the user's laptop, giving *de facto* control of the content to the server, not to you.

EU policymakers in the area of online privacy are more proactive in their efforts to warn subscribers about such privacy hazards as tagging,[463] while Americans prefer the "notice and choice" system in keeping with the US entrepreneurial perspective. One commentator notes that such facial recognition technologies create "the biggest creep factor" if it were to fall into the hands of governments."[464] That fear might already have been realized as government databases already include sufficient facial data of our every mundane function from renewing our driver's license to updating travel documentation.

---

[460] *What is tagging and how does it work?* Facebook, http://www.facebook.com/help/124970597582337. Similar facial recognition technology is offered by Google's Picasa and Apple's iPhoto.

[461] *What is Timeline review? How do I turn Timeline review on?* Facebook, http://www.facebook.com/help/168229546579373(advising that Facebook warns a photograph taken by you or a third party might show up in Timeline Review, a function that requires an active opt-out, or News Feed.)

[462] Smith, *Facebook Photos: Opt-Out or Tag You're It*, Networkworld (7 Jan. 2011) http://www.networkworld.com/article/2228269/microsoft-subnet/facebook-photos–opt-out-or-tag-you-re-it.html.

[463] *Online Privacy,* Europa.eu, http://ec.europa.eu/digital-agenda/en/online-privacy. Click on 'Radio Frequency Identification Devices' for an itemization of tagging activities. The principal concern in Europe is that, "[u]nlike ubiquitous UPC bar-code technology, RFID technology does not require contact or line of sight for communication."

[464] Ian Paul, *Facebook Photo Tagging: A Privacy Guide,* PCWorld (9 June 2011) http://www.pcworld.com/article/229870/Facebook_Photo_Tagging_A_Privacy_Guide.html.

Tagging presents exposure risks in job searches, university admissions, [465] and other opportunities.[466] A 2013 commercial study of personal postings incurred as much damage as those describing illegal drug use, sexual behavior, gun use, and alcohol consumption.[467] Tagging is also an enabling tool for cyberstalkers and identity theft perpetrators. As Pew Internet's Lee Rainie summarized the exposure of tags: "It's hard to have privacy and be social at the same time. It's the classic human struggle/tension."[468] The future of tagging might be secure, however, if only because there is no community norm discouraging it.[469]

Revenge porn and the creation of false social media accounts comprise another category of online vindication that risks reputational harm in several ways: through defamatory content, the intentional infliction of emotional harm or the enabling of identity theft.[470] In both activities, an anonymous user posts nude or compromising images of others for their embarrassment potential or creates a false account using profile and other personal information that mirrors a valid account. In the latter case the perpetrator uses the bogus site to duplicate the target's contact list in order to send false and damaging content. Offending posts might even involve false information about the recipient, damaging *her* reputation at the same time. False trust is built by engaging the target's list of 'friends' in order to announce the new account and attract input by well-intended personal and professional contacts. That information can further expose the target. This ruse is notoriously employed by ex-spouses or former friends aiming to diminish the professional or social credibility of the target.

---

[465] Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, NYTIMES (9 Nov. 2013) http://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html (reporting a commercial telephone survey of 381 college admissions officers who admitted to visiting applicants' Facebook or other social media page to learn more about them).

[466] Peter Harris, *The three things that employers look for the most in your social media profiles*, Workpolis (22 Feb. 2014), http://www.workopolis.com/content/advice/article/the-three-things-that-employers-want-to-find-out-about-you-online/.

[467] *Id.*

[468] Mark Glaser, *Top 10 Media Stories of 2010: WikiLeaks, Facebook, iPad Mania*, PBS (30 Dec. 2010) http://www.pbs.org/mediashift/2010/12/top-10-media-stories-of-2010-wikileaks-facebook-ipad-mania364.

[469] Lillian Edwards, *Privacy, Law, Code and Social Networking Sites*, in IAN BROWN, ED., RESEARCH HANDBOOK ON GOVERNANCE OF THE INTERNET, University of Oxford UK, 19, (2013), http://ssrn.com/abstract=2200163.

[470] In most common law jurisdictions infliction of emotional harm is addressed through civil torts while identity theft attracts criminal sanctions.

The practice is sufficiently widespread that social networking innovators are publicizing the extent of the problem.[471] While laws dealing with mirror sites vary from one jurisdiction to another, search companies are taking some responsibility for the easy access of personal information by employing facial recognition technologies or other authenticating precautions.[472] Social media sites are also instilling policies about the acceptable parameters of posts, with Twitter, Reddit, and Blogger announcing privacy changes.[473] Empirical evidence is starting to emerge assessing the extent of the damage: a 2012 study of discrepancies in authentic and fake Facebook accounts determined that 1) almost 60 percent of fake Facebook creators claim to be bisexual, 10 times more than real users; 2) fake accounts indicate having six times more friends than real users; 3) fake accounts use photo tags over 100 times more than real users; and 4) fake accounts claim to be female in 97 percent of the cases, as opposed to 40 percent for real users.[474] The ultimate aim of such fake 'friending' is to create the widest possible networked audience to damage the target's reputation.[475]

Anonymity for social or professional reasons provides legitimate reasons for maintaining fake accounts. For example, a performance artist creates a work that delves into issues about being black and queer within an Islamic environment, a pursuit she

---

[471] See, for example E. Protalinski, *Facebook: 5-6% of accounts are fake*, ZDNet (8 Mar. 2012), http://www.zdnet.com/blog/facebook/facebook-5-6-of-accounts-are-fake/10167(wherein the author relates the concern of Facebook authorities that, in 2012, somewhere between 42.25 million and 50.70 million Facebook accounts were fake, according to measurements of monthly and daily active users as per the company's own estimates.)

[472] *See, for example,* 'How to Reveal a Fake Facebook Account', Wikihow, http://www.wikihow.com/Reveal-a-Fake-Facebook-Account (explaining that "Google uses facial recognition and other algorithms to match a picture, and will either return an exact match (with information like names), or pictures similar to the original.")

[473] Brian Barrett, *Twitter Finally Banned Revenge Porn. Now How to Enforce it?* WIRED (12 Mar. 2015) http://www.wired.com/2015/03/twitter-bans-revenge-porn/.

[474] Study by private security firm Barracuda Networks as reported by E. Protalinski, *How to spot a fake Facebook profile (infographic)',* ZDNet (4 Feb. 2012), http://www.zdnet.com/blog/facebook/how-to-spot-a-fake-facebook-profile-infographic/8580.

[475] *Id.* The discovery of fake Twitter accounts following the campaign of presidential hopeful Mitt Romney, and the selling of tweets to give the impression of a significantly more engaged public in his campaign than was true, is a similar activity but intended to enhance, rather than damage, individual reputation and hence not within the framework of this dissertation. *See further* N. Perlroth, *Fake Twitter Followers Become Multimillion-Dollar Business*, NYTIMES (3 April 2013) http://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/?_php=true&_type=blogs&_r=0.

does not wish known to friends and family;[476] or police create false accounts to investigate political subversives or online child stalkers.[477] Discrediting a Facebook user to family and former friends through malicious fake social networking accounts is criminalized in some jurisdictions under laws of personation and identity theft. The arrest of a New Jersey resident was an event highlighted by Facebook authorities as an opportunity for users to comment on the issue. The tactic garnered 150 responses, most opposed.[478] The story was similarly posted on the American Bar Association website to alert practitioners in criminal law to the difficulty of prosecuting out-of-state offenders as only the states of California and New York have laws specifically banning online identity theft.[479] Such public education aims at deterring fakeries through an emphasis on shaming and the reputational repercussions of crime itself.

ii Exposure by Self

The term "user-generated content" (UGC) describes self-created and self-published online content.[480] It can be distinguished from engineered content from an established authority with a high level of oversight that created credibility with public readers.[481] UGC is the primary source of self-exposure. The myriad forms in which that can occur include photographs, videos, podcasts, articles, and blogs. Social networking is completely user-generated and regenerative, in that they provide hyperlinks to other social network accounts and UGC.

---

[476] Alicia Eler, *Why People Have Fake Facebook Profiles'*, Readwrite (23 Jan. 2012) http://readwrite.com/2012/01/23/why_people_have_fake_facebook_profiles – awesm=~oGOrS2OC.

[477] *Belleville Woman Charged over Facebook Identity Theft,* Facecrooks (27 Oct. 2011) http://facecrooks.com/Internet-Safety-Privacy/Belleville-Woman-Charged-over-Facebook-Identity-Theft.html/ (describing that the woman's fake Facebook profile was alleged to have depicted her ex-boyfriend, a narcotics detective, as a sexual deviant and a drug addict.)

[478] As accessed on Facebook 10 June 2014 at <https://www.facebook.com/Facecrooks/posts/280129868676470.

[479] Mark Hansen, *NJ Woman Can Be Prosecuted Over Fake Facebook Profile, Judge Rules*, ABA JOURNAL (4 Nov. 2011), http://www.abajournal.com/mobile/article/woman_can_be_prosecuted_over_fake_facebook_profile_judge_rules/

[480] Unless the content is dealt with anonymously, in which case attribution becomes a matter of forensic skill.

[481] John Krumm *et al., User Generated Content,* PERVASIVE COMPUTING (Oct. – Dec. 2008), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4653465

UGC is technologically possible due to the Web 2.0 second generation of services that enables user collaboration and sharing.[482] With Web 2.0 our computers and mobile devices become platforms for producing, consuming, exchanging, and remixing data from innumerable sources. Those functions expand our role from content consumer to producer, publisher, critic, journalist, public performer, confidant, commentator, broadcaster and, when our activities cross the boundaries set by law, perpetrator. The cultural ethos behind Web 2.0 is collaboration, cooperation, interactivity, and social networking.[483]

UGC also includes the concept of sourcing from a crowd, or the harnessing of the power of users. For example, with peer-to-peer (P2P) technology every participant becomes a server; the BitTorrent website, for example, promotes itself as offering a protocol[484] that enables users to download files quickly and to upload or distribute parts of them at the same time. BitTorrent is often used for sharing very large and popular files as it is a lot cheaper, faster and more efficient than a commercial download.[485]

The resultant surge in Web 2.0 distribution and sharing of content has both positive effects, such as the empowering of ordinary citizens on a previously unimagined scale, and negative repercussions, including the creation of content that harms the creator's reputation and potentially breaks the law. On the face of it, such self-exposure would seem to have two principal causes: user ignorance of the background mechanics of 'free' online services, or an impetuous response to socializing cues that we later regret or outgrow. Regarding the former, ignorance could be related to unfamiliarity with privacy settings offered by site administrators. For example, when creating a Facebook account, the subscriber is prompted to answer a number of questions regarding intended recipients, specific conditions for sharing, and duration. If those questions are not addressed, the default action is full exposure to anyone who searches the homepage.

---

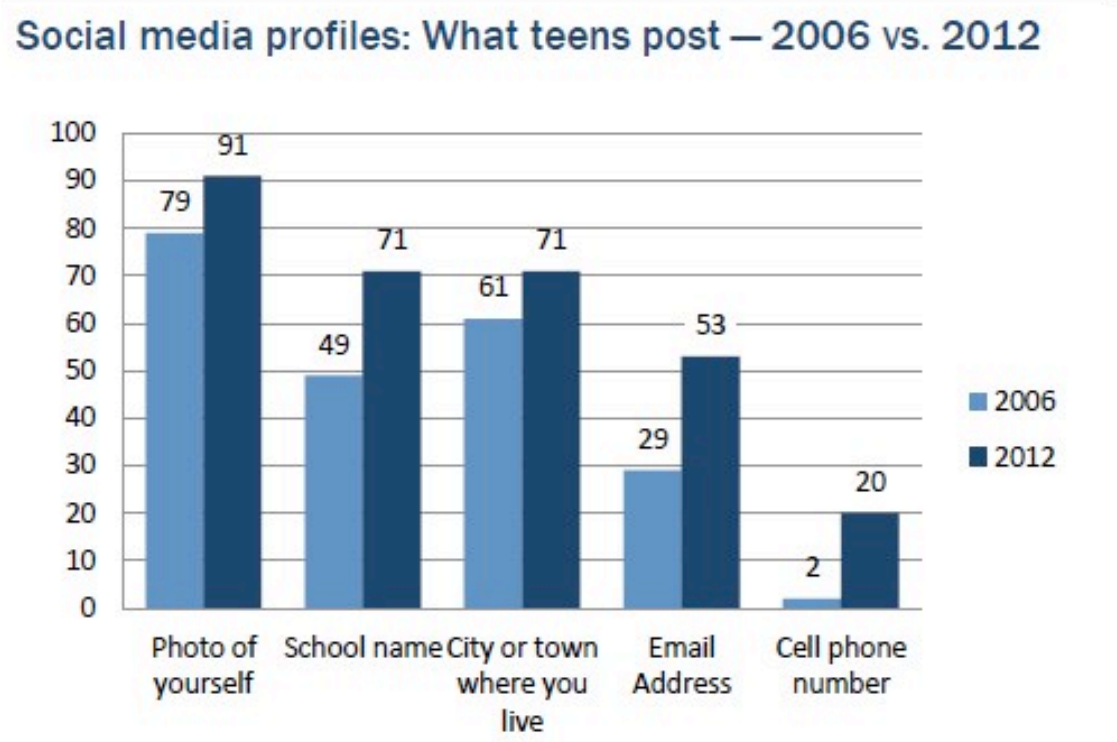
[482] First used by Media Inc., publisher of computer texts and technology-related conferences, under the ownership of Tim O'Reilly in 2004. *See further* Oreillynet.Com, http://www.oreilly.com/pub/au/27 - Biography .

[483] Carlisle George & Jackie Scerri, *Web 2.0 and User-Generated Content: legal challenges in the new frontier,* J. INF., L. & TECH. (JILT) (2007), reporting that one of the most common legal issues regarding UGC is the number of defamatory entries on Wikipedia. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/george_scerri/

[484] A set of guiding rules and procedures.

[485] *A Beginner's Guide to BitTorrent,* http://netforbeginners.about.com/od/peersharing/tp/Torrent-Download-Guide.htm

Adjusting those settings takes thought: studies exist that suggest younger subscribers are more adept at orchestrating such privacy settings, but also increasingly more prone to over-sharing with their circle of 'friends'.[486] In *Figure 2* below, the comparative results of a Pew study of what teens were posting on social media in 2006 and 2012 is presented.



Source: Pew Internet Parent/Teen Privacy Survey, July 26-September 30, 2012. n=802 teens ages 12-17. Interviews were conducted in English and Spanish and on landline and cell phones. Margin of error for results based on teen social media users is +/- 5.1 percentage points. Comparison data for 2006 comes from the Pew Internet Parents & Teens Survey, October 23-November 19, 2006. n=487 teens with a profile online. Margin of error is +/- 5.2 percentage points.

Table 2: Social Media Profiles: what teens post – 2006 vs. 2012

As indicated, teenagers from 12 to 17 are sharing more personal information in all categories than those surveyed six years ago. That change indicates a major shift in

[486] Mary Madden *et al., Teens, Social Media, and Privacy,* Pew Research (21 May 2013), http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/. N=802 in 2012; N=485 in 2006.

attitudes about privacy, particularly regarding photo-sharing which have become the preferred currency of social exchange. The significant surge in sharing email addresses and mobile phone numbers suggests a general relaxation in personal standards of privacy amongst friends. Results were also analyzed along gender and racial lines, with boys showing a higher tendency to share their mobile phone numbers than girls and a less likelihood of African-Americans disclosing their real names on their social media profile than white teens.[487]

Opportunities for exposure are significant: in 2011, for example, 85% of US college students spent an average of 6.2 hours per week on Facebook[488] and 77% of college students in another study used Snapchat on a daily basis during the first few months of 2014.[489] Despite the requirement that all new subscribers to social media sites read and agree to Terms of Use to reduce privacy risks, the attraction of socialization through such platforms and devices seems to cloud the prospect of subsequent regret, embarrassment, or loss of opportunity.

Socio-psychologists question why social media users display a propensity to over-share personal details. A self-reporting study suggests motivations include vanity that exceeds caution, and extroverted needs to maintain social ties.[490] Rather than escaping from or compensating for their offline personality, social networking service (SNS) users appear to extend their offline personalities into the online domain. So extroverts seek out virtual social engagements that "leave behind a behavioral residue in

---

[487] The Pew study sample size for African-American teens was relatively small (n=95), but judged to be statistically significant.

[488] Jamison Barr & Emmy Lugus, *Digital Threats on Campus: Examining the Duty of Colleges to Protect Their Social Networking Students*, 33 W. NEW ENGLAND L. REV., 757, 761 (2011).

[489] Similarly, 77% of US college students use Snapchat on a daily basis, according to a study by New York-based marketing company Sumpto, as reported by Kurt Wagner, *Study finds 77% of College Students use Snapchat Daily*, Mashable.Com (24 Feb. 2014), http://mashable.com/2014/02/24/snapchat-study-college-students/. Study Breaks College Media reported that, of 260 college students polled in the Fall of 2013, 95% used Facebook, 80% tweeted, 73% posted images on Instagram, 48% posted photos on Pinterest, and 40% used Google+. *See further* S. Viner, *Social Media Statistics: How College Students are Using Social Networking*, Study Breaks College Media (7 Feb. 2014), http://studybreakscollegemedia.com/2014/social-media-statistics-how-college-students-are-using-social-networking.

[490] Samuel A. Gosling *et al.*, *Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information*, 14 CYBERPSYCH. BEH. SOC. NETW. 483 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3180765/ .

the form of friends lists and picture postings."[491] The study concludes that, rather than characterizing over-sharing behavior as an escape from reality, SNSs exist as a microcosm of people's larger social worlds.

Such behavior can have therapeutic value as well, especially for emotionally uns or apprehensive individuals.[492] Online interactions offer a non-threatening experience, social bonding, and a buffer for negative feelings in the short.[493] On the other hand, psychological theories of disinhibition and disindividuation, as discussed above, also throw light on the propensity of some SNS users to post selfies in socially questionable situations.[494] Social psychologist John Suler speaks of "toxic disinhibition", the elevated tone or uncharacteristic behaviors exhibited online. In his words,

> We witness rude language, harsh criticisms, anger, hatred, even threats. Or people visit the dark underworld of the Internet—places of pornography, crime, and violence—territory they would never explore in the real world.[495]

And yet to choose not to be on SNSs has its social costs as well.[496] Postings that are too antithetical to the social expectations of our peer communities create exclusion, as was apparently experienced by Canadian teenager Raeteah Parsons when photographs of her alleged gang rape were posted online.[497] Oxford University's Lillian Edwards is more circumspect about the causes of such anguish: she suggests SNSs have become the whipping boy for "almost every possible social blight imaginable by the mass media",

---

[491] *Id.* at 485.

[492] Jonah Berger & Eva Buechel, *Facebook Therapy? Why Do People Share Self-Relevant Content Online?*, SSRN, http://ssrn.com/abstract=2013148.

[493] *Id.* at 3. Berger and Buechel tested 81 participants and found those who were emotionally unstable were more likely to post self-relevant information online.

[494] *See, for example,* Ian Sparks, *Schoolboy French journalists annoy White House staff by taking selfies while covering Francois Hollande's U.S. visit*, DAILY MAIL (13 Feb. 2014), http://www.dailymail.co.uk/news/article-2558620/French-journalists-annoy-White-House-staff-taking-selfies-covering-Francois-Hollandes-U-S-visit.html; *Duquesne cancels Rivera over 'selfie'*, DUQUESNE STUDENT MEDIA (15 Sept. 2013)detailing the cancellation of Geraldo Rivera of Fox News as a participant in a Duquesne University symposium due to a shirtless posted 'selfie' on Twitter; Judith Soal, *Barack Obama and David Cameron pose for selfie with Danish PM*, GUARDIAN (11 Dec. 2013), http://www.theguardian.com/world/2013/dec/10/nelson-mandela-world-leaders-selfie(suggesting 'selfie' of Obama and other heads of state at Nelson Mandela's funeral created diplomatic embarrassment at high levels).

[495] Suler, *supra* fn 434 at 321.

[496] Edwards, Privacy, *supra* fn 469.

[497] Kevin Dolak, *Rehtaeh Parsons Suicide: Justice Minister Revisiting Alleged Rape Case*, ABC NEWS (11 Apr. 2013), http://abcnews.go.com/International/rehtaeh-parsons-suicide-justice-minister-revisiting-alleged-rape/story?id=18924592.

especially in relation to young people, from encouraging social predators and sexual grooming to inciting and enabling fraud, deception, stalking, harassment, bullying, abuse and victimization. SNSs are also blamed for "encouraging young people to inflict antisocial behavior on each other."[498]

The trade-off for social media companies offering convenient technologies is the use of our content for marketing purposes. For example, Facebook Terms of Use claim that subscribers own all personal information they post on their profile page, including photographs. That statement contradicts another Facebook provision that, upon subscribing, users "grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any intellectual property (IP) content that you post on or in connection with Facebook'.[499] That IP License should end when you delete your content, except for third party access that is not retrievable and probably has been retransmitted to unknown recipients.

SNSs also freely use the email addresses of subscribers and their 'friends' to inform them about new content postings, endorsements, and changes in location. Facebook and LinkedIn subscribers receive an average of two emails per day notifying them of new endorsements or postings by friends. That routine has been challenged in a San Jose, California district court regarding the practice of professional networking site LinkedIn to send several sequential emails to friends of its subscribers, inviting them to endorse those subscribers.[500] The judgment determined that, while the initial email is on consent from the account holder as per the terms of the user agreement, subsequent requests are not. Those emails could injure users' reputations by giving the impression they are harassing their contacts or that they are the type of people who spam their contacts.[501]

In contrast, the same San Jose judge denied certification for a class action against Google Inc. that would have marked the largest class action case in US litigation history. The complainants were disgruntled email users who accused Google

---

[498] Edwards, *supra* fn 469 at 7.
[499] *Statement of Rights and Responsibilities,* Facebook, https://www.facebook.com/legal/terms.
[500] Jonathan Stempel, *LinkedIn must face customer lawsuit over e-mail addresses,* GLOBE AND MAIL (13 June 2014) http://www.reuters.com/article/2014/06/13/linkedin-lawsuit-idUSL2N0OU0LB20140613 .
[501] *Perkins v. LinkedIn Corp.,* Case No. 13-cv-04303, U.S. District Court, Northern District of California (San Jose).

of intercepting, reading, and mining the content of their email messages.[502] The Court denied certification on the basis that consent is an individually determined matter and cannot be pleaded on a class action basis. Similar cases accusing Yahoo!, Facebook, and Hulu of monetizing personal content for an online advertising market are pending.[503]

iii Exposure by Journalists

The speed of news coverage is also accelerating to meet viewer demand for social media as a source of up-to-the-minute journalism. Mainstream news services, such as major television networks, have responded by using software to incorporate social media reports, via Twitter and Facebook, into their real time news broadcasts.[504] Such media integration allows more accurate and timely coverage from the field, as seen in the 2011 Tsunami in Japan, and the 2013 US presidential elections. A 'social media newsroom' is evolving where journalists develop stories by engaging with communities on Twitter, YouTube, Google+ and anyone with an Internet connection. Those sources then feed into live onscreen television coverage, along with items from news services like Reuters and newspapers such as the New York Times, Le Monde or The Guardian. [505] That integrated approach maintains the impression that major networks remain the official information source.

Digital news media has expanded from a corporate-controlled entity to unmediated citizen journalism. That shift raises the risk of hyperbole, inflammatory speech, and libelous commentary. In addition, a declining readership and failing economic model of traditional newsrooms puts into question the ongoing viability of a mass media based on advertising and circulation. In response, many journalists have created non-profit news sites seeking support from foundations and viewer donations.

---

[502] *Re Google Inc. Gmail Litigation*, Case No. 13-md-02430, U.S. District Court, Northern District of California (San Jose).
[503] Joel Rosenblatt, *Google Won't Face Group E-Mail Privacy Lawsuit: Judge*, BLOOMBERG (19 Mar. 2014) http://www.bloomberg.com/news/2014-03-19/google-won-t-face-group-e-mail-privacy-lawsuit-judge-rules.html.
[504] Grant Buckler, *Breaking a story with the speed of social media*, GLOBE AND MAIL (1 Dec. 2011), http://www.theglobeandmail.com/report-on-business/small-business/sb-digital/biz-categories-technology/breaking-a-story-with-the-speed-of-social-media/article4179877/ .
[505] Denisa Dzunkova, *Storyful Helps News Organizations Monitor Social Media*, PBS MEDIASHIFT, http://www.pbs.org/mediashift/2013/02/storyful-helps-news-organizations-monitor-social-media036/.

Such entrepreneurial journalism challenges journalistic standards of impartial coverage. Equally at risk in this new arrangement are journalistic reputations.

b Disclosure Harms and Case Studies

This section will detail the three most prevalent opportunities for disclosure of personal information generated online: the mishandling of Big Data; activities of data brokers; and the refusal of take-down orders. Reports of studies and cases will be used throughout to illustrate key principles and to personalize the harm to reputation suffered as a result.

i Mishandling of Big Data

Big Data can be defined as data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process within a tolerably elapsed time.[506] Descriptions of Big Data capabilities and collections are replete with awe-inspiring quantifiers, as seen in this excerpt from Science Magazine in 2011:

> Data sets grow in size in part because they are increasingly being gathered by ubiquitous information-sensing mobile devices, aerial sensory technologies (remote sensing), software logs, cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks. The world's technological per-capita capacity to store information has roughly doubled every 40 months since the 1980s; as of 2012, every day 2.5 exabytes (2.5×1018) of data were created.[507]

The terms 'exponential' and 'ubiquitous', so favoured by researchers of Big Data, are inadequate to describe the size of the data collection activities that infuse our daily lives. Authors Mayer-Schönberger and Cukier suggest that, with the onslaught of such 'datafication' of our every move and preference, the entire gestalt of information collection and analysis has altered:

> In the spirit of Google or Facebook, the new thinking is that people are the sum of their social relationships, online interactions and connections with content. In order to fully investigate an individual, analysts need to look at the widest

[506] Chris Snijders *et al., Big Data': Big gaps of knowledge in the field of Internet*, 7 INT'L J. INT. SCI., 1, http://www.ijis.net/ijis7_1/ijis7_1_editorial.html.
[507] Martin Hilbert Priscila Lopez, *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE, 60 (2011).

> possible penumbra of data that surrounds the person — not just whom they know, but whom those people know too, and so on.[508]

The authors speak of entrepreneurs of Big Data having a big data mindset', devoted to the belief that certain data can be mined to reveal valuable secrets.[509] From that vantage, data gains in optional value as it is put to new purposes. The authors examine the three components of the Big Data enterprise within such industries as pharmaceuticals, financial services, and manufacturing: the collector of the information; those skilled with data; and the innovators who can foresee the novel ways that data can lead us to new information. The latter professionals are in most demand as they have the ability to extract wisdom from banks of raw data.[510] Their innovations are anticipated by political and financial leaders who have watched the bulk of manufacturing migrate to developing parts of the world. The good news that Mayer-Schönberger and Cukier can offer about Big Data is that, for the present, firms will gain by tapping data in clever ways.[511] Benign examples they offer include Google search algorithm's use of subscriber data for behavioral advertising, and Germany's use of car parts data to improve automobile components.[512] Market research as well is greatly advanced by Big Data analysis: the authors speak of the discovery by Walmart stores, through data analysis of their sales patterns, that customers purchase Pop-Tarts in greatly increased numbers just before a hurricane. That information was used to position Pop-Tarts beside flashlights and other emergency products in hurricane-prone locations with favourable sales results.[513]

The risks associated with the autonomous compilation of Big Data are many. For instance, state espionage agencies are no longer our major intruders: that distinction goes to our neighbours, service providers, and retailers. A second shift is that privacy has become a dominant social good that counters values of free speech,

---

[508] VIKTOR MAYER-SCHÖNBERGER AND KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).
[509] *Id.* at 124.
[510] *Id.* at 125.
[511] *Id.* at 149.
[512] *Id.* The authors observe that Big Data collection exaggerates a firm's strengths and weaknesses.
[513] Michiko Kakutani, *Watched by the Web: Surveillance is Reborn*, NYTIMES Book Review (10 June 2013), http://www.nytimes.com/2013/06/11/books/big-data-by-viktor-mayer-schonberger-and-kenneth-cukier.html?pagewanted=all&_r=0.

including commercial free speech or enterprise. As well, big data analytics means we are judged more by propensities, and by indicated preferences, than by completed acts.[514] Amazon and Netflix think they know more about our next consumer selections than we do from data that is autonomously collected each time we browse a book or movie online. Prediction and pre-supposition have supplanted analysis of done deeds.

Big Data use is encouraged by free storage costs and unlimited space, surgically adept technologies, and all the idiosyncrasies of the Internet we have listed above (section 3.1). While not all collected data is personal, such as algorithms that deliver better-refined oil or more precise predictions about airport weather, the triangulation of seemingly disparate bits of data can produce conclusions about individuals that could be personally devastating. A simple example is the autonomous correlation of three bits of information that could lead a potential employer to conclude (erroneously) that a job applicant has a fatal illness: 1) she has contributed to a Run for the Cure in the past; 2) she visited Princess Margaret Cancer Care Hospital twice over the past two years; and 3) she has conducted online search queries on vitamin therapy in the past year. Under such informational scrutiny, former US President Woodrow Wilson would never have been permitted to complete his last term due to a stroke he suffered, known at the time only to his personal physician and his wife.[515]

As an indication of public awareness of reputational risks associated with Big Data collection, three in five British citizens believe the general public has lost control of the way its personal information is collected and processed by others.[516] Those results are included in a 2013 study reported to the United Kingdom's Information Commissioner's Office (ICO) that also found 88% of respondents listed the protection of people's personal information as the most urgent issue affecting the public at the hands of government.[517] As if to substantiate those fears, two incidents of inadvertent

[514] *Id.*
[515] Michael Alison Chandler, *A President's Illness Kept Under Wraps*, WASH. POST (3 Feb. 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/02/02/AR2007020201698.html.
[516] Annual tracking of the ICO has measured public awareness of the Data Protection Act (DPA) since 1997 and Freedom of Information Act (FOIA) since 2003. The study cited the United Kingdom's state-run National Health Service as the repository of personal information most at risk (p. 5).
[517] N=2,500.

disclosure of sensitive personal data involving EU citizens were reported within months of the ICO study.

In the first, German language news service Neue Zurcher Zeitung reported the anonymous delivery to its editorial staff of data tapes belonging to Swisscom, a Switzerland-based telecommunications provider. The tapes contained private employee data from 2008 to 2010, including 14,500 emails from Swisscom employees, 600,000 phone numbers, and other private and business contract details.[518] Specifically, the NZZ claimed its editorial office was in possession of four data tapes originating from Swisscom data centres. Swisscom immediately filed a criminal complaint against persons unknown for data theft. The NZZ went on to analyze the data further and revealed the names of a number of customers in a subsequent article in 2013. Swisscom sought an injunction against further publication, arguing the ongoing release of such personally identifying customer data served no public interest. Not all data sets were checked, however. Swisscom took the view that a comprehensive and time-consuming check of all data sets, which in total contain more than a terabyte of data, was "not expedient", even though it could have allayed fears of its customers.[519] That decision left much personally identifying data open to data theft or other exposure, so Swisscom eventually demanded that the NZZ release and destroy the data still in its possession.[520]

The second incident involved the Bank of Scotland's erroneous misdirection of faxes to an unsuspecting third party several times over a four-year period that contained sensitive customer data. Home addresses and telephone numbers were disclosed, along with pay-slips, bank statements, account details, and mortgage applications.[521] The documents' misdirection was caused by staff error in using a fax number one digit

---

[518] Adam Greenberg, *Telecommunications provider Swisscom investigations stolen data,* SC MAGAZINE FOR IT SECURITY PROFESSIONALS (18 Sept. 2013),

[519] *Judge Rules on Temporary Injunction,* Swisscom (14 Feb. 2014), http://www.swisscom.ch/en/about/medien/press-releases/http://www.washingtonpost.com/wp-dyn/content/article/2007/02/02/AR2007020201698.html/.

[520] *Id.*

[521] B. Davidson, *Bank of Scotland Receives 75K GBP Penalty Notice for Misdirected Faxes,* PRIVACY ADVISOR (IAPP) (27 Aug. 2013) https://privacyassociation.org/news/a/uk-bank-of-scotland-receives-75k-gbp-penalty-notice-for-misdirected-faxes ; *Bank of Scotland Fax Blunder leads to Fine,* BBC NEWS (5 Aug. 2013) http://www.bbc.co.uk/news/business-23572574. Although the Berne Commercial Court has now overturned the injunction, it clearly states in its reasons for judgment that any further piecemeal publication of information gained from these data tapes may constitute a breach of the *Swiss Unfair Competition Act*.

different than the one intended. The receiving organization first alerted the bank to its error in February of 2009, but the bank continued to send out the private information over three more years. When reported, the lack of response by the Bank of Scotland prompted a report to the ICO; the subsequent investigation revealed that a further 10 documents went to a member of the public due to another faxing error. The ICO official commented that sending a person's private financial records to the wrong fax number once was careless but 'to do so continually over a three year period, despite being aware of the problem, is unforgiveable' and in clear breach of data protection legislation.[522] No further action was taken against the bank.

ii Studies of Big Data Vulnerability

Both incidents highlight the growing vulnerability of Internet users to careless disclosure of their sensitive information to third parties despite legislative efforts to curb such activity. Similar disclosure dangers related to the use of mobile devices is reflected in opinions expressed in a 2010 Eurobarometer study.[523] Nine of ten Europeans reported their concern about mobile applications collecting their data without their consent, and seven Europeans of ten expressed concern about the potential use that companies might make of the information disclosed.[524]

Our vulnerability at the hands of institutional and corporate data collection practices and analysis is also alarming. Through use of de-anonymizing technology and the combination of seemingly discrete bits of information,[525] data analysts can unearth very private information. For example, we have been told that our gender and sexual preferences can now be ascertained from a mere examination of our use of the 'like' function on Facebook.[526] Similarly we have been alerted that we are only four mobile phone conversations away from government identification.[527]

---

[522] Christopher Williams, *Bank of Scotland fined for 'unforgivable' fax blunder*, TELEGRAPH (5 Aug. 2013), http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10223435/Bank-of-Scotland-fined-for-unforgivable-fax-blunder.html. The Bank was ultimately fined 75,000 pounds by ICO authorities.

[523] *Attitudes on Data Protection and Electronic Identity in the European Union,* Flash Eurobarometer 359 (June 2011), http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[524] *Id.*

[525] Daniel J. Solove, Scalia, *supra* fn 365.

[526] Rebecca Rosen, *Armed with Facebook 'Likes" Alone, Researchers Can tell Your Race Gender and Sexual Orientation*, ATLANTIC (12 Mar. 2013)

The degree of apprehension on the part of citizens appears to differ from one side of the Atlantic to the other. A survey of Internet users in the US found a much lower level of alarm than in the EU: despite revelations in 2013 that the NSA has been monitoring Americans' activities online and increasing backdoor access to Internet and telephone records, US Internet users appeared not as concerned as British citizens about the government having access to their home computers or email accounts, nor as concerned as other Americans had been in 2000. Only 35% of Americans expressed concern in 2013, compared with 47% in 2000.[528] Concerns were higher for software that enabled governments to tap into all Internet email searching for incriminating information of any type (51% in 2013 compared to 63% in 2000). Study analysts suggest that US Internet users might be more resigned to the idea that, in an advanced technological age, monitoring is inevitable whereas in 2000, the relatively new medium of the Internet "might have caused more concern about privacy than today when 87% of Americans use the Web."[529] The study report also suggested that Americans might be less concerned because they support the government's pursuit of foreign or domestic targets suspected of terrorism. The discrepancy might also be explained by the fact that America was the site of the 9/11 terrorist attacks, although England has suffered a chronicle of discrete national security incidents as well. Further study into this discrepancy holds promise for understanding public awareness of disclosure risks.

When it comes to users' knowledge of remedies for the harms of data disclosure, a 2013 study by the EU Fundamental Rights Agency (the FRA Study) determined that only a third of EU citizens were even aware of their right to data protection[530] or of the existence of Data Protection Authorities (DPAs) within their country to assist them in

---

http://www.theatlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-and-sexual-orientation/273963/

[527] Matt Warman, *Online anonymity: impossible after four phone calls,* TELEGRAPH (25 Mar. 2013) http://www.telegraph.co.uk/technology/news/9952841/Online-anonymity-impossible-after-four-phone-calls.html .

[528] *U.S. Internet Users Less Concerned About Gov't Snooping,* Gallup Report http://www.gallup.com/poll/165569/internet-users-less-concerned-gov-snooping.aspx(telephone interviews from 3-6 Oct. 2013, n= 887 Internet users, aged 18 and older, living in all 50 US states.

[529] *Id.*

[530] *Access to data protection remedies in EU Member States,* 2013 Report of the European Union Agency For Fundamental Rights, Publications Office of the European Union: Luxembourg (14 Mar. 2014), http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf (FRA Study).

accessing those protections.[531] The FRA study also found a significant lack of legal expertise in the privacy and data protection fields.[532] The policy context for the study was built around two fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union (The Charter): the right to the protection of personal data (Article 8)[533] and the right to an effective remedy before a tribunal (Article 47).[534] Most data protection violations in EU Member States were found to arise from Internet based activities, direct marketing and video surveillance with closed circuit television cameras.

FRA study participants in Europe stated they were aware of the following sources of Internet violations: social media, leakage of personal data from e-shopping sites, hacking of email accounts and databases, identity theft, security breaches and misuse of personal data by global Internet companies. Of particular concern were unauthorized data transfers of personally identifiable information from data controllers (employers, public authorities, Internet service companies, mobile operators, credit companies) to unauthorized third parties (such as online commercial enterprises and debt collection companies); nonconsensual data retention by police, other government agencies, and supermarkets; and unauthorized disclosure by the justice system of confidential personal data from criminal and divorce proceedings to the media and Internet sites.[535] Victims stated they became aware of the disclosure violations by receiving marketing emails and other spam, experiencing difficulty when accessing their

---

[531] *Id.* Methodology included a comparative analysis of the national legal frameworks in the area of data protection remedies and qualitative research in the following 16 EU Member States: Austria, Bulgaria, the Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland, Portugal, Romania, Spain and the United Kingdom. N=700, including alleged victims of data protection violations, judges, staff of DPAs, intermediaries, and lawyers.

[532] The FRA study confirmed findings of a 2011 Eurobarometer survey conducted by the European Commission on *Attitudes on data protection and electronic identity in the European Union,* that most of the Europeans (74 %) surveyed saw disclosing personal information as an increasing part of modern life. In addition, 70% expressed concern that their personal data held by companies might be used for a purpose other than that for which it was collected.

[533] As distinguished from the Charter's right to private life (Article 7).

[534] Charter Of Fundamental Rights Of The European Union, 2010/C 83/02, EC 2012/C 326/02 (final 26 October 2012) (the Charter) codifies all rights found in 1) the case law of the CJEU; 2) the European Convention on Human Rights (ECHR); and 3) other rights resulting from the common constitutional traditions of EU countries and other international instruments.

[535] *Id.* at 26.

online banking accounts or government websites, and discovering that personal data had been conveyed to third parties that were outdated, inaccurate, or false.[536]

A study of Americans reveals more public acceptance of Big Data practices. A 2012 Pew Internet/Elon University survey of American Internet experts, observers and stakeholders[537] measured opinions about the potential impact of human and machine analysis of newly emerging large data sets in the years ahead. The study revealed that US users are less pessimistic or suspicious about Internet data collection at the hands of authorities. Some 53% of those surveyed predicted that the rise of Big Data is likely to be "a huge positive for society in nearly all respects" by the year 2020. Respondents predicted that the continuing development of real-time data analysis and enhanced pattern recognition could bring "revolutionary change to personal life, to the business world and to government."[538] For the 39% of participants who stated they saw Big Data as more menacing in the hands of unauthorized authorities, concerns included the fact that governments and businesses had their own agenda for the use of Big Data, worries about the shortage of human analysts qualified to sort data, and the possibility that data could be manipulated or misread.[539]

In summary, all studies indicate a much more acute awareness by individuals of the misuse of personal information by authorities in the UK, and a lower level of concern, declining considerably over 15 years, by US participants. EU data protection laws are more harmonized and offer more direct supervision; for example, Internet Protocol addresses in the EU are considered personally identifiable information (PII) and hence merit privacy protection. In contrast, PII protection is localized in the US, depending for protection on the laws within each jurisdiction. Citizens in both jurisdictions reveal ignorance about available laws or remedies dealing with informational disclosure. Once victimized, however, the FRA study participants articulate a variety of psychological and social repercussions.

They described various personal harms from data disclosure, including emotional distress, feeling offended, experiencing insecurity or damage to reputation, as

---

[536] *Id.* at 27.
[537] *The Future of Big Data,* Pew Research (20 July 2012), http://www.pewinternet.org/2012/07/20/the-future-of-big-data-2/. (N=1,021; online survey).
[538] *Id.*
[539] FRA Study, *supra* fn 530.

well as the impact on their relations with other people.[540] The overwhelming majority of interviewees mentioned disturbance of daily life, the pressure of defamation suits, disappointment due to misplaced confidence, shock, fear, feelings of injustice, humiliation, and a sense of dispossession or lack of control over their own data. Financial damages were also mentioned but less frequently. Most interviewees sought remedies, such as lodging complaints with the national Data Protection Authorities (DPAs). Very few went through judicial procedures because of the lengthy and time consuming process, the complexity of procedures, and the high costs involved. Judges and practising lawyers involved in the study shared that view. Reasons for preferring to lodge complaints with national DPAs rather than seeking court remedies were again cost related: the complaint procedure was shorter and less complex, and the procedure did not demand legal representation. Hopes for outcomes included fixing an unjust situation, correcting damage to identity or image, clarifying wrong records, rectification or deletion of personal data, achieving rehabilitation, imposing sanctions against violators and stopping the abuse of power and excessive unlawful control by employers. An even greater share of respondents wanted to minimize a possible risk of other individuals becoming a victim of data protection violations. They most commonly mentioned prevention of future violations of rights, awareness raising, standing up for fundamental rights, teaching a lesson to concerned authorities, obtaining an acknowledgement of the violation from a competent authority, or imposing a sanction on the perpetrator.[541]

iii Data Brokers

Another source of data leakage or non-consensual retention is the activity of data brokers. Data brokers either collect or buy Big Data containing personal data and exchange it or sell it to others for purposes of identity verification, marketing of products, and fraud detection. In a 2014 report of a study into the activities of nine representative data brokers, the Federal Trade Commission (FTC) found that, while there are consumer benefits from data broker practices, there are exposure issues as

[540] *Id.*
[541] *Id.* at 29.

well.[542] Data brokers conduct consumer profiling to such an extent that they often know as much, or more, about us than our family and friends, including our online and in-store purchases, our political and religious affiliations, our income, and our socio-economic status.

The primary risk to consumers is that the information held by data brokers is often outdated, inaccurate, or collected or retained without the consent of the data subject. The example the study gives deals with 'Biker Enthusiasts.'[543] If the profile crafted from your PII places you in that category, you can expect to be targeted for road gear, bike discounts and helmet advertisements. However, insurance companies might use your interest in motorcycles to make a calculation about your inclination to engage in 'risky behavior' and your premiums would be higher than those of your non-biking enthusiast neighbour. Data brokers often store the data 'indefinitely' and use it for numerous unidentified purposes, practices that concern the FTC.[544]

The non-consensual retransmission of personal data still occurs. For example, within the health care system, doctors working under government funded health systems make PII details of our visits available, through our health plan numbers, to third parties or to governments for billing purposes. Within government-funded healthcare systems, our health information is tied to our health plan number. Those data might be retained far beyond the limits of our consent, perhaps because, as Lawrence Lessig has suggested, it is cheaper and administratively simpler to "push the save, rather than the delete button".[545] Such data might also be shared with other departments of government or with third parties without our knowledge or consent. For those privately insured, the network of data receivers might extend to third parties within and outside the hospital. For example, the hospitals we attend for procedures at the advice of our family doctor are likely to have provided our contact data to fundraising personnel within their organization or to business enterprises to whom that

---

[542] *Data Brokers: A Call for Transparency and Accountability,* Federal Trade Commission study (May 2014), http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. (including the following data brokers: Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future).
[543] *Id.* at vi.
[544] *Id.*
[545] Lawrence Lessig, *Against Transparency,* NEW REPUBLIC (20 Oct. 2009), http://www.newrepublic.com/article/books-and-arts/against-transparency

function is outsourced.[546] The pharmacy that fills our doctor's prescription might pass along our prescription information to pharmaceutical manufacturers, and their researcher staff, whose products they sell.[547] Those data reveal which drugs doctors are prescribing and from which manufacturers, information of significant marketing value to competitors. Pharmacies claim no harm is done because the data is anonymous as to patients' names. As we know, current data forensic capabilities include de-anonymizing practices.[548] The pharmacy might, in turn, sell our information to data brokers that, in turn, sell it to a widening network of pharmaceutical and biotechnology companies, consulting firms, advertising agencies, government bodies, and financial firms.[549]

One author relates the dilemma over PII control to four idiosyncrasies of the Internet: its convergence capabilities, scale, volume, and individual empowerment.[550] Convergence refers to the process by which media content is increasingly being unbundled from its traditional distribution platforms so it can find many paths to the consumers. As a result, it is now possible to disseminate, find, or consume the same content using many devices or distribution networks, a capability that complicates efforts to control information flow. The scale of that activity has burgeoned due to the elimination of geographic, technological, and cultural-language barriers. As discussed,

---

[546] Patients at Toronto's largest cancer care facility, Princess Margaret Hospital routinely receive promotional material on the hospital's largest fundraising event, the annual Princess Margaret Home Lottery. Patient consent is not obtained for promotional mail-outs, so contact information must be generated by the hospital through its patient files.

[547] *See, for example, Sorrell v. IMS Health Inc.*, No. 10-779 131 S.C. 2653 (2011) (detailing such practices in the US. The US Supreme Court held, however, that a Vermont statute restricting the sale, disclosure, and use of records that revealed the prescribing practices of individual doctors violated the First Amendment.)

[548] *See* Adam Tanner, *Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study,* FORBES (25 April 2013), http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/ (illustrating how the researcher was able to identify 40% of study participants from three pieces of information: zip code, date of birth, and gender. Disclosed date included abortions, illegal drug use, alcoholism, depression, sexually transmitted diseases, medications and the participants' DNA sequence.)

[549] The American pharmaceutical company involved in the *Sorrell* case, IMS Health, reports that it has assembled '85% of the world's prescriptions by sales revenue and approximately 400 million comprehensive, longitudinal, anonymous patient records'. *See* Adam Tanner, A. *Company That Knows What Drugs Everyone Takes is Going Public*, FORBES (6 Jan. 2014) http://www.forbes.com/sites/adamtanner/2014/01/06/company-that-knows-what-drugs-everyone-takes-going-public/.

[550] Adam Thierer, *Privacy as an Information Control Regime: the challenges ahead*, TECH. LIB. FRONT (13 Nov. 2010), http://techliberation.com/2010/11/13/privacy-as-an-information-control-regime-the-challenges-ahead/.

the lack of a central Internet regulatory agency in the US reduces the effective monitoring of online data sharing. Regulators would be faced with a monumental task because, as Internet scholar Adam Thierer observes, "there is just too much stuff for regulators to police today relative to the past."[551]

iv Cookies

Cookies are used to track web site activity.[552] When you visit some sites, the server leaves a cookie onto your site that acts as your identification card. Upon each return visit to that site, your browser passes the cookie back to the server. This allows a web server to gather information about which web pages are used the most, and which pages are gathering the most repeat traffic. Cookies are also used for online shopping. Online stores often use cookies that record any personal information you enter, as well as any items in your electronic shopping cart, so that you don't need to re-enter this information each time you visit the site.

Webmasters can track access to their sites, but cookies facilitate that function. In some cases, cookies come from advertising companies that manage the banner or sidebar ads for a set of sites. That access allows advertising companies to develop detailed profiles of the people who select ads across their customers' sites. Such access carries privacy issues. They also have more benign uses, however, such as providing research data for determining how search queries can be interpreted by a search company to best respond to your queries. Ron Dolin provides the example of a search site trying to decipher the best results to return for a 'GM' search which, depending on the language of the person conducting the query, could mean a brand of automobile, "genetically modified" food, "guerre mondial" or world war in French, and so on.[553] Internet companies justify the use of cookies in such functions as ultimately improving customer service. The autonomously generated notices on some sites that cookies are

---

[551] *Id.*

[552] This paragraph is informed by 'What are cookies?' Knowledge Base, Indiana University, https://kb.iu.edu/d/agwm.

[553] Ron A. Dolin, *Search Query Privacy: The Problem of Anonymization'* 2 HASTINGS SCI. & TECH. J. 137, 142-143 (2013), (citing P. Haar & S. Baker, *Making search better in Catalonia, Estonia, and everywhere else*, Google Blog (25 Mar. 2008) http://googlepublicpolicy.blogspot.com/2008/03/making-search-better-in-catalonia.html.

being employed is an indication that authorities are responding to user concerns about their invasive potential.

v Lingering Data, Autocorrection & the Power of Internet Companies

There is a divergence in opinion concerning the permanence of collected data within archival spaces on the Internet. That discrepancy creates uncertainty around the continuing accessibility of harmful content to third parties, even once a claim in defamation is successful.[554] Within the EU, there is a tradition in many Member States of expunging court records as of right once the sentence has been completely served. In most American jurisdictions, however, records are treated as part of the historical court record and data subjects can apply for a pardon, but criminal records do not autonomously expire when sentences are completed. That practice runs counter to the rhetoric in America of second chances and new beginnings. In many jurisdictions, while records might be removed from immediate public view, they still reside in archival spaces for future reference.

The US National Association of Criminal Defense Lawyers (NACDL) produced a 2014 report on the erosion of rights and status of convicted persons due to the persistence in online spaces of their criminal records. The report cites incidents where a total of 65 million Americans by 2008, or one in four, had lingering criminal records on file within the states people in America.[555] Those "collateral consequences" can create such significant reputational stigma as voting bans, immigration status issues, parental rights limitations, unfavourable credit ratings, problems in obtaining or using passports, as well as diminishment of employment opportunities and benefit eligibility.[556] Interestingly, the NACDL report refers to the 'stigmatization' and 'second class legal citizenship' of those with persistent criminal records,[557] but does not identify

[554] As was noted in the Mosley case where the plaintiff's vigilance led to the launching of over 20 lawsuits after his success with the British system.
[555] *65 Million Need Not Apply: The Case for Reforming Criminal Background Checks For Employment*, The National Employment Law Project 27, fn 2 (March 2011), http://www.nelp.org/page/-/65_Million_Need_Not_Apply.pdf; Us Bureau Of Justice Statistics, *Survey Of State Criminal History Information Systems* (2008), Table 1 (Oct. 2009).
[556] *In Search of Second Chances*, NYTIMES Op. Ed. (1 June 2014) SR-10.
[557] Referring to the ancillary statutes and regulations that provide a "half-hidden network of legal penalties, debarments, and disabilities" more lasting than the original penal sanctions, at 9.

them as harms to reputation. Among the report's recommendations is the retention of criminal records only if criminal conduct is recent and directly related to a particular benefit or opportunity.

Unless educated in the subject, the individual user is unaware of the nature and extent of stored data and of how Internet companies can misrepresent the workings of security features that they promote as privacy features. Several FTC cases involving Internet companies that have been sanctioned illustrate the myriad ways Internet companies can mislead individual users. I set out three below.

FTC v. Google Buzz

In the first case, Google created a new social networking service called Google Buzz in 2010 by linking its Gmail subscribers with each other without their knowledge.[558] The link was promoted as enabling subscribers to share updates, comments, photos, videos, and other information through posts or 'buzzes'. Google populated the Google Buzz network by gleaning personal data from profiles and other required information when users first subscribed to Gmail.[559] Without prior notice or the opportunity to consent, Gmail users were automatically linked with unknown 'followers' who had access to personal details of their account. When a user logged on, she could either choose to check out those users or go straight to her inbox. If she chose the latter, she could still be followed by all other users of Gmail who had been enrolled in Buzz, and without her knowledge; as well, a Buzz link would appear in the list of links on the margins of her Gmail page. If she clicked on that link, she would be taken to the Buzz welcome screen and automatically enrolled in Buzz, without any disclosure of that fact and without any further action on her part. In 2012, Google was discovered to be actively releasing cookies or other architecturally-altering programs into users' devices in order to extract more user information.

FTC v. Snapchat

The second group of cases involved the nonconsensual transfer and sale of subscribers' personal information. Snapchat is an application enabling users to share

[558] *United States v. Google Buzz* (FTC File 102 3136) https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.
[559] First and last names, photos, friends and their and email contacts, for example.

photos, record videos, text and drawings. It was found in 2014 to be misrepresenting to users the extent to which those features compiled their personal data and that of their recipients.[560] Similarly, in 2012 Myspace was found to be passing along users' personally identifiable to advertisers with whom they had information exchange contracts.[561] Those recipients, in turn, could sell such information to other advertisers unknown to Myspace or the users. Facebook and Google were prosecuted for similar invasive practices.

Snapchat was also found to have misrepresented the expiry feature of their photographs. In *United States v. Snapchat*[562], the defendant company used as a main marketing feature the 'ephemeral' nature of 'snaps'.[563] Snapchat claimed the user could pre-set the duration of each post, after which content would 'disappear forever' from both the sender's and recipient's device. Despite Snapchat's claims, the FTC complained of several ways that recipients could archive the content and continue to transmit it to third parties. Consumers could, for example, use third-party applications to log into the Snapchat service. Because the service's deletion feature only functions in the official Snapchat application, recipients could use these widely available applications to view and save snaps indefinitely. Indicative of the popularity of such applications is the report that they have been downloaded millions of times.[564] Despite a security researcher warning the company about this possibility, the complaint alleges, Snapchat continued to misrepresent expiry times.

In addition, the complaint alleged that any recipient could preserve content indefinitely by taking a screenshot, and that the company transmitted the user's geolocation if an Android system were used, despite its denial of the same in its privacy policy. The FTC complaint also alleges that Snapchat collected iOS users' contacts information from their address books without notice or consent.

---

[560] *United States v. Snapchat,* FTC File 132 3078, https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf .

[561] Such as Fox Advertising Network. Fox in turn would pass on user personal data if it did not have immediate advertising needs. Both of those activities violated MySpace privacy policies. The de-encrypted data contained, at a minimum, the user's full name, email address, date of birth, and gender.

[562] *FTC and Snapchat Inc.,* (FTC File 140 508).

[563] *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False',* FTC Press Release (8 May 2014) https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf .

[564] *Id.*

FTC v. Google

The third type of case[565] involved Google bypassing Apple users' privacy settings by placing cookies on their computers.[566] Specifically, Google used computer code to gain access, through Apple's Safari Web browser, to user data that it then monitored via cookies.[567] Safari, the most widely used browser on mobile devices, is designed to block such tracking by default. The technique reaches far beyond those websites, however, because once the coding is activated, it can enable Google tracking across the vast majority of websites. The findings appear to contradict some of Google's own instructions to Safari users on how to avoid tracking as contained in their online privacy policies. Until recently, one Google site told Safari users they could rely on Safari's privacy settings to prevent tracking by Google. Google defended its actions by stating that the cookies were only passively collecting personal information. Google continued to implant cookies even where users explicitly requested that no cookies be used. The FTC fine for that activity was 22.5 million, the highest monetary penalty ordered by the regulator against an Internet company.[568]

Autocorrection

One final feature within the control of the Internet company and its designers, that of autocorrection (and its correlate autosuggestion) has been introduced to facilitate browsing and search activities. Some of the search terms it autonomously prompts are specific to geolocation and its cultural sensitivities that can, in some contexts, provide

---

[565] *United States v. Google (*NO. CV 12-04177 SI) in relation to violation of court order in *Google Buzz* case, *supra* fn 558, fn 1.

[566] Jennifer Valentino-Devries, *Google to Pay $22.5 Million in FTC Privacy Settlement,* WSJ (9 Aug. 2012) http://online.wsj.com/news/articles/SB10000872396390443404004577579232818727246. *See also* Christian Stocker, *Puny Punishment for Goliath: Google Case Exposes Weak US Data Privacy Laws,* Spiegel International (10 Aug. 2012) http://www.spiegel.de/international/europe/americans-may-have-to-wait-for-europe-for-better-data-protection-a-849372.html.

[567] Julia Angwin & Jennifer Valentino-Devries, *Google Tracked iPhones, Bypassing Apple Browser Privacy Settings*, WSJ (17 Feb. 2012), http://online.wsj.com/articles/SB10001424052970204880404577225380456599176.

[568] At the time, Google reported that the penalty comprised only 0.81% of company profits for 2012's second quarter and that could reputedly be recouped in 5 hours of retail sales.

socially inappropriate content and embarrassing innuendo.[569] Under such circumstances it might suggest racial, sexual, or other discriminatory messages or search terms. Technically, the autocorrection feature depends on a relatively simple algorithm. The system can be similar to a word processor's spell checker: as you type, the software checks each word against a built-in dictionary and suggests alternatives when it does not find a match.[570] Many systems try to predict your intentions and suggest a word before you have finished typing it. When sent, the lingering damage can be considerable. Misunderstandings arise when words contained in the built-in dictionary do not reflect the cultural or legal climate of the user.

Some insults to reputation cross all cultural lines. For example, a Japanese plaintiff in a defamation suit suffered work loss due to Google algorithms linking his name to criminal acts he had not committed.[571] European courts seem similarly intolerant of autocorrection references to illegal activity.[572] An Italian court found liability, for example, in Google Inc.'s autosuggestions that linked a citizen's name with *truffa* (fraud) and *truffatore* (con man).[573] In France, Google faced a similar suit over search suggestions linking several persons' names to "Jewish", in violation of a French law prohibiting the recording of a person's ethnicity.[574] Google argued in its defence that autocorrection technology is based on most frequently searched terms, but has more recently modified its practice to exclude references to constitutionally protected groups. Other lawsuits for defamation involving autocorrection include claimants in Germany who requested that Google delete the autocomplete results "fraud" or

---

[569] Danny Sullivan, *How Google Instant's Autocomplete Suggestions Work,* Searchenglineland (6 Apr. 2011), http://searchengineland.com/how-google-instant-autocomplete-suggestions-work-62592.
[570] Farhad Manjoo, *Yes, I'll Matty You,* SLATE (July 2010), http://www.slate.com/articles/technology/technology/2010/07/yes_ill_matty_you.2.html.
[571] *Google ordered to change autocomplete function in Japan,* BBC News (26 Mar. 2012), http://www.bbc.com/news/technology-17510651.
[572] David Meyer, *Google loses autocomplete defamation case in Italy,* ZDNet (Apr. 5, 2011), http://www.zdnet.com/google-loses-autocomplete-defamation-case-in-italy-3040092392/.
[573] Padova Maria Luisa v Google Inc. (10847/2011) TRIBUNALE ORDINARIO DE MILAno (Mar. 31, 2011).
[574] Mike Masnick, *Google Works Out Deal Concerning 'Jew' Suggestions In France,* Techdirt (5 July 2012), https://www.techdirt.com/articles/20120705/03231519585/google-works-out-deal-concerning-jew-suggestions-france.shtml.

"Scientology" associated with their name search;[575] and an action by the wife of a former president of Germany whose name prompted search terms "escort" and " red light".[576] In that case, Internet companies were not ordered to preemptively vet auto suggestions; their liability is only triggered if and when they become aware of a violation of third party rights.[577] In practice, Google claims to routinely investigate the defamatory nature of suggested search terms when faced with a cease and desist request.

Those actions are arising in places *other than* the US due to the latter's failure, to date, to squarely address such potential liability. The major hurdle in enjoining an American Internet company as defendant in autocorrect or autosuggestion cases is the near carte-blanche they receive under the *Communications Decency Act, s. 230,* as pointed out above. In defence of their invasive practices, Internet companies claim they are personalizing online services, bringing information and social connections to an extent the subscriber would never enjoy without such services. As observed in one German publication, American companies are the great offenders as they dominate the market and have considerable influence in the effectiveness of FTC regulation:

> Internet companies benefit from America's lax privacy and data protection laws, which are unlikely to change any time soon. It's a stark contrast to Europe, where the EU wants to toughen its laws -- and apply them to American companies.[578]

One disincentive to compliance with privacy rules is that punitive fines, relatively low in relation to profits, can be rationalized as an everyday cost of doing business. All of the above examples illustrate the technological and economic power that Internet

---

[575] *Federal Supreme Court: Google Liable for Defamatory Autocomplete Search Terms,* Dispute Resolution In Germany Blog (14 May 2013), http://www.disputeresolutiongermany.com/2013/05/federal-supreme-court-google-liable-for-defamatory-autocomplete-search-results/(where the court found a violation of personality rights).

[576] Michael L. Smith, *Search Engine Liability for Autocomplete Defamation: Combating the Power of Suggestion*, 2013 J. L. TECH. & POLICY, 314, 314-315.

[577] *See further* Seema Ghatnekar, *Injury By Algorithm: A Look Into Google's Liability For Defamatory Autocompleted Search Suggestions*, 33 LOY. L.A. ENT. L. REV. 171 (2013), http://digitalcommons.lmu.edu/elr/vol33/iss2/3 (abstract).

[578] Stocker, *supra* fn 566.

companies have always exercised over our 'interests, needs, desires, fears, pleasures, and intentions.'[579]

3.3 Case Studies

In examining the Mosley and Martin cases, my purpose is to illustrate that the damage imposed on personal, familial, and societal relationships by persistent Internet content is profound and not particularly aided by practical legal responses. While each plaintiff turned for vindication to the traditional adversarial systems in Europe or America, neither one had their search for justice completely met. Much of that discontent was due to their awakening to the shortcomings of the litigation process. In both cases, the privacy invasion they felt at the hands of Internet companies was compounded by the inability of their respective legal systems to ease the sting of a damaged reputation.

a Exposure: The EU Mosley Case

The decision of the British High Court in the Max Mosley exposure case was favourable in its initial findings but has brought little reputational reprieve in the end. It illustrates the deep reputational damage incurred by public figures,[580] the extent to which they will go to restore their good name, and the shortcomings of the civil court process to bring satisfaction after the fact. Mosley is a world figure in auto-racing. On March 30th 2008, the UK Sunday tabloid *News of the World* (NoW) published an article about Mosley under the heading "F1 boss has sick Nazi orgy with five hookers". The NoW published photographs and a link to its website that displayed video footage of the applicant that was secretly recorded by a paid participant to the sexual activities. Public response was viral: the original publication enjoyed a circulation in excess of 3 million, the online video received 1.4 million views the first day, and the online article attracted 400,000 views on each of the first two days.

---

[579] Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV., 1433, 1435 (2008).

[580] Mosley served as the President of that non-profit federation of motoring organizations dedicated to world motor sport.

Mosley sued the NoW and its owners, News Group Newspapers Ltd, for breach of confidence "by way of conduct inconsistent with a pre-existing relationship".[581] The nature of that pre-existing relationship was never made clear.[582] He also sought, unsuccessfully, an interim injunction to prevent the NoW showing footage of the covertly recorded video on their website. In his defence, Mosley admitted to having a party but denied the Nazi theme and found fault with the press characterization of his private conduct. [583] Mosley was awarded £60,000 in actual damages.

When Mosley applied to the ECtHR for a reference on the matter of injunctive relief, the Court cited the ECHR,[584] the UK Human Rights Act of 1998,[585] and the successful defamation case of Canadian singer Loreena McKennitt that expanded confidence actions to circumstances involving public figures where no prior relationship existed. Mosley petitioned the ECtHR for support of his claim that Article 8 of the ECHR imposed a positive obligation on the State to require prior notification of newspaper publications interfering with privacy rights. Only by advanced notice and a corresponding injunction, Mosley proposed, could he meaningfully preempt publication of such highly personal material. He argued that the available remedies in English domestic law inadequately protected his right to respect for private life, as guaranteed by Article 8 of the ECHR. The ECtHR agreed that privacy breaches were irreversible

[581] *Mosley v News Group Newspapers Ltd* [2008] EWHC 687 (QB)(Mosley 1). Although there was no action for defamation and therefore no ruling on damage to reputation, Justice Eady pointed out the judicial obligation to apply such legislation as the *UK Human Rights Act 1998, c. 42*: "[T]he law is concerned to prevent the violation of a citizen's autonomy, dignity and self-esteem. It is not simply a matter of "unaccountable" judges running amok. Parliament enacted the 1998 statute which requires these values to be acknowledged and enforced by the courts".

[582] Breach of confidentiality had been successfully argued in the UK case of Canadian singer Loreena McKennitt in *McKennitt v Ash* [2008] QB 73 at [8], per Buxton LJ, a significant precedent for privacy rights of public figures.

[583] The press use of the word 'nazi' was intended, according to Mosley, to generate public discussion of Mosley's father, Sir Oswald Mosley, well known during the interbellum years as the founder of the British Union of Fascists. Mosley had previously denounced his father's past associations, so saw the press reference as an implication of his duplicity in secretly played Nazi sex games.

[584] ECHR, *supra* fn 534 at art 8 and 10. Article 8 provides for the right of respect for private and family life, one's home and correspondence, with no public interference in that right except in accordance with law and in the interests of national security, public safety, the country's economic wellbeing, the prevention of crime, protection of health or morals, or the protection of the rights and freedoms of others. Article 10 addresses the countervailing right of free speech.

[585] *UK Human Rights Act 1998*, c. 42: Article 8, s. 12(3) serves to buttress the protection afforded to freedom of speech at the interlocutory stage.

under any circumstances, but pointed out that news of defamation awards could serve to restore some of the plaintiff's reputation. Citing with approval the distinction made by Justice Eady in the court of first instance, the court commented:

> [L]ibel damages can achieve one objective that is impossible in privacy cases. Whereas reputation can be vindicated by an award of damages, in the sense that the claimant can be restored to the esteem in which he was previously held, that is not possible where embarrassing personal information has been released for general publication. As the media are well aware, once privacy has been infringed, the damage is done and the embarrassment is only augmented by pursuing a court action.[586]

Mosley's case does not illustrate that distinction: he is a wealthy[587] former lawyer with worldwide influence in motor sports. While the monetary award assisted in bringing his case against Internet companies in other European jurisdictions for retransmitting the offending images, it was of little consequence in removing the stain to his reputation: he was forced to resign as President of the auto sport governing body Fédération Internationale de l'Automobile. Further, the Queen's Bench Justice Eady denied his request to stem further dissemination of the harmful content by granting an injunction to any further re-publication of the video on the Internet, citing the practical futility of trying to suppress the highly generative medium once the dams had burst.

Greatly affected by news of his son's drug-induced death, exacerbated in Mosley's view by the devastating effect of the NoW story, he then sued Google Inc. for its continued listing of his Nazi-themed orgy amongst its search results and Nazi-themed photographs in Google Image.[588] He pursued takedown orders in the courts of twenty-two countries and ordered the removal of material from 193 websites in order to vindicate the false accusations of the NoW press.[589] In 2013, Mosley won injunctive and financial relief from courts in France[590] and in Germany. Mosley commented on the

---

[586] *Mosley v United Kingdom,* Reference Application no. 48009/08; [2012] EMLR 1; *Mosley v United Kingdom* (2011) 53 EHRR 30.

[587] Gossip sites estimate Mosley's net worth at $US16 million: *Max Mosley Net Worth,* http://www.celebritynetworth.com/richest-businessmen/max-mosley-net-worth/.

[588] *Leveson Inquiry: Max Mosley describes outrage at story,* BBC News (24 Nov. 2011), http://www.bbc.com/news/uk-15874015.

[589] Josh Halliday, *Max Mosley sues Google in France and Germany over 'orgy' search results',* GUARDIAN (25 Nov. 2011), http://www.theguardian.com/media/2011/nov/25/max-mosley-google-france-germany.

[590] *Max Mosley v Google Inc. and Google France,* TGI Paris, Court of First Instance, RG# 11/07970 (6 Nov. 2013) (Mosley II).

harm that the exposure of private actions caused him ("enormous and continuous damage"),[591] caused his wife of 48 years ("totally devastating") and his sons (he could think of "nothing more undignified or humiliating" for his two sons to experience).[592]

The Mosley case has been ongoing since 2008 and has exacted a personal toll for the plaintiff in the lowering of his esteem and that of his family in the public eye, the embarrassment and humiliation that have resulted, and the formidable cost of pursuing retribution.[593] For the average income earner, litigation on the Mosley scale would be completely inaccessible.

b Disclosure: the US Martin Case

The David-and-Goliath case of Lorraine Martin is about a Connecticut nurse and single mother who sued the Hearst Corporation media giant for persistent online media accounts of a criminal charge for which she was never convicted. The ongoing case for erasure that was denied in the US District Court of Connecticut and is now before the state's appellate court, and is noteworthy for the additional layer of complexity added to claims for reputational redress when the Internet is involved.[594] Martin's persistent efforts to assert erasure rights have brought her no remedial relief to date.

Martin was arrested in 2010 on a warrant, along with her two adult sons, for possession of a narcotic (traces of cocaine) and drug paraphernalia (scales) and possession of a controlled substance (marijuana), evidence police needed to substantiate an informant's contention that the Martin sons had been selling drugs in the neighbourhood. Ms. Martin was arrested and released on bail. Her charges were

[591] Tim Lowles, *Max Mosley wins his case against Google in France*, Collyerbristow.Com, Press Release (6 Nov. 2013), http://www.collyerbristow.com/Default.aspx?sID=90&cID=1214&ctID=43&lID=0.
[592] *Mosley wins court case over orgy*, BBC News (24 July 2008), http://news.bbc.co.uk/2/hi/7523034.stm.
[593] Mosley reported to the Leveson Inquiry that he had spent, to that point in 2011, 500,000 BPS on defending his name. *See further* Leveson Inquiry Into The Culture Practices And Ethics Of The Press (5 Apr. 2014), http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/
[594] *Lorraine Martin v. Hearst Corp. et al.*, District Court of Connecticut case number 3:12-cv-01023 (Martin I).

withdrawn a year later for lack of evidence.[595] Martin argues her case has been expunged from court records and should similarly be removed from online websites.[596] Its persistence in Internet searches serves as a virtual scarlet letter in terms of Martin's future chances at employment in the medical field.[597]

Martin's arrest was covered by three Hearst publications, both in print and online.[598] Upon the withdrawal of her charges, Martin invoked a clause in a Connecticut erasure law arguing that while the original accounts of her arrest were true, from the point of their dismissal they should be considered never to have happened and so should be removed from both online and offline news archives as a conviction had never been registered. Most American states have some version of such erasure laws.[599] Martin maintained that any sustained media account of her arrest was therefore defamatory because it was untrue, brought untold damage to her reputation, robbed her of opportunities for employment and social acceptability, and did not allow her to move forward without the stigma of the arrest. She sought expungement of the accounts of her arrest from all online sources and archives, claiming four tortious causes of action: libel, publicity placing her in a false light, negligent infliction of emotional distress, and invasion of privacy.

The District Court of Connecticut applied strict statutory interpretation to deny all four claims and dismissed the case. The court acknowledged that the law mandates the erasure of the arrest records by law enforcement and court officials but states:

---

[595] *Lorraine Martin v. Hearst Corporation, Main Street Connect, and News 12 Interactive Inc.,* File §3:12-cv-01023-MPS, DOC 58, United States District Court, District of Connecticut, (2013) at 3 (Martin II).

[596] Tim Powers, *Expungement: what does it mean for your record?* Denton County Criminal Defense Lawyer Blog (9 Oct. 2012), http://www.timpowers.com/dentonCriminalDefense/2012/expungement-what-does-it-mean-for-your-record.html.

[597] Bill Keller, *Erasing History*, NYTIMES (28 Apr. 2013). http://www.nytimes.com/2013/04/29/opinion/keller-erasing-history.html?_r=0.

[598] Anna Helhoski, *Crack Cocaine Raid Nets Two,* GREENWICH DAILY VOICE, (25 Aug. 2010), http://greenwich.dailyvoice.com/news/crack-cocaine-raid-nets-two.

[599] *Connecticut General Statute* §54-142a, provision e(3) "Any person who shall have been the subject of such an erasure shall be deemed to have never been arrested under the meaning of the general statutes with respect to the proceedings so erased and may so swear under oath." The criminal laws of several EU Member States carry similar provisions.

> [T]he expungement statute does not transmute a once-true fact into a falsehood. It does not require the excision of records from the historical archives of newspapers or bound volumes of reported decisions or a personal diary. It cannot banish memories.[600]

The dismissal is considered a win for the First Amendment, both freedom of speech and freedom of the press.[601] The judge's decision shields the factual reporting of news organizations from being erased from the Internet just because its archived version might seem detrimental to someone's reputation years later. The case, however, does not resolve the stickier ethical questions surrounding news organizations' responsibilities in the digital age, where news stories linger online and can be dredged up indiscriminately long after most paper copies would have been buried and forgotten. Martin subsequently brought a class action pleading similar grounds to the state's Court of Appeal. An *amicus* brief filed by the Reporter's Committee for Freedom of Expression argues in support of the defendant publishers that parties who use erasure laws to 'remove factually accurate newspaper stories' threaten the First Amendment rights of freedom of expression.[602] It stresses that, while erasure is required of court staff, police, and prosecutors, the Connecticut law would violate individual constitutional rights if it required journalists who report the truth to rescind it retroactively once the facts were no longer true.[603]

c Significance of Mosley and Martin Cases

The significance of the Martin case lies in the extra layer of complexity brought to the law of journalism by the Internet. In the class action, Martin could argue that the ethics around the censorship question are skewed when considering the extent of harm to her reputation with a medium with permanently cached information, instantaneous access, and global redistribution capabilities to third parties. The defendant news publishers rely on standard ethical and constitutional principles espoused by journalists

---

[600] Martin I *supra* fn 594 at 8.
[601] Marie K. Shanahan, *Archived Arrest Stories are like Zombies Arising from the Grave*, Blog (1 Sept. 2013), http://www.mariekshanahan.com/hearst-news-12-and-main-street-connect-defeat-lawsuit-over-archived-arrest-stories/.
[602] *Martin v. Hearst Publications,* Case 13-3315, filed 17 March 2014 in the US Court of Appeals for the Second Circuit, http://www.rcfp.org/sites/default/files/2014-03-17-martin v hearst.pdf (Martin III).
[603] *Id.* at 9.

regarding the inviolable truth of their news at the time it is reported, and the practical difficulties inherent in 'unpublishing' and foreshortening the 'long tail of the news'.[604]

The legal issue of who controls news online has been broadened with Google's claim that news organizations can block Google from indexing specific content. It is webmasters who control web content, Google maintains, not Internet companies, and news publishers control webmaster decisions about what stories have public access, when, and at what price.[605]

Meanwhile Mosley continues to sue Google in one country after another, as domestic laws are the current route to relief in the absence of any pan-European or international judicial authority over transborder transmission of reputation-destroying information. Journalist Bill Keller describes the ongoing stigma experiences by Martin:

> [She] found that when she applied for jobs that should have been well within her reach, she got the cold shoulder. She Googled herself and discovered what any vigilant employer would have seen: stories still sitting in online news archives with headlines like "Mother and sons charged with drug offenses."[606]

While the EUDR might help in bringing some clarity and consensus to an effective legal response to such damage, for now litigants like Mosley and Martin must endure the legal uncertainty and the sensational or titillating accounts that publicize individual efforts at stemming reputational damage.[607]

In terms of existing legal remedies to protect reputation, the Mosley case illustrates there are few tools and most are financial. As Mosley's comments about his family show, injuries to reputation are not borne exclusively, or even primarily, by the affected individual. Defamation scholar Ardia explains that, in many ways, reputation is a quintessential public good in that it is a product of cooperation with others and

---

[604] Kathy English, *The longtail of news: To unpublish or not to unpublish,* TORONTO STAR, Journalism Credibility Project (October 2009), http://www.apme.com/?Unpublishing (reporting that publishers are increasingly inundated with 'unpublish' requests and aware they must come to a practical resolution of the issue.)

[605] *Working with News Publishers*, Google Public Policy Blog, https://groups.google.com/forum/ -!forum/public-policy-blog/join.

[606] Keller, *supra* fn 597.

[607] Kelly Fiveash, *Mosley thrash'n'tickle vid case against Google opens in Hamburg: Ex F1 chief's clip campaign flogging a -erm-dead horse?* REGISTER (28 Sept. 2012), http://www.theregister.co.uk/2012/09/28/.

relative to our relationships with them.[608] Ardia urges understanding of reputation's "important signaling function" in communicating complex information about an individual and about the individual's place within society. To malign that reputation, in his view, is to degrade the value and reliability of that information and of the community identity as a whole.[609]

The factor of online permanence is highlighted by the Martin decision. In Europe, where journalists and citizens do not have the First Amendment protections, a right to be forgotten allows for those with cleared records to demand every trace of the record be completely erased.[610] That demand extends to print and electronic media accounts (including European bureaus of US-based media) and includes a demand that all records of a case be completely erased, not just updated. *Toronto Star* editor Karen English reports that misdemeanors and other criminal charges are an increasing source of requests to "unpublish" news accounts for North American publishers.[611] She cites with approval a 'sunset' provision instituted at one news corporation whereby certain news items autonomously 'drop off' the news organization's website six months after initial publication.[612]

Both Mosley and Martin have become victims to what, in the world of US defamation law, is a commonplace occurrence of time-lapse or "incremental" thinking: jurists within many legal systems struggle in their own ways with legal culture and laws that are remnants of simpler times. Another unfortunate and unhelpful influence on both plaintiffs is what is known as the 'Streisand Effect'.[613] The phenomenon, named after American entertainer Barbra Streisand, reflects the unsatisfactory results obtained in an invasion of privacy action she filed in 2003 against a photographer for capturing images of her Malibu oceanfront home to promote a government coastal erosion project. Streisand maintained that inclusion of those images in the proposal implied she was

---

[608] Ardia, *supra* fn 10, 262.
[609] *Id.*
[610] Genevieve Balmaker, *Erasing the Record, One Story at a Time*, QUILL (July/August 2013), http://digitaleditions.walsworthprintgroup.com/display_article.php?id=1475867&_width=.
[611] English, *supra* fn 604 at 7.
[612] *Id.*
[613] The Streisand effect is a phenomenon whereby an attempt to censor or gag a report has led to greater interest in the story than would have been garnered had they not attempted to ban or censor it in the first place. Some people have proposed that it be called Streisand's law given the inevitability of the effect (*Streisand Effect,* Rationalwiki, http://rationalwiki.org/wiki/Streisand_effect.)

insensitive to coastal erosion, a false impression she judged would cause her great reputational damage, both personally and as an entertainer. Upon the filing of Streisand's legal action for invasion of privacy, public interest in the images on YouTube soared from six to more than 420,000 downloads within one month.[614] The continued access to the story on YouTube substantiates the fear of every potential litigant that, far from ameliorating personal suffering, court actions can perpetuate anyone's negative reputation.

3.4 Summary

Life in the post-analogue world offers a richness of choice in communications. The downside is that we become what we behold: we move from being shapers of tools to being shaped *by* them.[615] We experience opportunities to express, inform, consume, advance professionally, and entertain ourselves in ways only sketchily drawn by science fiction authors. With innovation in digital communications comes mobility, plasticity, speed, ambit, a-spatiality, and ephemeral storage - all creating enhanced risks of personal privacy invasion. Those invasions damage our reputation or personal identity within the communities in which we work and interact socially. That result would not surprise futurist authors such as George Orwell or Michel Foucault or Marshall McLuhan, but it poses important legal questions that need to be tackled to restore the balance of key ingredients in post-modern life such as technological convenience, information management, privacy, free expression, and attribution.

The role of law in remedying damage to reputational privacy within that complex environment is explored in the next two chapters. Several crucial questions raised in this chapter prompt that inquiry: is anonymity practically possible or even desirable in digital transactions; can the power of Internet companies to control our online presence be shaped to our protection rather than our vulnerability; is digital

---

[614] Mike Masnick, Streisand Suing Over Environmentalist's Aerial Shots Of Her Home, TechDirt (1 June 2003), https://www.techdirt.com/articles/20030601/1910207.shtml. Streisand received no compensation from the court and was ordered to pay her opponent's legal fees.

[615] MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN, xxi (1994) (pointing out "We become what we behold. We shape our tools and then our tools shape us.")

speech sufficiently different than real-time communications to warrant a new legal regime? As set out in Chapter II, the normative and political differences between US and EU legislators and jurists regarding those broader questions have produced two very different regulatory regimes that could lead to a trans-Atlantic clash of values. But first, an examination of the current legal tools available to those who suffer reputational injury perpetrated through digital communications.

CHAPTER 4 LEGAL RESPONSES TO REPUTATIONAL INJURY

4.0 Introduction

> Meaning is the essential starting point in any claim for defamation. The same set of words can legitimately be given quite varied interpretations by different individuals, but the law of defamation applies a *"legal fiction"* that a publication can only be understood to bear one 'natural and ordinary' meaning. This is the meaning as understood by a hypothetical, reasonable reader.[616]

The Web has augmented and diversified ways to intrude upon our private lives. It is reasonable as individuals that we look to law to either safeguard our needs for reputational integrity or to offer a remedy when other mechanisms fail.[617] International, regional, and domestic laws each provide a particular response, either for state-citizen conflicts (primarily in the area of data protection) or for disputes that arise between private individuals (such as defamation, privacy, and breach of confidence cases). Since the end of World War II, the international community has formulated a handful of significant legal conventions that address reputation, primarily by framing those concerns broadly within values of privacy, family life, and personal dignity as entitlements of membership in the human race. As world wars have shrunk to more regional and asymmetric conflicts in the ensuing decades, the ambit of our interpersonal communications have expanded – from localized gossip to global, instantaneous messaging. We might anticipate, therefore, that the wide selection of international treaties would provide some conceptual reference point and inspiration for collaboration among jurists. Similarly, with the emergence of the Internet as the dominant

---

[616] *The Leveson Inquiry Into The Culture Practices And Ethics Of The Press,* UK Government National Archives, para. 3 (2 Mar. 2012) http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/wp-content/uploads/2011/11/Witness-Statement-of-Max-Mosley.pdf.

[617] This dissertation views legal privacy protection as including control over our personal information while recognizing that not all breaches of personal data involve injury to reputation. Alan F. Westin described such control as, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Stephen E. Henderson, *Expectations of Privacy in Social Media,* 31 MISS. COLLEGE L. REV., 226 at fn 13, citing Westin's *Historical Perspectives on Privacy: From the Hebrews and Greeks to the American Republic",* (unpublished manuscript on file with Henderson).

interpersonal messaging tool within the past decade, it would be reasonable to expect the evolution of Internet-specific laws protecting our virtual selves and that accommodate speech idiosyncrasies that were not in existence in the analogue era. In this chapter I begin with international instruments and look for their influence on regional (EU) and domestic (EU and US) law. Their degree of influence should be somewhat predictive of how effective and international law of the Internet might be. I then look to more regional and local causes of action (defamation, privacy, and confidentiality laws) and case samples to determine how they have incorporated those international legal norms. I conclude with a discussion about whether digital speech is *ontologically* different and hence deserving of a discrete legal or extra-legal response for our protection. That question is important to an understanding of whether courts are approaching Internet cases of reputational and privacy violations in a novel way or are merely applying real time solutions to online content. In summarizing the chapter I mention alternatives to our traditional legal practices if we are to approach online speech as an evolving and discrete form of expression.

4.1 International, Transnational & Domestic Response

a Conventions & Declarations

Two earlier international instruments expressly address reputation as a basic human right, the first crafted by United Nations members as they emerged from the destruction and atrocities of the Second World War and the second, somewhat ironically, created in the midst of the Vietnam War of the mid-1960s.[618] The *Universal Declaration of Human Rights*[619] (UNDR) and the *International Convention on Civil and Political Rights*[620] (ICCPR) use almost identical wording to stipulate that "no one shall

[618] *Vietnam Timeline: 1966,* http://www.vietnamgear.com/war1966.aspx.

[619] Universal Declaration Of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) 10 Dec. 10 1948, Article 12. International law creates a hierarchy of instruments: a *convention* (used synonymously with *treaty* and *covenant*) is binding between states. Conventions are therefore stronger than *declarations* that constitute an agreement of standards without legal enforcement. Declarations frequently are products of UN Conferences, and can be produced by government representatives or NGOs. Although the declaration was intended to be nonbinding, through time its various provisions have become so respected by states that it can now be said to be customary international law.

[620] International Covenant On Civil And Political Rights, S. Exec. Rep. 102-23, 999 U.N.T.S. 171, 16 Dec. 1966, art. 17 (ICCPR). The Human Rights Glossary appended to the UNCR defines 'civil and political rights' as "The rights of citizens to liberty and equality; sometimes

be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and *reputation*" and that "everyone has the right to protection of the law against such interference or attacks."[621] The ICCPR qualifies "interference" and "attacks" with addition of the word "unlawful".

The UNDR in article 19 also addresses a human right to free speech "through any medium and regardless of frontiers."[622] Reputation is treated as a right devolving from social and political life, and so is significantly more open-ended regarding interpretation than the protections against violent and arbitrary treatment with which the Declaration begins. As one source explains, the UNDR leaves larger scope for variation in different social and political contexts, because " individuals everywhere have the right to be free of torture, but different countries may legitimately come to different conclusions about the conditions under which private property may be taken for public use,"[623] Or, we might add, the import of privacy and reputation as elements of family and social life. Such differential treatment sets up the conditions for a hierarchy of rights in actual state practice.

The US and EU Member States have all signed both the UNDR and the ICCPR and ratified the multilateral UN treaty.[624] Both treaties have enforcement bodies: for the Universal Declaration several oversight bodies are provided.[625] The ICCPR is monitored by the UN Human Rights Committee that reviews regular reports from

---

referred to as first generation rights. Civil rights include freedom to worship, to think and express oneself, to vote, to take part in political life, and to have access to information." http://www1.umn.edu/humanrts/edumat/hreduseries/hereandnow/Part-5/6_glossary.htm.

[621] *Id.,* Article 17. Those instruments, in combination with the International Covenant On Economic Social And Cultural Rights, are considered the International Bill of Human Rights.

[622] "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[623] Mary Ann Glendon, *The Rule of Law in the Universal Declaration of Human Rights*, 2 NW. J. INT'L HUM. RTS. 1 (2004), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1008&context=njihr

[624] The US signed on 5 Oct. 1977. EU Member States signed upon gaining EU membership unless they had signed previously.

[625] Including the Committee on Economic, Social, and Cultural Rights, the Office of the UN High Commissioner on Human Rights, the Human Rights Council, and treaty-monitoring bodies like the Committee on the Elimination of Discrimination against Women and the Committee on the Rights of the Child.

State parties on how the rights are being implemented.[626] In practice enforcement for both treaties is more nominal than of real weight, with diplomatic pressure and other 'soft law' tools being preferred.

The UNDR is not legally binding as such; it carries no formal legal obligations but might carry moral obligations or attain the force of law as customary international law. Most of its rights had already received a significant degree of recognition by 1948 in the constitutions of many nations, if not in their practices. Since that time, most of its rights have been incorporated into the domestic legal systems of most countries.

In contrast, neither the ECHR nor the US Constitution contain direct references to honour or reputation as a *human right*, although the ECHR includes a reference to a respect for privacy and family life, in the spirit of article 12 of the UNDR and refers to reputation as a legitimate aim that might justify interference with the right of free speech, not by granting it rights status but by speaking of "protection of the reputation or rights of others."[627] The use of "reputation" as a qualification of free speech rights seems deliberate, as appears from the preparatory work on Article 8 of the ECHR.[628] It took the *Pfeifer v Austria* decision of the ECtHR in 2007 to recognize reputation as a right equivalent to free speech at European common law.[629]

In the case of the ICCPR, as with other international treaties, the US and all EU Member states who are parties to the Convention must comply with and implement the provisions of the treaty just as it would any other domestic law, subject to reservations, understandings and declarations (RUDs) requested by other signatories. One RUD of

---

[626] States must report initially one year after acceding to the Covenant and then every four years or upon request of the Committee.

[627] The ECHR refers expressly to "reputation" but only in the context of Article 10.

[628] *See further* the information document prepared by the Secretariat of the European Commission, "European Commission of Human Rights Preparatory Work on Article 10 of the European Convention on Human Rights", Council of Europe, Strasbourg (17 Aug. 1956) DH (56) 15 Oe.Fr. (noting the following proposals that were made but did not appear in the final document: a French proposal (Dec. E/1371, p. 21) that free speech could be limited by the protection of "the reputation or rights of other persons"; a UN conference on freedom of information suggestion that free speech be restricted by expressions of other persons that "defame their reputations or are otherwise injurious to them without benefiting the public." (para. 2(g)); and a similar proposal by the British Government (para 8(3)(2)). Subsequent references to a Committee of Experts eliminated references to 'reputation'.)

[629] *See further* Heather Rogers, "Is there a right to reputation?" Part 1, Inforrm's Blog (26 Oct. 2010) https://inforrm.wordpress.com/2010/10/26/is-there-a-right-to-reputation-part-1-heather-rogers-qc/

considerable weight in foreign relations, as requested by the US, establishes that the US Constitution shall prevail over any contested free speech use involving the terms of the ICCPR. Another key RUD attached by the US Senate is a "non self-executing" Declaration, intended to limit the ability of litigants to sue in a US court for direct enforcement of the ICCPR. That Declaration effectively challenges any external enforcement mechanism, although the US continues to file a report every four years with an ICCPR Human Rights Committee that oversees compliance.[630]

Cases relating to reputation that expressly reference the UNDR and the ICCPR are very limited; one reason might be the strength of RUDs requested by the US. Another could be the comparatively lower significance of reputational harm and privacy invasions on the scale of human rights violations, ranging from violent physical harms to intangible ones, that each instrument addresses. Rights to remedies, as discussed in the *UN Basic Principles and Guidelines on the Rights to Remedies*, seem restricted to 'gross' violations of International Human Rights Law and 'serious' violations of International Humanitarian Law, a bar the indignities and social exclusion caused by reputational injury might not be able to hurdle.[631]

In its last report to the ICCPR Human Rights Committee in 2014, the US was criticized by a committee of the UN for its surveillance activities on foreign as well as US citizens[632] that showed non-compliance with the privacy provisions in Article 17 and with international law principles of legality, proportionality and necessity.[633] Reputation rights as included in Article 17 were *not* specifically addressed. The report noted, however, but cannot enforce, recommendations that any interference with the right to *privacy*, *family*, *home or correspondence* be authorized by laws that: 1) are publicly

[630] States must report initially one year after acceding to the Covenant and then whenever the Committee requests (usually every four years).
[631] Basic Principles And Guidelines On The Right To A Remedy And Reparation For Victims Of Gross Violations Of International Human Rights Law And Serious Violations Of International Humanitarian Law, GA 60/147 (16 Dec. 2005).
[632] Specifically highlighted were NSA's bulk phone metadata surveillance programme (Section 215 of the USA PATRIOT Act); surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act, conducted through PRISM (collection of communications content from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic).
[633] Human Rights Committee (ICCPR) Concluding Observations On The Fourth Periodic Report Of The United States Of America, CCPR/C/USA/CO/4, para 20ff. (23 Apr. 2014), http://www.refworld.org/docid/5374afcd4.html .

accessible; 2) are tailored to specific legitimate aims; 3) detail the precise circumstances of data collection and obtaining consent, and 4) provide for effective safeguards against abuse.[634] Also mentioned as excessive invasions of personal privacy are practices that mandate that third parties (such as ISPs and other Internet companies) retain personal data for state use; and that the judiciary be involved in "authorizing or monitoring" surveillance activities.[635]

With respect to the ICCPR, its Human Rights Committee has assessed its provisions relating to free speech as describing a much narrower right than that articulated in US constitutional laws. Article 20(2) of the ICCPR requires prohibition of any negative statements towards national groups, races or religions that *"constitutes incitement to discrimination, hostility or violence"*. The US Supreme Court has determined the First Amendment addresses free speech in three fora: public speech, used in public spaces such as parks, where all speech is protected unless leading to violence; designated forum speech, such as meetings held in universities, where speech enjoys the same protection as public speech but for a designated time; and limited forums where only certain classes of speech are protected, such as a meeting on a religious subject.[636] In any conflict between a US citizen's free speech rights and those of a non-US citizen subject to a non-US free speech law, the US position is likely to prevail due to its wider ambit. That is particularly the case with hate speech. The US subscribes to an even wider tolerance: only incitement that is intended to cause *imminent* violence justifies restricting fundamental speech right.[637] Some EU states, however, such as Finland, Belgium, Iceland, and Denmark, oppose the term 'hate speech' as potentially restricting democratic debate on religion and minorities. Those protections are broader still than those in American law.

The International Bill of Human Rights, then, has been extensively elaborated through numerous conventions and declarations, both at the universal level and at the regional level. Altogether they comprise a wide range of human rights and that form an interrelated normative system. More recent additions include the *International*

[634] *Id.* at para. 20(b).
[635] *Id.* at para. 20(c) and (d).
[636] *See further,* Forums, WEX Legal Dictionary, Legal Information Institute, Cornell University Law School, https://www.law.cornell.edu/wex/forums.
[637] *See further* Hate Speech, ARTICLE 19, http://www.article19.org/pages/en/hate-speech-more.html.

Convention on the Protection of the Rights of All Migrant Workers and Members of their Families that mentions reputation as a qualification in the balance to be struck between privacy and free speech.[638] So even temporary citizens are afforded a basic right to a good reputation, although its wording suggests it might be subordinate to free speech rights. Other international instruments and initiatives that are relevant to online reputation are: the *UN Convention on the Rights of the Child*;[639] (prohibiting arbitrary or unlawful interference with a child's privacy, family, or correspondence, and unlawful attacks on his or her honour and *reputation);* the *UN Convention on the Rights of Persons with Disabilities*[640](with similar provisions for the disabled, including protection from unlawful attacks on reputation and privacy rights for correspondence "and other types of communications"); and the *UN Resolution on a Global Agenda for Dialogue among Civilizations*[641] (urging full utilization of communication technologies including the Internet to further global dialogue and understanding).

With respect to regional initiatives, the *European Convention on Human Rights and Fundamental Freedoms* (ECHR) expressly addresses reputation as one limitation on the right to free expression. It also suggests reputational protection obliquely through the right to respect for private and family life, home and correspondence.[642] It qualifies that right for national security, public safety, the economic well-being of the state, the

---

[638] International Convention On The Protection Of The Rights Of All Migrant Workers And Members Of Their Families, G.A. Res. 45-158, U.N.P.M. 69, Dec. 18, 1990, Article 14.

[639] Convention On The Rights Of The Child, 1577 U.N.T.S. 3, Nov. 20, 1989, Article 16: "1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and *reputation*." [emphasis added]

[640] Convention On The Rights Of Persons With Disabilities, Dec. 13, 2006, 2515 U.N.T.S. 3, Article 22: 1) No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence or other types of communication or to unlawful attacks on his or her honour and *reputation*. Persons with disabilities have the right to the protection of the law against such interference or attacks; 2) States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others. [emphasis added]

[641] Global Agenda For Dialogue Among Civilizations, G.A. Res. 56-6, U.N.Doc. A/56/L.3 and Add/ 1, Nov. 21, 2001, Article 9: "Utilization of communication technologies, including audio, video, printed press, multimedia and the *Internet*, to disseminate the message of dialogue and understanding throughout the globe and depict and publicize historical instances of constructive interaction among different civilizations". [emphasis added]

[642] Art. 10. The ECHR does refer to reputation as one of the legitimate aims that might justify interference with freedom of expression. However, it does not do so by granting rights status to reputation, but instead speaking of "protection of the reputation or rights of others".

prevention of disorder or crime, the protection of health and morals, and the protection of the rights and freedoms of others." [643]

The recognition of reputation as a distinct right was slow coming in EU case law. In the first defamation case brought under article 10 of the ECHR, *Lingens v. Austria*[644] in 1986, the ECtHR denied the Government's argument that the case concerned a conflict between two equal Convention rights; the court held that a right to reputation only acted as a qualifier of the right to free expression. With the article 10 case of *Chauvy and others v. France*[645] in 2004 and the article 8 case of *Pfeifer v. Austria*[646] in 2007, however, the right to protection of reputation was established as a full Convention right under article 8 of the ECHR. The *Pfeifer* case decided "a person's right to protection of his or her reputation is encompassed by Article 8 as being part of the right to respect for private life".[647] EU law had finally incorporated international legal norms expressed by the UNDR and ICCPR. That development has its critics: Stijn Smet of the University of Ghent criticizes the ECtHR for elevating reputation to convention right status as it will naturally conflict with another, stronger right, that of freedom of expression which comprises its "strongest enemy".[648] He cites the ECtHR case of *Polanco-Torres* (where a judge's wife fought defamatory claims that she and her husband engaged in unlawful business transactions) as a judicial attempt to balance the

---

[643] ECHR, Article 8 provides for the right of respect for private and family life, one's home and correspondence, with no public interference in that right except in accordance with law and in the interests of national security, public safety, the country's economic wellbeing, the prevention of crime, protection of health or morals, or the protection of the rights and freedoms of others. Article 10 addresses the countervailing right of free speech.

[644] *Lingens v. Austria* (1986) 8 EHRR 407.

[645] *Chauvy and others v. France* (2005) 41 EHRR 29, regarding a book that suggested by innuendo that Jean Moulin, Resistance Leader in WW2 was betrayed and killed because of the actions of Raymond Aubrac who escaped. ("the book is little more than pure conjecture and constitutes a direct assault on the integrity and identity of Mr and Mrs Aubrac that robs them of their dignity. It is necessary to reaffirm respect for human dignity as one of the most important Convention values and one which historical works must also foster.")

[646] *Pfeifer v. Austria* (2007) 48 EHRR 175 regarding an article alleging the Jews attacked Germany in 1933 and trivializing the actions of the Nazi regime. (stating "A person's reputation, even if that person is criticised in the context of a public debate, forms part of his or her personal identity and psychological integrity and therefore also falls within the scope of his or her private life under Article 8.").

[647] For further analysis see Stijn Smet, *The Right to Reputation under the European Convention on Human Rights* STRASBOURG OBSERVERS (1 Nov. 2010), (Strasbourg) http://strasbourgobservers.com/2010/11/01/the-right-to-reputation-under-the-european-convention-on-human-rights/.

[648] *Id.*

human rights pendulum that had swung too far on the side of reputation. In Smet's opinion the court wrongly set a high standard for proof of harm as one that "compromises personal integrity".[649] Smet is persuasive in arguing that, by creating the integrity standard, the ECtHR has created a situational right, not balanced an existing right with a competing right of free speech using the traditional proportionality test. In the *Polanco* case "in some situations one enjoys a right to reputation and in others not."[650]

In the Western Hemisphere, the *American Convention on Human Rights*, promoted by the Organization of American States (OAS) with state members in North, Central, and South America, sets out the right to privacy, honour and dignity.[651] It prohibits arbitrary interference with the right to *privacy or one's reputation* and stipulates that everyone has the right to protection of the law against attacks or interferences with that right.[652] It further subjects the right of expression to a "respect for the rights or reputations of others".[653] The American Convention also provides for a right of reply to individual complaints of reputational violations through the designation by every publisher (including online publishers) of a person without immunity to respond to such complaints.

The American Convention was inspired by the *American Declaration of the Rights and Duties of Man* (the Declaration of the Americas) that marked the world's first general international human rights instrument, predating the Universal Declaration of Human Rights, 1947 by one year.[654] The US and Cuba are the only parties to have signed but not ratified the American Convention, although a few states have actually

---

[649] *Polanco Torres and Movilla Polanco v. Spain*, ECHR 34147/06, [21 Sep 2010] 1341.
[650] Smet, Strasbourg, *supra* fn 648.
[651] Article 11: "1. Everyone has the right to have his honor respected and his dignity recognized;
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or *reputation*; 3. Everyone has the right to the protection of the law against such interference or attacks." [emphasis added]
[652] American Convention On Human Rights, Organization of American States [OAS], American Convention on Human Rights, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123 (American Convention).
[653] *Id.*, Article 13, para 2a.
[654] Inter-American Commission on Human Rights (IACHR), American Declaration Of The Rights And Duties Of Man, (2 May 1948) http://www.refworld.org/docid/3ae6b3710.html.

attempted to rescinded their ratification.[655] In practice, the OAS and the American Convention are seen as "more Latin American than Inter-American" and there is strong pressure for the US to become a State Party to the alternative OAS Inter-American treaties.[656]

Although not well known outside of the legislative histories of the parties, the Declaration of the Americas has been referenced in the jurisprudence of both the Inter-American Court of Human Rights (IACHR) and the work of the Inter-American Commission on Human Rights (the Commission) that acts as a court of first instance for the OAS and that works at enforcement of the Declaration in all OAS Member States. In contrast to the EU system of human rights litigation, individual citizens of the OAS Member States are not authorized to take cases directly to the IACHR.[657]

Akin to its position regarding the ICCPR, the US holds that its own laws provide the same or stronger human rights protections than those of the Declaration of the Americas and the latter was not referenced in my search of US jurisprudence dealing with inter-American human rights cases. In fact, there were no cases of US origin coming before the IACHR. Key objections in the US to OAS rights protections relate to issues of federalism, sovereignty, and incompatibility with US domestic laws, most prominently the US Constitution.[658] In political terms, US exceptionalism[659] regarding OAS activities within the Inter-American System is heavily criticized by

---

[655] Trinidad and Tobago has rescinded; Peru tried, but used the wrong procedure.

[656] Monica Pinto, *The Role of the Inter-American Commission and the Court of Human Rights in the Protection of Human Rights: Achievements and Contemporary Challenges,* Human Rights Brief, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1840&context=hrbrief

[657] Cases must be referred by the Inter-American Commission on Human Rights or a member state.

[658] *Id.,* at 21 (advising the US to ratify the American Convention to show international leadership regarding human rights). The federalist question asks whether ratification by federal authorities could legally encroach on exclusively state matters; sovereignty concerns question the interrelation of international and domestic legal regimes; and the third objection deals specifically with the incompatibility of the Convention's provisions with US legal positions on abortion and the death penalty.

[659] The term "U.S. exceptionalism" is used here to indicate the belief that, unlike other states, the United States does not need to ratify international human rights treaties because its domestic legal system provides the same or better protections. *See further* Stephen M. Walt, *The Myth of American Exceptionalism,* Foreign Pol. (Oct. 11, 2011), http://foreignpolicy.com/2011/10/11/the-myth-of-american-exceptionalism/

other members who have contemplated the creation of alternatives to the American Convention and exclusion of US participation.[660]

With respect to data protection in Europe,[661] two international instruments are crucial to ongoing oversight of transborder data flow: the Council of Europe's *1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (Convention 108),[662] and the *1980 Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, drafted by the Organization for Economic Cooperation and Development (OECD).[663] Those rules were devised to deal specifically with personal information that crosses international borders, targeting the adequacy of protection afforded in the exporting country. The former, Convention 108, was devised in 1981 and has been described by the European Data Protection Supervisor as "the only legally binding international treaty dealing with privacy and data protection.[664] Privacy advocates recognized in the Convention 108 an opportunity to close a gap in data protections: the ECHR was a 'closed' instrument, that is, one not

---

[660] Francisco J. Rivera Juaristi, *U.S. Exceptionalism and the Strengthening Process of the Inter-American Human Rights System,* Human Rights Brief (2012), http://www.wcl.american.edu/hrbrief/20/2juaristi.pdf (noting that US exceptionalism has left the Inter-American Human Rights System vulnerable to attacks aimed at undermining its legitimacy and credibility.)

[661] Data disclosure affects reputation in that its revelation can affect social, financial or professional tasks, status, or opportunities.

[662] Council Of Europe Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data (ETS No. 108), (Jan. 28, 1981) (108 Convention). *See further* Graham Greenleaf *"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?* 29 COMPUTER L. & SEC. REV. (2013), http://ssrn.com/abstract=2262296 (documenting efforts to globalize Convention 108 to protect the transborder flow of data related to EU citizens and to enjoin non-European states in protection of their citizens within a globalized information flow and communications environment).

[663] OECD Privacy Guidelines (2013) http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. *For OECD Commentary on secondary use of data and enforcement of privacy guidelines see* ICT Regulation Toolkit, CH 1.7 *New Technologies and their Impact on Regulation,* http://www.ictregulationtoolkit.org/1.7 - note1, and OECD Cross Border Privacy Law Enforcement, (2007), http://www.oecd.org/document/25/0,2340,en_2649_37441_37571993_1_1_1_37441,00.html (highlighting data leakage and privacy law enforcement across geopolitical borders). *For a historical overview see also* Jennifer Stoddard, Thirty Years After The OECD Guidelines, (2011).

[664] European Data Protection Supervisor, *Data protection legislation Q&A,* https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/.../QA/QA2; *See also* Sylvia Kierkegaard, *et al., The review of the Council of Europe Data Protection Convention 108,* 23 COMP. L. & SEC. REV. 223, 223-4 (2011) (Kierkegaard).

open to participation by non-European or non-member states.[665] It applies to both private and public authorities, such as police organizations, but has been heavily criticized for lack of enforcement mechanisms and for its Euro-centered membership.[666]

It provided the framework for the 95 Directive in the mid-1990s when data privacy regulation was viewed as "a niche activity".[667] Today, Internet use is no longer an exclusive activity: even the purchase of a morning coffee routinely involves computer-based caching or storage of personally identifying information such as name, banking data, geo-location, and consumer preferences.

The OEDC guidelines, the 95 Directive, and Convention 108 are crafted using "technologically neutral" language to avoid the dating of legal instruments by too specific a reference to the technologies intended. They provide broad principles that serve as a template for the more specific and practical details that will become law as the EU Data Regulation.[668] The Convention 108 places more emphasis on protection of human dignity and human rights through individual control of our data but does not expressly mention "reputation" or the personal cost of data leakage.[669]

Similarly, the OEDC Guidelines, the first internationally agreed-upon set of privacy principles, addresses the importance of consumer information to the global economy and foresees the vulnerability of individuals to automated processing of their personal information. While the original guidelines do not express concerns over

---

[665] Convention 108 drafting involved representatives from Australia, Canada, Japan and the United States, which was carried out in close collaboration with the OECD. *See further,* Jorg Polakiewicz, *Convention 108 as a global privacy standard?* International Data Protection Conference, Budapest (17 June 2011), http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/Convention_108/.

[666] Polakiewicz, *id.*

[667] Directive 95/46/EC Of The European Parliament And Of The Council Of 24 October 1995 On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (95 Directive).

[668] Technologically neutral language has been defined by the EC Opinion of the Economic and Social Committee on the Proposal For A Council Recommendation Concerning The Protection Of Minors And Human Dignity In Audiovisual And Information Services, OJ C 214 (10 July 1998) at 25 para. 3.2.5: "Regulation should be 'technology-neutral': as few as possible new regulations, policies and procedures should be specific to the new services".

[669] *Propositions of Modernization,* The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, ETS 108 Preamble ("that it is necessary, given the diversification, intensification and globalisation of data processing and exchanges of personal data, to guarantee human dignity and the protection of human rights and fundamental freedoms of every person, in particular through the right to control one's personal data and the processing of such data".)

individual reputation, revisions in 2013 mention reputation for the first time within the context of the "reputational impact" and "loss of trust or confidence" caused to individuals in organizations that experience a data breach, whether by inadvertence, negligence, or victimization at the hands of data thieves.[670] Reputation as an individual right, within the context of data protection, is a legal principle that has developed more in the breach – driven more by punitive than precautionary intentions.

Both the 108 Convention and OEDC Guidelines are under continuous review and part of a push for global consensus on universal regulation of personal data collection. Despite those efforts, they have been criticized as ineffectual, as "burdensome to those whose motives are benign and ineffective towards those more malignly inclined." [671]

On a more regional basis, the 95 Directive was created to regulate the misuse of personal data before the popularization of the personal computer. The Directive is the predecessor to the proposed omnibus EUDR that would update and expand the EU data collection regime to accommodate the emergence of the Internet, other digital communications, and data collection technologies that were not in existence when the 95 Directive was implemented. The EUDR's more novel provisions will grant the right of access to data by the data subject[672] and the right to an effective remedy for leakage before a complex system of administrative tribunals.[673] It will also regulate, on a mandatory basis, any Internet postings that are no longer true, are outdated, have been collected or retained without the data subject's consent, or are embarrassing to the reputation of the data subject who can request their deletion.[674] The proposed EUDR

---

[670] Supplementary Explanatory Memorandum To The Revised OECD Privacy Guidelines, 26 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[671] Kierkegaard, *supra* note 664 at 231.

[672] Article 8 states (in part):

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

[673] Article 47 states (in part):

"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective or before a tribunal in compliance with the conditions laid down in this Article."

[674] Under Article 17, data subjects are granted the right to "obtain from the controller the erasure of personal data relating to them […] and from third parties the erasure of any links

makes specific mention of the protection of "reputation" eleven times in the draft document.[675]

With the accelerated saturation of the communications market with digital media, transfers across geopolitical borders have become a major concern. The 95 Directive generally restricts the transfer of personal information about identifiable individuals from the EU to the United States, unless there is "adequate protection" for such information when it is received in the United States or third party countries. The resultant Safe Harbor regime has come under review with the EUDR preparations because its level of protection for data of EU citizens is less rigorous than that demanded of exporters of such data from one EU country to another.[676]

Two additional directives relate expressly to online information and aim at protecting personal reputation. *The Electronic Commerce Directive*, (e-Commerce Directive)[677] effective since 2000, provides legal certainty for EU businesses and consumers alike on issues such as information requirements for online service providers,[678] the execution of electronic contracts, and limitations of liability of intermediary service providers (ISPs).[679] Under the e-Commerce Directive, ISPs are subject to the law of the Member State in which the service provider is established. In turn, the Member State whose residents receive the service cannot arbitrarily restrict incoming services. In addition, the e-Commerce Directive encourages administrative cooperation between the Member States and the individual user through a balancing of self-regulatory actions. Examples of services covered by the e-Commerce Directive include e-newspapers, the online sale of books and videos and services (financial advising and travel services) as well as online advertising, professional services from

---

to, or copy or replication of that data", where the data are no longer necessary in relation to the purposes for which they were collected, for which that individual withdraws consent or objects to the processing of his/her personal data, or where the processing of such data contravenes other parts of the Regulation.

[675] In recital 67, for example, it states: "A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to *reputation." [emphasis added].*

[676] *See, for example,* Paul M. Schwartz & Daniel H. Solove. *Reconciling Personal Information in the United States and European Union,* 102 CAL. L. REV. (2014) (Reconciling).

[677] 2000/31/EC.

[678] For example, agents who receive tax information filed online.

[679] This paragraph is informed by *The EU Single Market: E-Commerce Directive,* European Commission (Mar. 20, 2014), http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm.

lawyers, doctors, and estate agents, and entertainment services including basic access to the Internet.

The second directive influencing online personal data is the *Directive on the Retention of Data* (e-Privacy Directive)[680] that relates to publicly available electronic communications or public networks, such as mobile phone and texting data plan companies. The Directive advises those companies that they have to store citizens' telecommunications data for a minimum of 6 months and a maximum of 24 months, to allow for official scrutiny by government agents if authorized by law, but is intended to curb data retention beyond an individual's original consent. The directive enables the police and security agencies to request access to details such as the IP address and time of use of every email, phone call and text message sent or received. A 2014 decision of the CJEU, *Digital Rights Ireland Ltd. v Ireland & Karntner Landesregierng & others*, ruled certain provisions of the e-Privacy Directive are unconstitutional in that they are so broad as to permit mass surveillance by state authorities that challenge individual and fundamental human rights.[681]

Across the pond, there appears no pan-American legal regime for privacy or reputational protections. The federal *Privacy Act of 1974* arose out of concern in the 1960s and 1970s for protecting individuals from the increasing capabilities of computer systems to compile and store personal data.[682] Its aim is to protect records that are retrievable by the use of personal identifiers such as a name, social security number, or other identifying data. A data subject can prohibit disclosure of her data: her written consent is needed before records are disclosed and she can request correction of any

[680] Directive On The Retention Of Data Generated Or Processed In Connection With The Provision Of Publicly Available Electronic Communications Services Or Of Public Communications Networks
2006/24/EC (15 March 2006), amending Directive 2002/58/EC [ePrivacy Directive].
[681] *Digital Rights Ireland Ltd. v Ireland & Karntner Landesregierng & others* (Joined Cases C-293/12 and C-594/12) CJEU (April 8, 2014) seeking preliminary ruling on ePrivacy Directive (OJ 2006 L 105, p. 54) in the light of Articles 7, 9 and 11 of the Charter of Fundamental Rights of the European Union (Digital Rights Ireland).
[682] *Privacy Act Of 1974*, (Publ. L. No. 93-579), 88 Stat. 1896 (December 31, 1974), as amended 5 U.S.C. §552a. The federal law introduces a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals as maintained by federal agencies.

information she finds is incorrect.[683] The Privacy Act addresses only data collection by federal agencies; states each have their own privacy law regime. It is not referenced often in the US jurisprudence selected for examination in this chapter. The US system is developing in a more *ad hoc* and sectoral fashion than the harmonized and uniformly applicable system within the EU region. For example, each of the following federal US laws addresses discrete sectors of online privacy: the *Children's Online Privacy Protection Act*[684]; the *Health Insurance Portability and Accountability Act*[685], and the *Cable Communications Policy Act of 1984.*[686]

Privacy principles underscoring US legislation reinforce the concept of a "right to be left alone" and a somewhat more amorphous concept of the "right of personality" than that recognized by French and German legal traditions, as first articulated in America by Warren and Brandeis in the 1890s.[687] As suggested above, the US system incorporates legal principles contained in the US Bill of Rights[688] as enshrined in the amendments to the US Constitution. Although neither the US constitution nor its amendments expressly refer to "privacy" or "reputation", the US Supreme Court in its federal jurisdiction has given definition to rights to personal privacy as against the state through such decisions as the 1973 *Roe v Wade*[689] case (invoking the right to privacy to protect a woman's choice to have an abortion), *Griswold v Connecticut*[690] (a 1975 decision protecting the rights of married couples to contraception use), and *Lawrence v Texas*[691] (recognizing in 2003 the right to privacy regarding the sexual practices of same sex

---

[683] *The Privacy Act,* US Department of Health and Human Services, https://www.law.cornell.edu/uscode/text/5/552a .
[684] (COPPA), 15 U.S.C. §§ 6501-6506 (Pub.L. 105-277), 112 Stat. 2681-728 (October 21, 1998).
[685] 42 U.S.C. §§300 & 29 U.S.C. §§1181 *et seq* (Pub. L. No. 104-191), 110 Stat. 1936 (1996)
[686] 66 U.S.C. (Pub.L. No. 98-549), 98 Stat. 1984 (26 January 1983).
[687] Warren & Brandeis, *supra* note 112 at 205 (citing continental European reliance on the concept in their privacy laws).
[688] As incorporated in the Amendments to the US Constitution; notably the right to free speech is articulated (1st Amendment), as well as due process (14th Amendment) and freedom from unlawful search (4th Amendment: "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").
[689] 410 U.S. 113 (1973).
[690] 381 U.S. 479 (1975).
[691] 539 U.S. 558 (2003).

couples).[692] Constitutional protection usually excludes private activities between citizens, who must pursue actions in private law, and is less stringent for celebrities, public officials, or participants in newsworthy events. Individual states also recognize privacy as a defensible right, as seen in the constitutions of the states of California[693] and Montana[694].

Data protection in the US has also been uniquely shaped by laissez-faire economic policies that privilege private industry in the digital age and so present more complex challenges to individual privacy rights.[695] As a result, there is no single data protection regime comparable to the EU's 95 Directive or EUDR, although policymakers and academics now urge a move in that direction.[696] Regulation has proceeded on an industry-specific basis, relying more on commercial and individual self-regulation, as can be seen in such federal legislation as the *Cable Television Protection and Competition Act* (1992)[697] and the *Fair Credit Reporting Act.*[698] The latter, designed more as a credit history protection tool than a privacy law, meets growing concerns over automated collection and storage of personal data. It allows individuals to check and correct their credit information and restricts credit reporting to authorized organizations.

---

[692] *See* contra *Paul v Davis,* 424 U.S. 693, 96 S. Ct. 1155, 47 L. Ed. 2d 405, (1976) (wherein the US Supreme Court determined that "[the Plaintiff's] interest in reputation is simply one of a number which the State may protect against injury...[a]nd any harm or injury to that interest, even where as here inflicted by an officer of the State, does not result in a deprivation of any "liberty" or "property" recognized by state or federal law, nor has it worked any change of respondent's status as theretofore recognized under the State's laws.)

[693] *CA Const*. Art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.")

[694] *Mont. Const*. art. 2 § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest").

[695] *See further* Framework For Global Electronic Commerce, United States Government Report, Washington DC, (1 July 1997) promoted by former US President Bill Clinton and former US Vice-President Al Gore, http://Clinton4.Nara.Gov/WH/New/Commerce/.

[696] Schwartz & Solove, Reconciling *supra* fn 676 at 1816, (at note 2 citing recent initiatives such as the Department of Commerce Report Internet Policy Task Force, Commercial Data Privacy And Innovation In The Internet Economy: A Dynamic Policy Framework (2010) And The Federal Trade Commission's Protecting Consumer Privacy In An Era Of Rapid Change.)

[697] *Public Law* §102-385, 102 Stat.

[698] *Fair Credit Reporting Act 1970,* (Pub. L. No. 91-508), §601, 84 Stat. 1128, *codified as amended,* 15 U.S.C. §1681-1681x (Oct. 26, 1970) 15 USC §1681 *et seq.* (Pub.L. 113-142).

Another outcome of US concern over data collection was the drafting in 1973 of the *Code of Fair Information Practices*. That code of principles had significant input from the US Department of Health and Human Services that was concerned about individual privacy amidst the burgeoning collections of personal information within their agencies. That input also led to the federal *Privacy Act of 1974* mentioned above. The Federal Trade Commission (FTC), an independent agent of the US government devoted to consumer protection and fair competition practices since 1914, oversees enforcement of Fair Information Practices, emphasizing principles of Notice, Choice, Access, and Security. The FTC has powers of sanction over companies that breach those principles, primarily through hefty fines.[699]

In conclusion, the European model presents a more comprehensive, uniformly developed, and administratively centralized legal regime with a more accessible internal organization than the US system. With data information authorities in place once the EU Data Regulation is enacted, EU citizens should have a 'one-stop',[700] streamlined, and affordable resource to meet their need of protection or redress for both online exposure of personal reputation and excesses of online data retention. The US sectoral system, in contrast, relies on self-regulation, in deference to commercial and individual free speech rights and freedom of information, with the FTC as the oversight mechanism for any commercial practices that threaten consumer protection. The OAS forum does not appear to figure prominently in the US regarding human rights issues around misuses of personal information. A search of cases decided by the OAS Committee in recent years does not identify any US-related parties. The US has not made frequent use of its provisions, preferring instead the international OEDC principles and the domestic Fair Information Practices.

The borderless flow of personal information enabled by the Internet and Big Data collection, and the different laws it inspires on either side of the Atlantic, results in two significant legal issues that challenge any individual trying to protect or recover her reputation from online attack or sabotage: jurisdiction and choice of law. Once a

[699] *See further* Federal Trade Commission, http://www.ftc.gov.

[700] Vivian Reding, *Data Protection Day 2014: Full Speed on EU Data Protection Reform,* Press Release (7 Jan. 2014), http://europa.eu/rapid/press-release_MEMO-14-60_en.htm (explaining the Regulation's 'one-stop' policy and proposing that every company operating in the single market should have a single regulatory interlocutor in the EU).

victim decides to entrust her reputational recovery to a lawyer and decides on a cause of action, they must reach consensus on the most favourable forum in which to file suit. That decision determines the choice of applicable law. In the next section, I examine how the Brussels I mechanism, in tandem with the Rome II statute, was intended in principle to provide certainty and flexibility for such procedural decisions facing EU plaintiffs. We also see how a decision of the CJEU has given such a wide interpretation to those principles, and others listed above, with the resultant clouding of the very legal certainty that they had intended.

b EU/US Jurisdiction & Choice of Law in Internet Decisions

Personality rights have been described as one of the most contentious areas of private international law.[701] When tortious conduct involving personal data or defamatory content crosses national borders the issue of a multistate conflict of laws arises.[702] On the personal level, such conduct can create devastating exposure for the private citizen who needs to know where to bring a lawsuit. It should also be reasonably foreseeable to the defendant in which court she will be sued. That prospect has been of concern to Europeans since the initial formation of the EEC in 1958 and throughout its subsequent formulations to harmonize the laws across Europe.[703]

Given the unique architecture of Internet communications, such reputational harm now crosses borders widely and instantaneously and far more frequently. For example, as we saw in Chapter III, it is increasingly common for the operators of websites to use cookies in the browser programs of those visiting their sites to automatically collect their personal data. That activity brings the website operator based in a non-European country within the four corners of two EU legal instruments:

[701] Csongor Istvan Nagy, *Jurisdiction, Applicable Law and Personality Rights in EU Law – Missed and New Opportunities,* 8 J. Priv. Int'l. L., 251, 253 (2012). Also cited as Nagy, Csongor Istvan, *The Word is a Dangerous Weapon: Jurisdiction, Applicable Law, and Personality Rights in EU Law – Missed and New Opportunities,* 8 J. PRIV. INT. L. 251 (2012). (Nagy).

[702] For a US-EU comparison of *contractual* conflict of laws, a relatively new focus of private international law, *see* Tamas Dezlo Czigler, *Choice of Law in the Internet Age: US and European Rules,* 53 ACTA JUR. HUNG. 193 (2012).

[703] Adrian Briggs, The Conflict Of Laws, 1-5 (2013) (describing the "hybrid corpus" of private international law in jurisdiction and choice of law for non-contractual matters).

the Brussels I Regulation[704] (governing the *jurisdiction* or the location of courts for hearing transborder civil matters, including torts involving media) and the Rome II regulation [705] (addressing the *choice of laws* that will apply to non-contractual obligations). The third instrument, the E-Commerce Directive is also involved as it addresses publication of information on the Internet, particularly the issue of "mere conduit" or the determination of whether an Internet service is involved in content decisions (as a controller) or is a mere conduit (or transmitter) of such information.[706] What becomes important under Brussels I is not the location or domicile of the plaintiff but that of the defendant and, due to the variety of recognized exemptions, the geo-location where harm is experienced.[707]

With respect to reputational disputes, the Rome II Regulation has been a most anticipated mechanism for clarifying "all matters relating to privacy and personality rights, including defamation".[708] It marks an effort by the EU to coordinate judicial cooperation regarding civil matters with cross-border impact, such as the import and export of online information. Such harmonization is intended to reduce or eliminate forum shopping for plaintiffs not satisfied with the legal parameters within their home jurisdiction regarding personality or privacy rights. Information flow over the Internet has been a particular impetus for solidifying such rules[709] and there have been decades of preparation for its introduction.

The 1969 Benelux Uniform law on private international law marked the first attempt to codify choice of law for torts at a multinational level.[710] Although never

---

[704] Jurisdiction And The Recognition And Enforcement Of Judgments In Civil And Commercial Matters, 2001/44/EC, (22 December 2000) [Brussels I],

[705] Regulation On The Law Applicable To Non-Contractual Obligations, 2007/864/EC (11 July 2007) Article 1(2)(g) [Rome II].

[706] 2000/31/2000 [e-Commerce Directive].

[707] For a more detailed analysis of Brussels I, *see* The Brussels I Regulation, Ch 1, http://www.dutchcivillaw.com/content/brusselsone011.htm.

[708] On 11 July 2007 the European Parliament and the Council adopted the 'Rome II' Regulation on the law applicable to non-contractual obligations (OJ L 199, 31.7.2007, p. 40). Under Article 1(2)(g), 'non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation' are excluded from the Regulation's scope.

[709] Rome II, final sentence. Unlike directives, any regulation of the EU is "binding…and directly applicable" in each member state without the need for implementation into domestic legislation.

[710] Kurt H. Nadelmann, *The Benelux Uniform Law on Private International Law,* 18 AM. J. COMP. L. 406 (1970)(containing the draft law in English), 420.

passed into law, its basic principle was to choose the place of tortious conduct as the venue for a private action, subject to a very broad escape clause. If the consequences of the conduct were experienced in another jurisdiction with a different system of law, that system would determine any obligations flowing from the tortious conduct.[711] In 1972, the EEC drafted a Convention on Contractual and Non-Contractual Obligations that also adopted the place of conduct rule (*lex loci damni)* with an even broader escape clause.[712] With the development of Rome II, those efforts were to be realized.

Rome II has universal application in that it applies to conflicts of torts committed outside of the EU involving an EU citizen's reputation or privacy and so will have effect the very nanosecond that information regarding EU citizens crosses into a non-EU state. Rome II takes a major step towards the harmonization of EU private law regarding non-contractual disputes. Unfortunately for legal clarity and predictability, defamation law is not included in the provisions of Rome II at present, withdrawn at the eleventh hour due to a flood of protest from the publishing industry as well as a lack of consensus between the European Commission and the Council of Europe.[713] To illustrate the diversity of opinions that led to that decision, a meeting of the Council's Rome II committee in January 2006 debated thirteen different options for choice of law applicable to violations of privacy and personality rights.[714]

In the void left by Rome II's inapplicability to media issues, a study commissioned by the EC determined that domestic laws on the right to privacy and to freedom of expression varied widely between the Member States.[715] The jurisprudence of the Member States' High Courts showed a "difficult and imprecise balance" between

---

[711] Benelux Uniform Law, Article 14.

[712] EEC Draft Convention On Contractual And Non-Contractual Obligations, Article 10(2) (providing that, if the place of the tortious conduct and that of the resulting event were not connected, but another state had a predominant connection to the situation the law of that state could apply).

[713] Symeon C. Symeonides, *Rome II and Tort Conflicts: Missed Opportunities,* 56 AM. J. COMP. L. (2008).

[714] Jan-Jaap Kuipers, *Towards a European approach in the Cross-Border Infringement of Personality Rights*, 12 GERM. L. J. 1681, 1697 (2011), (where the author attributes the comment about the 13 options to Andrew Dickenson, *Privacy and Personality Rights in the Rome II Regime – Not Again?* Conflict Of Laws.Net (July 19, 2010), an article no longer available on the website cited.)

[715] Comparative Study On The Situation In The 27 Member States As Regards The Law Applicable To Non-Contractual Obligations Arising Out Of Violations Of Privacy And Rights Relating To Personality. JLS/2007/C4/028. Final Report, http://ec.europa.eu/justice/civil/files/study_privacy_annexe_3_en.pdf(EC Privacy Study)

the two values,[716] and that some Member States already had mature rules of law in this respect, while others did not. The study consulted professionals within the legal, judiciary, and other professional sectors[717] and concluded that the common principles enunciated in the *EU Charter of Fundamental Rights* (ECHR) that codified the *Convention for the Protection of Human Rights and Fundamental Freedoms (an unwritten set of principles on which the ECHR was based)*, developed within the Council of Europe, were insufficient to overcome the problems arising from divergences in national law, particularly involving issues of digital technology.[718] In fact, most countries were found to have made no special provision for conflict rules at all. Regarding the choice of law question, the vast majority of respondents were in favour of allowing the offended party to choose, based on the criterion of *lex locus damni* or the law in the jurisdiction where the damage occurred. With the borderless and amorphous nature of Internet transmissions, however, and the re-distribution options available to third parties, such a criterion has little practical meaning. For example, where does Internet harm occur, where read by the data subject, where accessed by the majority of public readers, or where the ISP is headquartered? Nevertheless, press and media associations preferred the law of the country in which the publisher is established,[719] a position clearly in their favour. The study recommends some combination of the three.[720]

The Brussels I Regulation, which provisions include non-contractual conflicts involving torts and including the media, provides a greater measure of clarity regarding jurisdiction. It holds that jurisdiction is to be exercised by the EU country in which the defendant is domiciled, regardless of his/her nationality.[721] In the case of legal persons or firms, domicile is the country where they have their central administration or principal place of business. For Google Inc., for example, domicile could be Mountain View, California but if the suit involves an individual plaintiff domiciled in France, the matter could involve Google France and hence a French court. Brussels I also provides

---

[716] *Id.*
[717] A total of 10,000 professionals were sent a survey questionnaire that yielded 371 valid responses.
[718] EC Privacy Study *supra* fn 715 at 6.
[719] *Id.* at 7.
[720] *Id.* at 9.
[721] Brussels 1, Article 2.

that jurisdiction can be determined by the "place where the harmful event occurred".[722] That provision is problematic in that it creates a number of possibilities along the chain of causation. In the *Bier Bv* case, the CJEU interpreted that clause to mean either the place where the harmful conduct occurred (the domicile of the defendant who posted the defamatory content, for example) or where the harm was experienced (the domicile of the plaintiff who suffered the resulting publicity, for example).[723] That interpretation was made in pre-Internet days, however, when points along the causal chain were more easily identified.

The *Bier* issues were revisited in 1996 CJEU case of *Shevill* that decided harm occurs where the defamatory material is accessed or read (offline newspapers in this case), not where the publisher is headquartered or where the plaintiff is located when discovering the offending content.[724] In that case, a French newspaper published an article accusing an English student of money laundering while on a three-month job in France. The newspaper was primarily marketed in France with some circulation in other countries. The CJEU ruling, therefore, made all locations where the newspaper was read an acceptable forum for bringing suit. Thus Miss Shevill was able to sue a French publisher in England in respect of the damage to her reputation caused by the 250 copies of France-Soir distributed throughout the UK.[725] Both the *Bier BV* case and the *Shevill* judgment of the CJEU, therefore, have done little to narrow the issue of jurisdiction, and continue to be applied to Internet cases by European courts despite the fact that *Shevill* dealt with newsprint, not new media.

Choice of jurisdiction is also a principal challenge for US cases, often involving EU litigants as well. One of the first major high profile decisions to highlight US-EU personal jurisdiction and choice of law issues involving worldwide Internet transmission was that of *LICRA & EUJF v. Yahoo!* handed down by the Tribunal de Grande Instance[726] in Paris in 2000.[727] The Internet company Yahoo! transmitted its

---

[722] *Id.,* Article 5(3) for all torts (non-contractual matters).
[723] *Bier BV v Mines de Potasse d'Alsace* [1976] ECR 1735 (Case 21/76) [BIER]. *See generally* Csongor Istvan Nagy, *supra* fn 701.
[724] *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415 (Case 68/93 [SHEVILL].
[725] *See further* Mark Vinall, *EDate Advertising and Martinez,* Informm's Blog (3 November 2011), http://inforrm.wordpress.com/2011/11/03/case-law-edate-advertising-and-olivier-martinez-—-mark-vinall/.
[726] Court of General Jurisdiction with three judges sitting *en banc*.

auction website throughout many countries of the world advertising Nazi paraphernalia and providing links to Nazi doctrine sites. Both activities violated criminal laws in France.[728] The relevant issues involved jurisdiction, sovereignty, and enforceability of court decisions involving the worldwide web. The arguments of the parties, as well as the interim and appellate judgments, address aspects of Internet and web functioning that set them apart from traditional communications media cases.

For the Paris suit, Yahoo! argued that the French court lacked jurisdiction because the goods were offered for sale within the US on the Yahoo site targeted for US users. In the alternative they invoked US constitutional protections of free (commercial) speech. The bases on which the Paris court found it had jurisdiction reveal the layer of complexity added to conflict of laws cases by the Internet context: it found 1) that the Nazi memorabilia auction was open to bidders from any jurisdiction, including France; 2) the display of such objects on the French website caused a public nuisance in France; and 3) Yahoo! Inc. was aware that French residents were accessing its site because it displayed advertisements of the paraphernalia in the French language on the pages accessed by those users. The Paris court then used an "effects" test to find liability on the part of Yahoo! Inc. The test is typically used in torts cases and, the Paris court maintained, was sui to the Internet context. [729] The test measures the effects within the jurisdiction of the transmission of the impugned website. The court held that citizens of France who accessed the Yahoo! site suffered the effects of being exposed to "an affront to the collective memory of a country profoundly traumatised by the[Nazi] atrocities".[730] It convicted Yahoo! Inc. and, in light of the company's insistence that filtering content out of France was technologically beyond its capabilities, ordered a

---

[727] L'Union Des Etudiants Juifs De France (UEJF) & La Ligue Contre Le Racisme et L'Antisemitisme [LICRA I] Inc. & Yahoo! France, T.G.I. Paris, May 22, 2000, http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (condemning Yahoo! for its violation of French Penal Code R. 645-1). *See further* Elissa A. Okoniewski, *Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet,* 18 AM. U. Int'l L. Rev. (2002): 295-339 (distinguishing the hands-off role of government in limiting free speech rights expressed in the US First Amendment from the more active role for government in *la liberté* in France through the 1789 *Declaration of the Rights of Man and of the Citizen*).

[728] *Code Penal de France,* Art. R.645-1, http://www.lex2k.org/yahoo/art645.pdf for English translation.

[729] *Id.,* 1173-74 (as originally devised for the pre-Internet case of *Calder v. Jones* 465 U.S. 783 (1984).

[730] *Id,* Plaintiff's Application at 4.

consultancy with Internet experts who advised on the installation of geo-location filtering technology in Yahoo! servers in California.

Yahoo! Inc. appealed the French decision to the US District Court for the Northern District of California in San Jose seeking a declaration that the French decision was neither recognizable nor enforceable in the US. Yahoo! Inc. had to argue in that case that the California court *did* exercise jurisdiction over the French defendants. [731] The gamut of arguments used by Yahoo! illustrates the lack of clarity within conflict of laws matters created by online cross-border transmissions, and the resultant expenditure of financial resources for the two human rights organizations and time to pursue or defend such actions. The defendants in the California action[732] argued lack of jurisdiction as they did not maintain offices, assets or agents in the United States. Yahoo! replied that jurisdiction could be established using the "targeting" approach that emphasized the defendants were 1) sending a cease and desist letter to Yahoo in Santa Clara demanding removal from the U.S. auction site of items constitutionally protected in the United States; 2) repeatedly using the U.S. Marshal's Office to serve complaints and orders on Yahoo! in Santa Clara; and 3) establishing an e-mail account with the US site and thereby agreeing to Yahoo's Terms of Service that dictated that users would submit to the personal and exclusive jurisdiction of the courts of California. [172]

The principal conflict of laws issue in the California action was whether another nation could regulate speech within the United States without violating its Constitution, on the basis that the speech could be accessed through the Internet in that nation.[733] In addressing that question the California Court distinguished between the less regulated speech freedoms under US law and those dictated by the French *Declaration of the Rights of Man and of the Citizen* of 1789. In the end, the Court found that the French order called on Yahoo! to make actions that would chill or sensor protected speech, thereby causing "irreparable injury", all in the name of comity between nations as required by international law.[734] Yahoo! was issued its declaration

---

[731] *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme,* Plaintiff's Application for Declaratory Relief, 169 F. Supp. 2d. 1181(N.D. Cal. 2001) (No. 00-21275); Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168, 1171 (N.D. Cal. 2001) [LICRA II] http://www.cdt.org/speech/intemational/001221yahoocomplaint.pdf.
[732] LICRA and Union des étudiants juifs de France.
[733] Okoniewski, *supra* fn 727 at 317.
[734] LICRA I, *supra* fn 727 at 1189.

that the First Amendment precludes enforcement within the geopolitical borders of the US of a French order that in effect regulates speech via Internet of an American corporate citizen.

A second noteworthy case addressing conflict of laws (between US states) involving the Internet was decided on a sliding scale of website activity from passive to active. A district court judge in *Zippo Manufacturing* case found jurisdiction, and liability, in a trademark infringement involving Zippo lighters.[735] Within US jurisprudence, a combination of the Zippo sliding scale and the *Calder* test (discussed *infra)* has been most instrumental in determining jurisdiction and choice of law for interstate Internet disputes.

On a broader philosophical scale, the *Yahoo! France* case raised the flag regarding Internet disputes that have created "endless litigation in disjunctive legal systems [resulting in] stalemates and unenforceable judgments".[736] Mark Greenberg points out that France and the US share a long history of support for a free press and democratic principles in governance and, within the Internet age, the free flow of information and opinions limited only by a need to preserve domestic and international peace and to respect cultural values in each country.[737] The wider practice question in cases of personal jurisdiction is whether litigation in multiple fora is the best way to resolve the international disputes that are arising with increasing frequency over the clash between web content and local laws. Greenberg argues that the litigation route is fruitless and endlessly draining of valuable resources, and proposes that the international community restructure certain principles governing international jurisdiction in Internet cases and adopt shared guidelines on online content available to the world market.[738] This proposal and others will be considered further in Chapter V.

More recently, the CJEU took the opportunity to address the "Gordian knot"[739] that the jurisdiction and choice of law issues have become in defamation and invasion of privacy cases. In the jointly heard Internet cases *eDate Advertising* and *Oliver*

---

[735] *Zippo Manufacturing Co. v. Zippo Dot Com Inc.* 952 F. Supp. 1119 (W.D. Pa. 1997).
[736] Marc H. Greenberg, *A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market,* 18 BERKELEY TECH. L.J. 1191 (2003), http://scholarship.law.berkeley.edu/btlj/vol18/iss4/6.
[737] *Id.,* 1198.
[738] *Id., 1192.*
[739] Nagy, *supra* note 701 at 251.

Martinez,[740] the claimants alleged that their personality rights had been infringed as a result of online publications on websites that were based in different EU Member States to those in which they lived. In *eDate Advertising*, the plaintiff was a German national and resident that had been convicted of murdering a well-known actor in 1993 and released on parole in 2008.[741] He complained that an Austrian website publication, *eDate Advertising*, infringed his personality rights by reporting his full name, conviction for murder, and the fact that he was appealing his conviction.[742] The Bundesgerichtshof or Federal Court of Justice for Germany asked for a preliminary ruling on Brussels I regarding jurisdiction and the enforcement of judgments in civil and commercial matters[743] as well as the e-Commerce Directive relating to matters of tort, delict, or quasi-delict published on the Internet and the place of jurisdiction.[744]

In the enjoined case of *Martinez*, the French actor Olivier Martinez, while living in France, complained of an infringement of his privacy and of the right to his image by the UK-based Sunday Mirror website in an article entitled "Kylie Minogue back with Olivier Martinez". The online coverage used a dated photograph to erroneously suggest Martinez had reunited with a former girlfriend.[745] In both the *eDate Advertising* and *Martinez* actions, domestic courts faced arguments from the commercial defendants that the court did not possess authority to make orders restricting publication outside their jurisdictions.

In the *eDate Advertising/Martinez* decision, the CJEU determined that (1) with an alleged infringement of personality rights by Internet, the person offended has the option of bringing an action either in the Member State where the publisher is established or before the courts of the Member State in which the "centre of his

---

[740] Joined cases *eDate Advertising v X* and *Olivier Martinez & Robert Martinez v MGN Limited*, [2011] EUCJEU C-509/09 & C-161/10, [2012] QB 654, Grand Chamber, http://curia.europa.eu/juris/document/document.jsf?docid=111742&doclang=EN (Edate/Martinez)

[741] *EDate Advertising GmbH v X* (25 October 2011) Bundesgerichtshof, Germany.

[742] Nagy, *supra* fn 701 at 252-253, acknowledges that "personality rights" and privacy are much broader concepts than libel and defamation and might cover, for example, the right to human dignity, bodily integrity, and private communications.

[743] *Id., at* note 43.

[744] *Id., at* note 28.

[745] *Oliver Martinez & Robert Martinez v MGN Limited* (25 October 2011) Tribunal de grande instance de Paris, France (Martinez).

interests" is based.[746] In the alternative, he may bring his action before the courts of each Member State in the territory in which content placed online is accessible; (2) the e-Commerce directive must be interpreted as not requiring specific conflict-of-laws rules for Internet torts that are stricter on Internet service providers than those applicable in their own Member State.[747]

The first issue, then, involved the interpretation of Article 5(3) of Brussels I when dealing with transborder jurisdiction and recognition/enforcement of foreign civil judgments.[748] As suggested above, that provision had been interpreted in pre-Internet days (the *Shevill* case) to mean that the plaintiff could sue for harm to her reputation either in the place where the newspaper publisher was established or in every Member State where the newspaper was distributed.

The second issue in *eDate Advertising/Martinez* dealt with whether the context of Internet media justified a discrete rule of jurisdiction and choice of law. The judgment offered such comments as "the Internet reduces the usefulness of the criterion related to distribution in so far as the scope…is universal";[749] and "…the placing online of content…is to be distinguished from printed matter in that it is intended…to ensure the ubiquity of that content;"[750] and further reference to "the impact which material placed online is liable to have on an individual's personality rights". The matter of jurisdiction for Internet harms to personality are best determined by the courts located where the plaintiff has his "centre of interests".[751] That place will usually be the location of his habitual residence; that presumption can be defeated by other indications such as the pursuit of a professional activity in a specific jurisdiction. According to the CJEU, the publisher of the harmful content is usually the best source to determine the plaintiff's centres of interest, but the whole "centre of interests" concept calls for further judicial clarification.

---

[746] EDate/Martinez *supra* 740, para 48.
[747] *Id.* at para 46.
[748] Article 5(3) "A person domiciled in a Member State may, in another Member State, be sued: in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur."
[749] EDate/Martinez *supra* fn 740 at para 45.
[750] *Id.*
[751] *id.* at para 48.

The CJEU decision is not clear regarding the establishment of a discrete law of Internet defamation or privacy breach. *EDate Advertising/Martinez* has also been criticized for exposing online publishers to the jurisdiction of extra-territorial EU courts outside their core markets and for holding them liable for the totality of damage suffered across the Internet.[752] The opinion of the Advocate General preceding the CJEU judgment characterizes the digital era as putting an end to the "markedly national context" of more traditional media and perpetuating the "territorial fragmentation of the media".[753] In the end, however, Villalón recommends a technologically neutral solution, or one that deems irrelevant, for purposes of establishing jurisdiction, whether the defamatory statement was published online or in the print media.[754] That conclusion is neither helpful nor practical, given the dramatic changes evinced by the idiosyncrasies of the Internet.

The message for present purposes is that efforts to conduct a *mutatis mutandis* application of pre-Internet laws to online tortious conduct, particularly as it moves across political borders, have not brought the clarity and flexibility that European practitioners, academics, and policymakers have been seeking since the early Benelux days. The CJEU in *eDate Advertising/Martinez* did not opt for revising or replacing the *Shevill* standard to accommodate the Internet, but merely tacked on the "centre of interest" criterion if the offending content were transmitted by digital means.[755] The Court has also been accused of turning a blind eye to the new vulnerability of the publisher,[756] a group whose numbers and professional characteristics have transformed with online authorship but whose pockets regarding damage awards remain quite shallow. In addition, the *eDate Advertising/Martinez* decision does not leave us much more certain of the particularities of the e-Commerce Directive that could address specific harms perpetrated online but not addressed by criminal law. On a broader scale, the CJEU decision appears to favour individual rights to private life over freedom of

[752] *EDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited,* 5RB MEDIA & ENT. L., http://www.5rb.com/case/edate-advertising-gmbh-v-x-and-olivier-martinez-and-robert-martinez-v-mgn-limited/.
[753] Advocate General Cruz Villalón.
[754] Jan-Jaap Kuipers, *Joined Cases C-509/09 & 161/10,* 49 COMMON MARKET L. REV., 1211 (2012).
[755] *Id.* at 1230.
[756] *Id.*

expression, a not-surprising conclusion in light of the EU continental history of commitment to fundamental rights principles.

c Domestic Responses

The US has long been considered defendant-friendly terrain for defamation and privacy suits, in view of the strong constitutional support for free speech and the entrepreneurial spirit that has fostered ICT and, more recently, digital technologies.[757] Although Brandeis and Warren envisioned a privacy regime shaped much like that in *fin de siècle* Europe, US commercial interests and the fastidious taxonomy of William Prosser regarding defamation and privacy took the laws of tort into a very different direction than for plaintiffs in Europe. The impact of the *Sullivan* case on US domestic law related to reputation should not be understated.[758] It has put strict limitations on libel suits and kept the burden of proof with the plaintiff to establish intent and actual malice in the case of a public figure or celebrity.[759] The US Supreme Court also eliminated the common law presumption of falsity in defamation cases: henceforth a plaintiff was required to prove fault in addition to falsity, even if it involved a private figure.[760]

Conflict-of-laws principles are relevant to privacy and defamation harms when content crosses geographical borders that are the rule in the world of the borderless Internet, transient populations, and off-shore servers. A resultant patchwork of differing domestic laws from one state to another can be seen in both the EU and the US. Within the EU, for example, English defamation law has historically held that a reverse onus, or proof of truth by the defendant, was required, while French law recognizes a broader

---

[757] Laura E. Little, *Internet Defamation, Freedom of Expression, and the Lessons of Private International Law in the United States,* 14 EUR. YEARBOOK PRIV. INT'L. L. (2012) 2.

[758] Sullivan, *supra* fn 143 for facts of the case. The Alabama lower court ruled in favor of Sullivan, finding that the newspaper ad falsely represented the police department and Sullivan. Upon appeal, the New York Times invoked the First Amendment. The US Supreme Court held for the newspaper, requiring actual malice for libelous claims of public figures, meaning with knowledge that they are false or with reckless disregard for the truth.

[759] Christopher J. Kunke, *Rome II and Defamation: Will the Tail Wag the Dog?* 19 EMORY INT'L. L. REV. 1733 (2005) (suggesting that, in America, the legal requirement of intent traditionally does not mean moral fault, but the intent to publish) 1762.

[760] Not so in the UK or Australia. *See further* Fredrick Oduol Oduor, *The Evolution of Internet Defamation Law: Will Dow Jones v. Gutnick Survive the International Legal Schisms and Legislative Onslaught?* (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1646168.

privacy right for which neither good faith nor truth is a defence.[761] As well, French judiciaries over the years have taken a defendant-friendly approach to libel laws, primarily through very tight procedural requirements.[762]For example, any suit for defamation against press or online statements must be filed within three months of the statement's first availability to the public, a requirement that necessitates tracking the first third party access date.[763] Meanwhile in the Netherlands and Germany, truth is not a complete defence to defamation. Regarding procedural rules, in Germany and Italy, the plaintiff may choose the most favourable law whereas the French and Austrians prefer the law of the location where the defendant's conduct occurred.[764] The Swiss, Portuguese, and Polish may apply either rule, as dictated by the facts of a particular case.[765]

Those substantive and procedural discrepancies can create considerable expense and doctrinal confusion for plaintiffs whose efforts to salvage their reputations involve bringing suit in several foreign jurisdictions. The Mosley case illustrates the legal complexity, as well as financial and personal burdens, created by those differences in domestic defamation laws.[766] Similarly, the *Yahoo! France* judgment ordering a blocking of Nazi paraphernalia commercial websites from France was determined to be inapplicable in California, the corporate headquarters of Yahoo! due to the refusal of a California court to recognize the jurisdiction of French courts over California corporations.

Similarly, defamation cases within the US are governed by myriad sectoral laws at the federal level and at the state level as well. Courts at both federal and state levels

---

[761] Alan Reed, *The Anglo-American Revolution in Tort Choice of Law Principles*: *Paradigm Shift or Pandora's Box?* 18 ARIZ. J. INT'L & COMP. L. 867, 878 (2001). The requisite mental element is one aspect of defamation law that is much changed in the *Defamation Act 2013*.

[762] Taylor Wessing, *Defamation and Privacy*, (2013). http://www.taylorwessing.com/uploads/tx_siruplawyermanagement/IP_Defamation_and_privacy.en.pdf . Over 70% of defamation cases are brought under the civil law, according to this source.

[763] Niri Shan, & Timothy Pinto (eds), *Defamation and privacy law and procedure in England, Germany & France,* Taylor Wessing (Spring 2006) http://www.taylorwessing.com/uploads/tx_siruplawyermanagement/.

[764] Mathias Reimann, *Codifying Torts Conflicts: the 1999 German Legislation in Comparative Perspective,* 60 LA. L. REV. 1297, 1307 (2000).

[765] Kunke, *Will the Tale Wag the Dog*, *supra* note 759 at 1738, notes 22-26.

[766] In his UK civil actions, Mosley chose breach of confidentiality law that avoided some of the doctrinal and procedural complexity of English defamation law.

has assigned priority to rights of belief and free expression (as inspired by the US First Amendment), rights against unreasonable search and seizure (Fourth Amendment), the right against self-incrimination (Fifth Amendment regarding personal information), and the provision that enumerated rights do not abrogate those not expressed in the Bill of Rights (Ninth Amendment).[767]

Substantive law issues vary from one US state to another, such as separating public figures in Texas law into all-purpose and limited-purpose agents of government.[768] Virginia defamation law recognizes as a *per se* cause of action implications that the plaintiff is unfit to perform the duties of an office or employment of profit, or lack of integrity in the discharge of such duties.[769] Pennsylvania maintains a wire service defence on its books for the republishing of a news item from a "repu news service".[770] As indicated below, several states maintain criminal defamation laws despite renewed appeals within state legislatures and in Congress to abolish them.

Reliance in some US states on the jury system for private actions in defamation and privacy intrusions has resulted in monetary awards of a size unheard of within most common law countries in Europe. For example, a Florida jury in 2006 awarded $11.3 million in damages to Susan Scheff for Internet defamation. The Broward County, Florida resident was inundated with caustic messages posted by a Louisiana resident charging that Scheff was a "con artist" and a "fraud", allegations that turned out to be completely false.[771] Plaintiff Scheff was aware the defendant would be unable to satisfy judgment, but even offered to meet her own costs to achieve vindication against the Dutch courage with which the Internet seems to imbue online defamers.[772]

---

[767] Amendments to the US Constitution comprise the US Bill of Rights.
[768] *Texas Defamation Law,* Digital Media Rights Project, http://www.dmlp.org/legal-guide/texas-defamation-law.
[769] *Virginia Defamation Law,* Digital Media Law Project, http://www.dmlp.org/legal-guide/virginia-defamation-law.
[770] *Wire Service Defence,* Digital Media Law Project, http://www.dmlp.org/legal-guide/wire-service-defense.
[771] *Scheff v. Bock,* Broward County Circuit Court, FLA, Digital Media Law Project, http://www.dmlp.org/legal-guide/wire-service-defense.
[772] Laura Parker, *Jury awards $11.3M over defamatory Internet posts,* USA TODAY (Oct. 11, 2006), http://www.usatoday.com/news/nation/2006-10-10-internet-defamation-case_x.htm.

4.2 Private Law Responses

a What Plaintiffs Seek: Types of Remedy

The law addressing reputational injury is principally framed in Western democracies as private law claims in defamation, breach of privacy, or breach of confidentiality.[773] In addition, perpetuating rumour and gossip focusing on public figures is punishable in some EU Member States and some US states through criminal defamation laws. Plaintiffs who employ the private law to seek redress from online reputational injury, whether from posted content or leaking of personal data, are usually granted remedies that fall short of the scope of personal damage the Internet can incur. The most sought-after remedy is pecuniary,[774] with the implication that lost status does have financial worth. One US study has found that plaintiffs prefer financial settlements despite their reported lack of effectiveness in meeting their expectations.[775] Other remedial options include vindication through retractions (conveying the idea that the impugned trait or activity was wrongly reported), containment through injunctions (to stem the damage at source), and restitution through erasure mechanisms (self-censoring of stories, images, and data that are no longer true or that cause irretrievable damage to professional, social, and financial opportunities).[776]

The advent of new communication technologies has increased the availability of discursive remedies as well, thereby expanding immeasurably the audience for apologies, corrections, and rights of reply. With the resurrection of the French notion of *le droit a l'oublie*, or the right to be forgotten or right of oblivion, as contained in the proposed EUDR, another remedial variant is introduced: the deletion from the Internet or other digital sources of personal information or data that was once true within

[773] At public law, individual reputation is addressed through crimes of cyber-bullying, identity theft, extortion, or harassment.

[774] Damage awards are customarily allocated in two categories, compensatory (or actual) damages and punitive damages (known as exemplary damages in Cyprus, England and Wales where they are extremely rare). There are other modifying terms placed in front of the word damages like "liquidated damages," (contractually established damages) and "nominal damages" (where the court sets a figure to reprimand the defendant, such as awards of one dollar).

[775] Randall Bezanson, *Libel Law and the Realities of Litigation: Setting the Record Straight*, 71 IOWA L. REV., 226, 227 (1985). *See contra* Ardia, *supra* note 10 (reporting results of a study in Iowa that plaintiffs prefer retraction to pecuniary settlements.)

[776] *Id.* at 703. Criminal remedies include penal consequences such as incarceration, fines, probation, community service, or other methods of public shaming.

certain defined contexts but that is no longer accurate or whose collection or publication will bring embarrassment and hence is no longer desirable.[777]Critics of such mechanisms are uncomfortable with the self-censorship, revisionism, or filtering functions they enable.

The right of reply, or *le droit de réponse* in France, is of particular interest because it is available in most EU jurisdictions to varying degrees, except in the UK, but is not recognized as a right of remedy in the US.[778] The principle holds that the correction of the offending statement is offered through a counter declaration prepared by the plaintiff and published by the disseminator of the original statement.[779] The right is available in some jurisdictions even in non-tortious circumstances if the statement is incomplete or the result of "non-culpable ignorance" of the falsity.[780] In some EU Member States, the right extends to family members if the subject of the press account is deceased.[781]The *droit de réponse* extends farthest in France, where press reports of every kind, whether false or mere expressions of opinion, even artistic or scientific critiques, hold a right of reply.[782] The right even applies if the plaintiff is only indirectly named (designé) or referred to in the statement.[783] The *droit de réponse* is not a promising remedy for online defamation or privacy incursions because, at the time of publication of the reply, a large portion of the reputational damage has been incurred through retransmissions, retweets, and other methods of third-party dissemination that forms a convoluted network not reproducible for response.

David Ardia suggests a more conceptually based taxonomy of remedies that measures the societal harm experienced by the plaintiff: pecuniary loss to the plaintiff;[784]

---

[777] That concept is examined in more detail in Ch. 5 *infra*.
[778] William Bennett, *Rome II and Defamation,* British Institute of International and Comparative Law (BIICL), http://www.biicl.org/files/5177_bennett_27-09-10_biicl.pdf (2010).
[779] *Right of reply as a private law entity,* René David (ed.) International Encyclopedia Of Comparative Law, 163, 164 (1986).
[780] *Id.* In those cases, the aggrieved party must pay costs of the reply, if determined by the judge to be just.
[781] Characteristically by the children, spouse, parents, and siblings in that order.
[782] Other related systems of law, in Italy and Greece for example, carry similar provisions.
[783] *Id.* at 164.
[784] Ardia, *supra* note 10 at 292 (characterizing pecuniary loss in proprietary terms. His categorization gives the nod to Robert C. Post's three conceptual elements: reputation as dignity, honour, and property).

non-pecuniary loss to the plaintiff;[785] non-pecuniary loss to society of its social connections; the loss to society of its normative standards; and loss of meaningful discourse within the plaintiff's society. Ardia does not provide practical application as the law of remedies currently stands.[786]

b Causes of Action

i Defamation

"There is a great deal of the law of defamation that makes no sense."[787]

Defamation law is aimed at protecting reputation against harmful statements, whether framing the action as libel (written or permanent form),[788] calumny, slander (spoken or ephemeral form), insult, *desacato*,[789] or *lèse majesté*.[790] Defamation has been defined in American law as an oral or written statement which tends to "injure reputation in the popular sense; to diminish the esteem, respect, goodwill or confidence in which the plaintiff is held,"[791] and in English common law as words about a person that "excite adverse, derogatory or unpleasant feelings or opinions against him."[792] English common law has further developed three definitions that focus on the social harm caused. Defamation is made out 1) if the words tend to lower the plaintiff in the

[785] For Ardia those losses can be measured in emotional and physical distress.
[786] *Id. at* 293 (and as discussed in Chapter 2 *supra).*
[787] Prosser, *supra* n 156 at *737*.
[788] Generally considered to include video and other permanent digital forms of speech.
[789] "Disrespect" laws in many South American jurisdictions make it a criminal offence with penal consequences to criticize or show disrespect for the head of state or public officials. In its Report On The Compatibility Of "Desacato" Laws With The American Convention On Human Rights, OEA/Ser. L/V/II.88, doc. 9 rev. (17 February 1995), 197-212, the Inter-American Commission on Human Rights found such laws "lend themselves to abuse, as a means to silence unpopular ideas and opinions, thereby repressing the debate that is critical to the effective functioning of democratic institutions" (212).
[790] The term *lèse majesté* addresses the insult of a monarch. In Thailand, anyone who "defames, insults or threatens" the king or his family will be punished with up to 15 years in prison. *Thailand's lese majeste laws explained,* BBC NEWS (1 Dec. 2014), http://www.bbc.com/news/world-asia-29628191.
[791] W. PAGE KEETON *ET AL.*, PROSSER AND KEETON ON THE LAW OF TORTS, §111 at *773* (5th ed. 1984).
[792] *Case de Libellis Famosis*, *77* Eng. Rep. 250 (1606) as cited by James R. Bayer, *Defamation : Extension of the 'Actual Malice' Standard to Private Litigants, - Colson v. Stieg,* 59 CHI-KENT L. REV. 115 (1983). *Famosus libellus*, or written defamation laws, can be traced back to the Roman Empire, when the offense was often punishable by death. Insult laws or *iniuria* also existed in Roman times and evolved from bodily assault and other harms to the person.

estimation of right-thinking members of society generally";[793] if a publication "is calculated to injure the reputation of another by exposing him to hatred, contempt, or ridicule;[794] or if "it tends to make the plaintiff be shunned and avoided".[795]

Defamation has undergone a very uneven history in terms of its conceptual development, its location in public or private law, and the requisite elements for a claim in either civil or criminal law. As William Prosser summed up, the law of defamation is full of "absurdities for which no legal writer ever has had a kind word".[796]

In this section, I survey the general principles of defamation in both the EU and US jurisdictions, with case examples, and suggest in the footnotes further reading on more tangential points. An additional layer of complexity has been added with the emergence of the Internet and social media: primarily the challenge of anonymity, limitless dissemination, permanence of storage, and difficulties in defining and proving the requisite mental element. I will discuss each of those challenges in turn.

a Conceptual Differences

As the above definitions suggest, defamation in the US is conceptually more aligned with traditional English common law and tends to focus on case law regarding the loss of social esteem and goodwill, or a loss of social capital in economic terms. By contrast and as discussed in Chapter II *supra*, legal principles of continental Europe, primarily reflected in the ECHR and other statutes, tend to link reputation to one's dignity or honour among peers. To defame that dignity is to challenge the positive public appraisal of the person, and to defame his honour is to mar the self-appraisal of the person for his own public significance.[797] In the Germanic tradition, reputation is also linked to the concept of personality, a right of autonomy over one's name that German courts have determined survives death.[798] In contrast, most US law at federal

[793] *Slim v. Stretch* [1936] 2 All ER 1237, HL.
[794] *Parmiter v Coupland* [1840] 6 M&W 105;
[795] *Youssoupoff v Metro Goldwyn-Mayer Pictures Limited* [1934] 50 TLR 581, CA.
[796] WILLIAM PROSSER, HANDBOOK OF THE LAW OF TORTS, 737(4ed. 1971).
[797] Council of Europe, Defamation And Freedom Of Expression. *See also* the *French Press Act of 1881* that remained faithful to the spirit of the 1789 *Declaration of the Rights of Man and of Citizens* that proclaimed the freedom of the press "save to respond to the abuse of this liberty, in the cases determined by the law", ie to defamatory statements (art. 11).
[798] Hannes Rosler, *Dignitarian Posthumous Personality Rights - An Analysis of U.S. and German Constitutional and Tort Law*, 26 BERKELEY. J. INT'L L. 153 (2008) (illustrating that in the

and state levels does not tend to recognize the posthumous right to a good reputation or of third parties to sue for defamation to protect it.[799] The key rationale offered is that posthumous defamation actions would have a chilling effect on both historical recordkeeping and on journalism. That is a serious consideration given the public interest in maintaining historical debate and exercising "reasonable speculation" where records have gone amiss.[800] For those states that recognize posthumous reputational rights, it represents an important social value to have a person's dignity reinstated by survivors if its status is questionable his death.

Within the rights discourse, free speech has been viewed as the vehicle for the advancement of knowledge and the truth, as espoused in England by such theorists as John Milton and John Stuart Mill. European laws that define free speech rights traditionally balance those principles with a right to reputational privacy centered around home and family life. As discussed elsewhere, the right to reputation was first interpreted by the ECtHR to be subordinate to free speech; in 2004 it gained rights status of equal value.[801] The ECHR as an international convention within the EU has been particularly influential in gaining that status.[802] Any EU legal action involving defamatory content, then, would trigger a balancing of those two rights. In the US, the elements of the rights debate are similar, but debates over the relative merits of reputation and privacy have been dominated by the admonition to Congress contained in the First Amendment that it must make no law abridging the freedom of speech, or of

---

Mephisto decision, the German Federal Constitutional Court [BVerfG] established a right to posthumous personality protections).

[799] Kirsten Rabe Smolensky, *Rights of the Dead, 37* HOFSTRA L. REV. 763 (2009) (pointing out that the executor of an estate in the US cannot sue for the libel or slander of a deceased person, and proposing an 'Interest Theory' approach that would extent protections to the dead, similar to those of the mentally ill and infants, that would permit judges to make decisions affecting the decedent's dignity and honour based on cultural and social norms within his community.)

[800] Al McConnell, *Speaking Ill: an analysis of posthumous defamation,* https://alistairmcconnell.wordpress.com/essays/speaking-ill-an-analysis-of-posthumous-defamation/

[801] Lingens, *supra* fn 644. *For a conceptual background of reputation see* Ch 2, s. 2.1 *supra.* Lingens states: "With the article 10 case of *Chauvy and others v. France* in 2004 and the article 8 case of *Pfeifer v. Austria*[801] in 2007, the right to protection of reputation was established as a full Convention right under article 8 of the ECHR." *See further* Hugh Tomlinson, *Privacy and Defamation, Strasbourg blurs the Boundaries,* Inforrm's Blog (23 Jan. 2014), https://inforrm.wordpress.com/2014/01/23/privacy-and-defamation-strasbourg-blurs-the-boundaries-hugh-tomlinson-qc/.

[802] *For wording of articles 8 and 10 of the* ECHR, *see* fn 643ff.

the press.[803] Such an eminent role for free speech is justified for the free flow of democratic discourse and the development of rational human capacities. Anathema to such necessary opinion that keeps public officials trustworthy is any paternalistic interference of the state. Such signature concepts perpetuated the American Horatio Alger Jr. dream that participation and prosperity were determined by personal attributes, not social order.

b Public or Private Law?

We generally think of defamation as a matter for private law. In many jurisdictions, however, including some states within the US and some member states within the EU, defamation can involve the criminal law either as an alternative or an adjunct to private law. This topic is addressed more comprehensively in section 4.3(a) *infra* and the EU countries still practising criminal defamation are set out in Appendix B, Map 2 with penalties listed in Chart 4. I will provide an overview of defamation law elements and point out regional differences that add complexity to its application. I focus on US private law and its comparison to that of the UK, and provide a general overview of criminal defamation laws in the US and EU member states.

The involvement of the criminal law in individual reputation suggests a matter in which the state holds an important interest. Criminal defamation is much criticized as a heavy-handed response by the state to affairs of a more personal nature and as endowing autocratic regimes with physical enforcement mechanisms out of proportion to the offence. The hybrid nature of legislative response to defamation, addressing it variously as a tort or contract matter in private law, or as criminal libel, brings further conceptual confusion to an area of law that has come under historical criticism as replete with "meaningless and grotesque anomalies"[804] and doctrinal inconsistencies.[805] The result for both plaintiff and accused is uncertainty regarding jurisdictional and choice of law decisions in private law, differing standards of proof, and lack of clarity regarding remedies meted out by the courts. Discrepancies in criminal defamation laws among EU

[803] That provision is part of the original twelve constitutional amendments that comprise the US Bill of Rights.
[804] Van Vechten Veeder, *The History and Theory of Defamation Law,* 3 COL. L. REV. 546 (1903).
[805] Ardia, *supra*, fn 10.

member states is set out in chart form in Appendix B;[806] US states holding various forms of criminal defamation laws are similarly numerous and set out below.[807]

c The Requisite Elements

A case for defamation should exhibit the following elements: the publication to third parties of a harmful statement[808] which concerns the plaintiff and causes him public embarrassment and/or professional and financial suffering, and made without adequate research into the truthfulness of the statement.[809] When those elements are present, and the plaintiff is reduced in the social estimation of his community as a result, a private case in defamation is usually made out.

Regarding the form of the complaint, an action can be framed as defamation *per se* (a statement is so obviously defamatory according to prevalent social or moral standards that no proof is required) or as a *per quod* action (not so obvious, so the mental element becomes important). *Per se* actions have historically been made out in the following circumstances: where false statements relate to charges that a person has contracted a contagious or venereal disease; charges that a woman is of unchaste character; other untrue statements that tend to injure a person in his profession, trade, or business; or accusations of the commission of a crime involving moral turpitude. Of late, *per se actions* are becoming more restrictive as certain insults to reputation, such as calling a person a homosexual, are gaining social acceptance and hence no longer deemed to offend community standards or reduce one's esteem in society.

The role of truth in identifying a defamatory statement varies with the laws of particular jurisdictions. This variation can be seen in EU member states: for example in Sweden truth is an absolute defence; in Latvia, by contrast, truth is not a defence in law, but defamation can only be committed by the distribution of "fictions". In Croatia, truth

[806] Mike Harris, *The EU's commitments to free expression: Libel and privacy,* Index On Censorship, http://www.indexoncensorship.org/2014/01/eus-commitments-free-expression-libel-privacy/#footnote (2 January 2014).
[807] David Pritchard, *Rethinking Criminal Defamation,* 14 COMM. L. & POL'Y 303 (2009), (listing the following US states as having criminal defamation laws: Colorado, Florida, Idaho, Kansas, Louisiana, Michigan, Minnesota, Montana, New Hampshire, New Mexico, North Carolina, North Dakota, Oklahoma, Utah, Virginia, Washington and Wisconsin, as well as Puerto Rico and the US Virgin Islands). Colorado repealed its criminal defamation laws in 2012 further to the Colorado Senate Bill 102 (Sen. Greg Brophy).
[808] Some states further require that the statement be defamatory; others require it be false.
[809] Sullivan, *supra* fn 143.

is not a defence if the defendant acted with actual intent to harm the offended party's reputation. In Poland, defendants must prove, apart from truth, that they were acting in the public interest.[810] Within the UK, the onus of proving truth rested with the defendant prior to the *2013 UK Defamation Act* that shifted that onus to the claimant.[811] Again, further comparisons among EU member states are contained in Appendix B, particularly through the link provided.

In the US, truth is accepted as an absolute defence in some state jurisdictions, but not in others.[812] A plaintiff who is a public official or celebrity must prove both falsity and malice on the part of the defendant.[813] A statement does not need to be literally true in order for this defense to be effective, just substantially true in the legal sense. This means that even if the defendant states some facts that are false, if the "gist" or "sting" of the communication is substantially true, then the defendant can rely on the defense.

It can be argued that untruthful statements create social harm because they upset the "relational interest" that an individual has in maintaining personal esteem in the eyes of others.[814] Another social harm would be to put at risk of exposure a journalist's sources.[815] In a 2015 study of civil defamation laws within the EU for how helpful they are to journalists, it was concluded that most were unclear and confusing

---

[810] Scott Griffen, *Key Findings: Defences in Defamation Cases,* in Barbara Trionfi, *et al.* eds, Out Of Balance: Defamation Law In The EU, Report For The International Press Institute (10 Mar. 2015), http://www.freemedia.at/ecpm/defamation-law-report.html (providing a relatively complete comparison of defamation laws in EU states).

[811] *UK Defamation Act of 2013,* c 26. For an analysis of the truth defence debate, *see* Elizabeth Samson, *The Burden to Prove Libel: A Comparative Analysis of Traditional English and U.S. Defamation Laws and the Dawn of England's Modern Day*, 20 CARDOZO J. INT. & COMP. L. (JICL) (2012), http://ssrn.com/abstract=2170040. http://ssrn.com/abstract=2170040.

[812] *Cf* a claim for invasion of privacy in the US where truth provides no defence.

[813] Sullivan, *supra* fn 143 at 279-283. Sullivan did not prevail, as he could not establish that the statements were made with actual malice or that they related to him, at 285-292.

[814] Lyrissa Barnett Lidsky, *Defamation, Reputation, and the Myth of Community,* 71 WASH. L. REV. 1, 37 (1996); and Rodney A. Smolla, *Let the Author Beware: The Rejuvenation of the American Law of Libel,* 132 U. PA. L. REV. 1, 18 (1983).

[815] The issue of legal protection of the journalist/source confidential relationship is not settled at common law and affords different protections at the state and federal levels within the US, as set out in Rodney A. Smolla, *The First Amendment, Journalists, and Sources: A Curious Study in Reverse Federalism',* 29 CARDOZO L. REV. 1423 (2008), http://cardozolawreview.com/Joomla1.5/content/29-4/29.4_smolla.pdf.

and that, currently, "vagueness is the name of the game".[816] Only Ireland, Macedonia and the UK were named as having passed legislation specific to defamation that reasonably conforms to international standards and that would assist journalists.[817]

A consideration of the requisite mental element in civil cases of defamation also points up complex differences from one jurisdiction to the next. In the US, for example, prior to the 1964 case of *New York Times Co. v. Sullivan* a plaintiff had to prove the defendant's general intention to publish a false statement, or his negligence as to the truth of the statement.[818] With *Sullivan*, the US Supreme Court refined that mental element as one of more specific intent with respect to public officials; henceforth the plaintiff had to prove some malice on the part of the defendant.[819] The malice standard appears, when examining the *Sullivan* decision, to be less about finding ill will feelings toward the plaintiff and more about establishing a wider protection for press free speech. That higher standard has been rationalized as appropriate for public figures because they voluntarily expose their views to greater public criticism.[820]

A decade after *Sullivan*, the US Supreme Court clarified in *Gertz v. Robert Welch Inc.* that, unlike public officials or public figures, private individuals could secure a remedy in defamation simply by proving negligence, as opposed to a higher standard of intent, on the part of a media defendant.[821] So, current US laws have set negligence as an acceptable level of mental liability when a plaintiff is bringing an action against a publisher, including digital publishers such as Google, Yahoo! and Tumblr as well as individual publishers of online blogs and social media content.

---

[816] Griffen, *supra* fn 810 at *Key Findings: Civil Defamation,* FREE MEDIA http://www.freemedia.at/ecpm/key-findings/civil-defamation-laws.html.

[817] The study also notes that Austria, Croatia and Luxembourg have passed general media legislation that specifically addresses defamation and provides most relevant defences.

[818] Sullivan, *supra* fn 143 at 256.

[819] See *Gertz v. Welch, Inc.*, 418 U.S. 323, 342 (1974) (describing how the "New York Times standard" requires "clear and convincing proof that the defamatory falsehood was made with knowledge of its falsity or with reckless disregard for the truth" for suits involving public officials).

[820] Ellyn M. Angelotti, *Twibel Law: What Defamation and its Remedies Look Like in the Age of Twitter,* 13 J. HIGH. TECH. L. 430 (2013), https://www.suffolk.edu/documents/jhtl_publications/ANGELOTTI-MACROFINALFINAL.pdf; see also *Wolston v. Reader's Digest Ass'n Inc.*, 443 U.S. 157 (1979)(viewing the primary achievement of *Sullivan* as establishing the American approach to libel as basically governed by the First Amendment).

[821] Gertz *supra* fn 819.

In UK law, the mental element has long been a more onerous standard. In other words, by shifting the onus of proof onto the defendant, who cannot always raise proof that the impugned statement is true, the plaintiff under UK law was generally successful in her claim for damages. As a result of such rigid evidentiary rules, the UK had come to be described as the most 'claimant friendly' jurisdiction in the world[822] while America continues to be known as the most protective of free speech, even to the extent of protecting some falsehoods in the arena of public discourse.

The *UK Defamation Act 2013* (2013 UK Act) set out to rebalance, rather than rewrite, the common law of defamation. It sets the requisite standard of harm at *serious* damage, thereby weeding out more trivial cases, but also doing away with the presumption in law that defamation causes reputational harm.[823] The defendant retains the defence of truth, but s/he must prove a statement is *substantially* true. New defences of honest opinion and publication on a matter of public interest are also introduced. British defamation suits with journalist/publisher defendants have long called on the qualified privilege defence, as developed in the *Reynolds v. Times Newspapers Ltd.* decision.[824] A journalist could claim privilege if reporting in good faith, on a subject of interest to her, and made without malice. The defence has been eliminated in the 2013 UK Act, along with the defence of fair comment. The former has been replaced with a public interest defence [825] and the latter with honest opinion. More precisely, 'justification' becomes 'truth', and 'fair comment' becomes 'honest opinion'. Malice remains a requisite element to prove within the journalism context.[826] In terms of procedural changes, the presumption of right to trial by jury is abolished.

In light of the growing use of the Internet, several provisions of the 2013 UK Act address online defamation. The Act creates a new defence for operators of websites:

---

[822] Trevor C. Hartley, *'Libel Tourism' and the Conflict of Laws,* 59 INT'L & COMP. L. Q. 25, 26 (2010).

[823] In line with the decisions in Thornton v Telegraph Group Ltd [2010] EWHC 1414 (QB)and Dell'olio v Associated Newspapers Ltd [2011] EWHC 3272 (QB).

[824] *Reynolds v. Times Newspapers Ltd* [2001] 2 A.C. 127 (HL).

[825] That is, that the impugned statement was on a matter of public interest and the defendant reasonably believed its publication was also in the public interest. The publisher need not prove that it has met a standard of responsible journalism but can argue reasonable belief.

[826] This paragraph is informed by George Tamunokuro, *Limitations on the Freedom of Speech by Defamation in UK law,* http://www.academia.edu/6910942/Limitations_on_the_Freedom_of_Speech_by_Defamation_in_UK_Law.

they will not be held liable for defamatory comments made on their website if they can prove that the statement was not posted by them and, upon receipt of a defamation complaint, they followed a procedure outlined in the Defamation (Operators of Websites) Regulation accompanying the Act. The defence will fail, however, if the claimant can prove that it was not possible for her to find the individual responsible for making the post, she issued a notice of complaint regarding the offending statement to the defendant and the defendant failed to act according to the regulations. The question of whether unmediated user generated content will place its author under the Act as a publisher remains to be developed with future case law.

Finally, the 2013 UK Act creates a limitation period for filing a claim involving online conduct, and assigning liability for the regeneration of posted content. Known as the single publication rule, it sets a one-year limit from first publication for making a claim; that provision should prevent indefinite liability for online publications, including Internet archives.[827] The provision does not apply to third party re-publication. It does apply, however whenever a publisher provides a new link to a news article or publishes a new edition of a book or refreshes links to an older obscure article that later becomes newsworthy. It is also applicable for an article that gets tweeted around the world.[828] The legal test is whether the new link, edition, or broadcast is materially different from the original. The 2013 UK Act came into force January 1, 2014 and so old libel law will therefore still apply in many 2014–2015 defamation cases where the events complained of took place before commencement.

In the EU more broadly, there is a broad discrepancy in the application of civil defamation laws from one Member State to the next, as there is with available defences, costs to litigants, and damage awards.[829] Regarding costs, for example, a 2008 study of defamation actions for EU Members, conducted by the University of Oxford, determined that total costs to plaintiffs ranged from approximately 600 euros in Cyprus and Bulgaria to over 1 million euros in Ireland and England.[830] That vast range speaks to the various perceptions from one jurisdiction to another regarding the relative

[827] *Id.* at 9.
[828] *Id.* at 7.
[829] Harris, *supra* fn 806.
[830] *A Comparative Study of Costs in Defamation Proceedings Across Europe,* Centre For Socio-Legal Studies, University Of Oxford, 173 (2008). http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/defamationreport.pdf (2008).

importance of reputation to other civil claims.

Acceptable remedies include monetary damages, retraction, declaratory relief that the statement is untrue, and injunctive relief against further publication of a defamatory statement. In America, a defendant who disparages a plaintiff's professional reputation is additionally punished upon losing the action by being assessed special damages without need for the plaintiff's prove of specific harm.

I have examined the *2013 Act* of the UK in some detail above to exemplify the breadth and complexity of issues at play in instituting a defamation claim. While discrepancies in laws from one jurisdiction to the next raise the ever-present risk of libel tourism, major revisions such as the 2013 UK Act are aimed at eliminating that practice, as well as incorporating references to digital publishing that raises its own roster of legal challenges.[831]

d Internet Defamation

As discussed throughout this dissertation, digital technology has introduced a breadth of additional challenges to the legal response to reputational harm. Most problematic in terms of preparing a civil suit involving new media are 1) defining a victim's community; 2) identifying and establishing the liability of the content publisher; 3) identifying anonymous defendants; and 4) assessing the probative value of digital speech. Each of those challenges is discussed elsewhere in this dissertation,[832] but those legal questions ask legislators and judiciaries to think in digital terms rather than in geospatial, chronological, sequential, and hierarchical ones. Of interest here is how the jurisprudence of our highest courts can provide guidance for such new media legal issues. I will make general observations about both the US Supreme Court and the ECtHR in their roles as high-level adjudicators of cases involving new media. Not all the cases below use defamation as a cause of action; the need for judicial clarity regarding new media infuses many areas of law. I then contextualize those observations

[831] Re libel tourism in US and UK laws *see* Michael McFall, *American and English Libel Law - Which Approach is Best?* EUR. J. L. & TECH. (2012), http://ejlt.org/article/view/173/261 - _ednref29.

[832] Community is dealt with in sections 4.3(c) and 5.4(a); ISP liability is addressed in section 4.2(c); anonymity is addressed in section 3.2(a)(i); and digital speech is discussed in section 4.4 and 5.4(a).

with two recent cases: the ongoing American case before the US Supreme Court of Anthony Elonis and the 2013 case of *Delfi AS v. Estonia* before the ECtHR.

The US Supreme Court had an opportunity to consider the legal implications of the Internet's borderless ambit with three cases involving student online postings of a defamatory nature. The Court declined to hear three student social media cases in 2012 that would have assisted school authorities in determining whether they held authority to discipline students for online speech while off-campus.[833] The cases focused on the necessary balance between school authority to provide a harassment-free educational environment, the reputation of school personnel, and the online free speech rights of students when not involved in school activities.

In the first of the three cases, from the US Court of Appeals for the Second Circuit, the court found no violation of a student's First Amendment rights when educational authorities disciplined her for criticizing faculty in vulgar terms, using off-campus web postings.[834] A second case, from the Third Circuit Court of Appeals, found there was indeed a violation of free speech rights in 2007 regarding the disciplining of a student who created a MySpace parody of his principal from his home.[835] In a third case, from West Virginia, a high school student used her home computer to create S.A.S.H. (Students Against Sluts Herpes) and invited approximately 100 individuals to join, including students from her high school. Her discipline by school authorities was upheld as not in violation of First Amendment rights.[836] Those conflicting results could be attributed to the fact that the U.S. Supreme Court has never explicitly ruled on whether a school official may punish student speech that occurs outside the supervisory authority of the school. If they had, such discussions could have made valuable contributions to how to reconcile the limitless reach of online content with the concern for geographical borders in local administrative laws.

---

[833] David Kravets, *Supreme Court Rejects Student Social Media Case,* WIRED (1 Jan. 2012), http://www.wired.com/2012/01/scotus-student-social-media/.
[834] *Doninger v. Niehoff* (2d Cir. Apr. 25, 2011).
[835] *Layshock v. Hermitage Sch. Dist.*, No. 07-4465 (3d Cir. Jun. 13, 2011). A case with similar facts, *J.S. ex rel. Snyder v. Blue Mountain Sch. Dist*. No. 3:07-cv-585, 2007 WL 954245 (M.D. Pa. Mar. 29, 2007) was enjoined with Layshock for consideration by the 3rd Circuit Court of Appeals.
[836] *Kowalski v. Berkeley County Sch.*, No. 1098 (4th Cir. Jul. 27, 2011).

In none of those recorded appellate decisions was there much helpful deliberation on the new legal terrain in which we find ourselves when it comes to online communications. Paul Easton of Boston College Law School, in comparing several similar decisions, has determined there is a clear need for direction from the Supreme Court to prevent such results as a conflict between results of the Second Circuit Appellate Court and the Third Circuit Appellate Court due to use of a different constitutional standard for student online off-campus speech.[837]

Court watchers have commented critically that the most up-to-date Supreme Court precedent available to those appellate courts was a 1969 pre-Internet case involving the right of students to wear black armbands in class to protest the Vietnam War.[838] So, what the Supreme Court could have provided by hearing the three 2012 cases was much needed clarity on the legal boundaries between private online communications and school-related online speech that considers new media's borderless reach, persistent memory, architectural autonomy, and indeterminate audience. The Court's thinking in digital terms, rather than geospatial ones, is much needed.

The silence of the US Supreme Court regarding social messaging has been assessed by Professor Little of Temple University as attributable to the more general chill to digital speech created by the *Communications Decency Act*'s blanket protection of ISPs from publisher liability.[839] I would include in that chilling effect the continuing influence of the *Speech Act* of 2010 that sets a very high bar for enforcement of foreign judgments against US journalists. Without such public discussion by the Supreme Court, the nature of intermittent questions posed by individual justices that reveal a lack of technological acumen is troubling, as will be discussed *infra* regarding the *Aereo* case.[840]

The situation in Europe is much more encouraging. The CJEU and ECtHR have been relatively active over recent months in their observations regarding the liability of

---

[837] Paul Easton, *Splitting the Difference: Layshock and J.S. Chart a Separate Path on Student Speech Rights*, 53 B.C.L. REV. E. SUPP. 17 (2012), http://lawdigitalcommons.bc.edu/bclr/vol53/iss6/3.
[838] Edmund H. Mahony, *U.S. Supreme court Declines review of off-campus, online student speech case,* Hartford Courant, (Oct. 31 2011) (stating the last relevant Supreme Court decision was *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969) where the US Supreme Court found a school board regulation banning the wearing of armbands by students was protected speech under the First Amendment.)
[839] Little, *supra* fn *757* at 2.
[840] S. 4.5 *infra.*

Internet companies and web content hosts for allegedly defamatory content they transmit but do not read or edit. The CJEU decision in *Google Spain*, for instance, was landmark in its characterization of ISPs and Internet companies as 'controllers' of such content with attendant liability for third-party retransmissions and hyperlinks. The court also ventured into novel legal terrain in its consideration of the appellant's right to be forgotten and its allocation of responsibility for takedown decisions to Internet companies.

A 2014 preliminary ruling in a case before the District Court of Amsterdam put those *Google Spain* rulings to the practical test in a case involving deletion requests of an escort agency owner.[841] The appellant had been convicted and sentenced to six years' imprisonment in 2012 for attempted incitement of contract killing. That conviction is still under appeal. The man wanted to have links removed to online publications that defamed him by continuing to connect him to the crime. Although Google was willing to remove part of the search results he complained about, the search engine refused to comply fully with his request. The Amsterdam decision clarified the *Google Spain* position on permissible erasure:

> The [Google Spain] judgment does not intend to protect individuals against all negative communications on the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions.[842]

The Dutch judge pronounced as relevant the reporting of the conviction and negative media coverage, but found excessive the online repetition of those factors, not for factual background but to launch into a "slanging match' against the plaintiff. The decision also deals with search company liability for autocomplete suggestions and anonymization of certain content.

Two cases in courts of final jurisdiction address those issues, one before the US Supreme Court and the other at the ECtHR. In the first, a pending appeal of a criminal conviction for US citizen Anthony Elonis will challenge the US Supreme Court to determine the free speech rights of an ex-husband who used his Facebook page to post

---

[841] *Arthur van M.*, C/13/569654 / KG ZA 14-960 (19 Sept. 2014).

[842] Joran Spauwen and Jens van den Brink, *Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals,* Inforrm's Blog (27 Sept 2014), https://inforrm.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink/.

hostile messages about his community and his estranged wife.[843] Anthony Elonis claimed his posted content dealt with rap lyrics and was not intended to threaten or endanger the objects of his posts: he offered the defence that he was, in fact, just kidding. [844] One such posting stated about his wife:

> There's one way to love you but a thousand ways to kill you. I'm not going to rest until your body is a mess, soaked in blood and dying from all the little cuts.[845]

Elonis' lawyer suggests it is difficult with decontextualized online speech to distinguish humour or high drama from the intent to defame, demean, or frighten:

> Increasingly people who speak on the Internet…could be held subject to felony liability not because they intended to…threaten anybody but because somebody misinterpreted their comments as a threat…That is a risk on the Internet, where you're frequently speaking to people…without the context of tone of voice, body gestures, and frequently talking to people who you don't even know in the physical world.[846]

The Supreme Court has been clear that intended threats do not garner free speech protection if they engender imminent violence.

The court is invited to distinguish threats from protected speech such as hyperbole or "unpleasantly sharp attacks", a reference to Justice Brennan's comment in the *Sullivan* case about the outer limits of tolerated speech that attacks government and public officials.[847] Elonis is arguing in his appeal that the requisite intent for online threats must be *specific* intent given the looser speech used in the medium. That determination of intent in the absence of offline corroborating evidence is difficult when the mode of communication is Facebook postings that can employ two-dimensional,

---

[843] *United States v. Anthony Douglas Elonis*, Case No. 12-3798 (14 June 2013), US App. Ct. 3rd Cir.

[844] *No clear cut outcome for Supreme Court's Internet free speech case,* CBS NEWS (1 DEC. 2014), http://www.cbsnews.com/news/no-clear-cut-outcome-for-supreme-courts-internet-free-speech-case/.

[845] Sam Hananel, *Supreme Court considers extent of free speech over Internet,* PBS (30 NOV. 2014), http://www.pbs.org/newshour/rundown/supreme-court-case-considers-extent-free-speech-internet/.

[846] No clear cut outcome, *supra* fn 844.

[847] Sullivan, *supra* fn 143, where Justice Brennan speaks of a US constitutional history exhibiting "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, *and* that [such debate] may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials." (376 U.S. at 376 U.S. 270).

hasty, and impulsive venting and more spontaneous and emotionally charged rants that can be easily misinterpreted by readers. Also problematic is the determination of the intended community or audience given Elonis' claim the contents are rap lyrics.[848] The case is urging the Supreme Court to weigh in on the novel challenge of special intent involved in threatening social messaging.

The ECtHR has been recently active in providing precedent in the EU for some of those issues. In the 2013 case of *Delfi AS v. Estonia* the Court upheld an Estonian court ruling that an online news service was liable for defamatory comments, including anonymous postings, submitted by its users regarding news stories.[849] Delfi is an Internet news portal that publishes up to 330 news articles a day, operating out of Estonia, Latvia and Lithuania. The articles received about 10,000 readers' comments daily, the majority posted under pseudonyms. The comments in question were online responses to one article suggesting a majority shareholder in a local ferry company was endangering public safety. The contents were profane and explicit in their threats of physical harm and other criminal acts.

Delfi had taken wide precautionary measures regarding offending content. There was a system of notice-and-take-down in place: any reader could mark a comment as *leim* (an Estonian word for an insulting or mocking message or a message inciting hatred on the Internet) and the comment would be removed "expeditiously". Furthermore, there was a system of automatic deletion of comments that fielded certain stems of obscene words. In addition, a victim of a defamatory comment could directly notify the applicant company, in which case the comment was removed immediately, as was done in the instant case, with removal accomplished the same day. Delphi also published conditions of postings on it site, advising users that the comments were not its opinion and that the authors of comments were responsible for their own content.

In finding Delphi liable as publisher and controller of content, the ECtHR relied on a proportioned balancing of free speech and privacy protections under the ECHR. The minimal fine, 5000 kroons or approximately $427 US, provided little deterrent effect, however. The Court reasoned that Delfi benefited financially from comments posted on its server by individual users, and assigned Delfi a positive duty to monitor

[848] Hananel, *supra* fn 845.
[849] *Delfi AS v. Estonia*, no. 64569/09, §§ 7, 94, Eur. Ct. H.R. (October 10, 2013).

comments on predictably controversial articles it transmits. Long ranging implications of the decision could be that anonymous commentary might be vetoed by Internet portals and servers[850] and that industry reliance on automatic word filtering capabilities or posted notice-and-take-down notifications would be insufficient to avoid liability.[851] It has also been suggested, more controversially, that the decision affords more protection to the right to reputation, as contained in the ECHR article 8 right to privacy, than in previous ECtHR cases.[852]

Meanwhile across the Atlantic, until the US Supreme Court provides more jurisprudential direction for the above issues, uncertainty regarding the law of defamation's "shifting sands of assumptions and policymaking"[853] will persist in that country.

Other uncertainties remain: with regard to the particular society in whose hands our reputation resides, whom do jurists include in our online communities when they attempt to measure the extent of our shame and embarrassment? Where do we measure losses to social, financial and professional chances, within that online community or within the broader community? Are we, as social media users and victims, a composite of our communities both online and off? Current jurisprudence has not delivered clear legal thinking on those puzzling issues.

Another uncertainty is the question of how a monetary award, besides conveying exoneration, works to retrieve our good name or future opportunities. As has been seen in the *Mosley* case in Chapter III, the distributive capabilities of the Internet and offline texting perpetuate defamatory content and necessitate a serial protocol of court challenges in various jurisdictions. To date, Mosley has initiated actions in 22 countries within the EU based on Google links to *News of the World* publications. That iterative process is expensive in both real costs and emotional wear. The UK 2013 Act limits

---

[850] Padraig Reilly, *European ruling spells trouble for online comment,* Index On Censorship (10 Oct. 2013), http://www.indexoncensorship.org/2013/10/european-ruling-spells-trouble-online-comment/.

[851] *Id.*

[852] Neville Cox, *Delfi AS v Estonia: The Liability of Secondary Internet Publishers for Violation of Reputational Rights under the European Convention on Human Rights, 77* MOD. L. REV. 619-629 (July 2014) (suggesting such stronger berth given reputational rights in the ECHR would conflict with the UK Defamation Act 2013, s. 5(2): "It is a defence for the operator to show that it was not the operator who posted the statement on the website.")

[853] Ardia, Defamation, *supra* note 10 at 292.

actions against such retransmission as well with its single publication rule. As well, the lack of deep pockets with online publishers means that, unlike institutional media that maintains a keen interest in safeguarding professional standards in reportage, freelance authors of blogs, tweets, and e-magazines comprise a new crop of defendant with little ability to pay and hence a reduced fear of large damage awards.[854]

There is also a noticeable surge of injunctive relief awarded in Internet defamation cases, notwithstanding the timeworn equitable principle that "equity will not enjoin a libel".[855] That remedial development goes against years of judicial concern over prior restraint to free speech rights.[856] In a review by David Ardia of fifty-six decisions involving injunctive relief in US defamation cases, well over half were found to have been delivered since 2000 and over half by separate calculation, involved Internet speech.[857] As well, the nature of injunctive relief awarded has been either disproportionate to the harm threatened or technologically unfeasible. For example, judges have ordered defendants to cease mentioning a plaintiff's name online[858] or to take down a complete website for a single defamatory remark,[859] both remedies that ignore the Internet's capability for third party regeneration of the offending message and the resilient memory of Internet archiving. In addition, injunctions afford scant procedural protection for the defendant who is compelled to obey under threat of severe punitive sanctions, usually a hefty fine or period of incarceration. Interestingly, plaintiffs have confirmed in hindsight that apologies, corrections, or a retraction from the defendant would have sufficed.

---

[854] *See, e.g.,* David S. Ardia, *Freedom of Speech, Defamation, and Injunction*s, 55 WILLIAM & MARY L. REV. 4 (2013) (Ardia Injunctions).

[855] *See further* Stephen A. Siegel, *Injunctions for Defamation, Juries, and the Clarifying Lens of 1868,* 56 BUFF. L. REV. 655 (2008).

[856] *Id.,* at 5 (as opposed to *post facto* solutions that allow offensive speech and then sanction it for first amendment violation); for a more historical perspective, *see also* William O. Bertlesman, *Injunctions Against Speech and Writing: A Re-Evaluation,* 59 KY L.J. 319, 323 (1971); Estella Gold, *Does Equity Still Lack Jurisdiction to Enjoin a Libel or Slander*? 48 BROOK. L. REV. 231, 262 (1982).

[857] Ardia, Injunctions, *supra* note 853 at 189.

[858] *Apex Tech. Grp. Inc. v Doe,* No. MID-L-7878-09 (N.J. Sup. Ct. Law Div. Dec. 23, 2009) (order granting preliminary injunction); *Cochran v. Tory,* (No. BC239405, 2002 WL 33966354 (Cal. Sup. Ct. Apr. 24, 2002) (granting permanent injunction) but vacated 544 U.S. 734 (2005).

[859] *See e.g.* Ardia Injunctions, *supra* note 853 at notes 8, 9.

The differing views on whether new media journalism merits legal protection equal to that of traditional media can be seen in two final cases I discuss at this juncture: the California *Courtney Love* case and the Oregon *Obsidian Finance* decision. In the first, the plaintiff was arguing that her tweets were not bona fide journalistic statements while in the second the defendant maintained her blogs were journalism to the *Sullivan* standard and hence deserving of constitutional protection.

Celebrity Courtney Love was turned down when she asked her former lawyer Rhonda Holmes to administer the estate of her deceased husband, singer Kurt Cobain.[860] Love subsequently published tweets suggesting Holmes had "been bought off" and therefore had acted against her client's best interests.[861] Holmes sued in 2013 in the California Supreme Court for defamation on the grounds that Love's tweets implied Holmes had an association with organized crime, accusations that impugned her good name and professional reputation. In an unsuccessful motion for summary judgment, Love's lawyers proposed in oral argument that it is the nature of tweets to use "hyperbole and sensational language" characteristic of communications by social media that are not to be scrutinized too carefully or taken as carrying deeper meaning. They asked that claims made via Twitter *not* be held to the same legal standards as speech used by offline (or online) news organizations.[862] Love's counsel were asking that the law of defamation shift to create a lesser category of speech that not be held to professional publishing standards, particularly given its unmediated status.[863]

The judgment on preliminary motion determined that, when both the language and context of the offending tweets were considered, they were sufficiently akin to real time communications to proceed to trial.[864] In the context of defamation law, the rights

---

[860] Nancy Dillon, *Courtney Love claims ignorance of Twitter in libel suit,* NY DAILY NEWS (Jan. 23, 2014), http://www.nydailynews.com/entertainment/gossip/courtney-love-claims-reckless-oath-article-1.1588397.

[861] *Gordon & Holmes et al. v. Love,* Motion for Summary Judgment BC462438, Sup. Ct Cal. (Dec. 29, 2013), (addressing Love's tweeted comments that her lawyer had stopped taking her calls because 'they got to her…she's disappeared'.)

[862] *Id.* See also *Courtney libel suit shows landmark 1964 case relevant in digital age*, CBC NEWS (Mar. 8, 2014), http://www.cbc.ca/news/technology/courtney-love-libel-suit-shows-landmark-1964-case-relevant-in-digital-age-1.2565330.

[863] *Id.* at 600. Hunt points out that Twitter is a revolutionary communications platform in that it enables, for the first time in modern communication, the participation of the average citizen with celebrities, major news networks, and politicians.

[864] *Gordon & Holmes et al. v. Love,* 24 Cal. 3d at 260-61 (2014).

of social media publishers were held to no greater or lesser standard than those enjoyed by institutional counterparts.

There was, in other words, an opportunity missed to address the potential for discrete treatment in law for digital messaging. A jury returned a verdict favouring Love on other grounds, due to the inability of the plaintiff to prove Love's knowledge that her statements were false. That is not surprising, given the cryptic messaging within the 140-character limitation that lacks any cues often available in more traditional media as to how Love received her information or her level of credulity when tweeting. The case does recognize, on a more basic level, that First Amendment protections for defendants can extend to tweets.[865]

In the 2011 case of *Obsidian Finance Group v Cox*,[866] the District Court of Oregon required Crystal Cox to prove that her blogging met the standard of a bona fide publisher in order to merit the *Sullivan* malice standard of speech protection.[867] The plaintiff Obsidian was a bankruptcy consultant business engaged in the reorganization of Summit, a company that had misappropriated client funds in the past. The defendant Cox was a blogger with a history of making allegations and seeking payoffs in exchange for retractions.[868] She considered herself an investigative journalist and posted accusations that the plaintiff company was involved in fraud, corruption, money laundering, and other illegal activities in connection with the Summit bankruptcy. She claimed that Oregon's shield law protected her from revealing her sources. The Court found the hyperbolic and figurative language of the postings to be personal opinion, not editorial opinion or journalism. It found the statement that Obsidian had failed to pay $174,000 in taxes sufficiently specific, however, to create a cause of action for defamation.

---

[865] For a detailed analysis of 'twibel' cases and constitutional protections *see,* Patricia Hunt, *Tortious Tweets: A Practical Guide to Applying Traditional Defamation Law to Twibel Claims*, 73 L.A. L. REV., 578, http://twitter.com/about.

[866] *Obsidian Financial Group., LLC v. Cox*, 812 F. Supp. 2d 1220, 1232–34 (D. Or. 2011) (Obsidian 1).

[867] Sullivan, *supra* fn 143 at 280.

[868] David Carr, *When Truth Survives Free Speech*, NYTIMES, B1 (Dec. 11, 2011) (arguing that the fact Cox had offered to take down the offending posts for $2,500 per month was a persuasive factor in denying her claim for shield protection.)

Cox argued for the higher malice standard of intent as a journalist but the Court disagreed. [869] Cox was held not to be a media defendant for the purposes of shield law or libel protection. That decision, based largely on Cox's use of the Internet as a medium and her lack of professional credentials, has potential to threaten legal protections of online citizen reporting and publishing. It also underscores the narrow construction of US state legislation related to journalism shield laws, a major block to wider legal protections for online citizen journalism in what we can agree is a formative time in its development.[870]

Cox appealed her loss, claiming that Obsidian and its partners were public figures, an assertion the Ninth Circuit rejected, holding that her posts involved private figures even while covering a topic of public concern.[871] It found that, "in the context of defamation law, the rights of the institutional media are no greater and no less than those enjoyed by other individuals engaged in the same activities."[872] In light of the Internet-induced decline of the unique hold on information by traditional media, the court found "the line between the media and others who wish to comment on political and social issues becomes far more blurred."[873]

The *Obsidian* appellate decision advances the law of intent by meshing the 1964 *Sullivan* decision (that public figures can only seek claims for defamation if false information is published with actual malice,[874]) and the 1974 *Gertz* decision of the same court (holding that the First Amendment required only a negligence standard for false information about private individuals to constitute defamation).[875] The import of the two decisions is, as one analysis states, that

---

[869] Obsidian I, *supra* fn 865 at 1238.

[870] John J. Dougherty, *Obsidian financial Group, LLC v. Cox and Reformulating Shield Laws to Protect Digital Journalism in an Evolving Media World,* 13 N.C.J.L.& TECH. ON. 287, 290, http://www.ncjolt.org/sites/default/files/6RD_Dougherty_287_322.pdf (proposing a medium neutral model of journalists' shield laws.)

[871] *Obsidian Finance Group v Cox,* Case §12-35238, Court of Appeal, 9th Circuit, from District Ct. of Oregon (Nov. 6, 2013) (Obsidian Ii).

[872] *Id.* at 9, citing *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.,* 472 U.S. 749, 784 (1985).

[873] Citing *Citizens United v. Federal Election Commission* 558 U.S. 310, 352 (2010).

[874] That is, at the time of publication certain information must either be *known* to be false or published with blatant disregard for the truth. There are currently no federal US shield laws for reporters.

[875] Sullivan, *supra* note 143; *Gertz v. Robert Welch, Inc.* decision [418 U.S. 323, 350 (1974)].

> [t]aken together, the two cases establish a meshing precedent: To count as defamation, false information about *public* figures must be published. False information about private figures, meanwhile, must merely be published negligently.[876]

A weighing in on these issues by the US Supreme Court is much needed for clarifying the requisite elements of Internet defamation.

ii Privacy Torts

European discussions on privacy enjoy a long history of framing it within family life and, in some countries, around the concept of individual personality rights.[877] The European statutory model has historically incorporated fundamental rights of privacy, personhood, and personality.[878] Across the Atlantic, any comprehensive consideration of privacy law in America begins with the seminal suggestions of Warren and Brandeis that privacy laws keep pace with "numerous mechanical devices [that] threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'."[879] The technological framework of Brandeis and Warren was yellow journalism and the Kodak camera. As judge in the *Olmstead* wiretapping case, Brandeis later makes mention of not only "what has but what may be," anticipating a future technology whereby Government, "without removing papers from secret drawers, can reproduce them in court," to reveal some of the most intimate occurrences of the home.[880] The advice of Warren and Brandeis regarding crafting a federal US privacy law was not followed immediately and, according to research by Neil Richards and Daniel Solove, the law of privacy in America veered away from the European model, including the law of confidentiality in the UK, to create a new conception of privacy

---

[876] Robinson Meyer, *U.S. Court: Bloggers Are Journalists,* Atlantic (21 Jan. 2014), http://www.theAtlantic.com/technology/archive/2014/01/us-court-bloggers-are-journalists/283225/.

[877] Notably in Germany.

[878] Warren & Brandeis, *supra* fn 112 at 195. *See further* Bratman, *supra* fn 240 at 624 (observing the Warren & Brandeis article was a "seminal force in the development of a 'right to privacy' in American law.")

[879] *Id.,* citing THOMAS COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT, 9 (1879).

[880] *Olmstead v. United States*, 277 U.S. 438, 474 (1927). Brandeis' reference to future surveillance technologies is noted by Jeffrey Rosen, Introduction, in Jeffrey Rosen and Benjamin Wittes (eds) Constitution 3.0: Freedom and Technological Change, 3 (2011).

based on the individual's 'inviolate personality'.[881] The principles promoted in that article of 1890, however, have shaped the development of statutory, constitutional, and other privacy protections from that point on.[882]

Privacy common law in America has developed in a particular direction due to the considerable efforts of William Prosser. His extensive taxonomy of privacy torts was meticulously catalogued. Prosser reviewed hundreds of US cases in the 1960s and relegated them to one of four torts: intrusion upon seclusion (invading a plaintiffs' physical solitude or seclusion), appropriation (commercial exploitation of the property value of one's name), public disclosure of private facts, and false light in the public eye.[883] His texts still form the backbone of US law school torts courses.

While Prosser's organization has been instrumental in producing a uniform reference for the tort law of privacy in the absence of a robust federal privacy law, his work has been criticized as too regimental in its categorization of tort law: it contains such arbitrary inclusions as the 'right of publicity' (that protects a celebrity's intellectual property from misappropriation and hence financial deprivation) within the 'appropriation' category (that protects the private person from the emotional harm of unwanted publicity). To some, such results produce contrivances that do not work well in practice.[884]

Most controversial are the uneven results played out in court. For example, false light claims are recognized in only about two-thirds of US states due to their doctrinal overlap with defamation actions. There are differences, however, that justify Prosser's inclusion of both torts. For example, false light actions avoid hurdles set by limitation and retraction statutes to which defamation actions are subject. In terms of substantive differences, false light claims have no access to defences available to the press in defamation actions.[885] Truth is a complete defence to defamation, while true statements

---

[881] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy,* 98 Cal. L. R. 1887, *passim* (2010) (Legacy).
[882] Bratman *generally, supra* fn 240 at 624.
[883] Prosser, Restatement *supra* note 156;. Prosser, Privacy, *supra* fn 242.
[884] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality,* 96 GEO. L. J., 123, 125 (2007) (arguing that Warren and Brandeis did not invent the law of privacy from meager precedents of the common law but took it in a new direction) (Privacy's Other Path).
[885] Patricia Avidan, *Protecting the Media's First Amendment Rights in Florida: Making False Light Plaintiffs Play by Defamation Rules,* 35 STET. L. REV. 227 (2005).

are actionable under false light law. Journalists must therefore be particularly wary of attracting false light claims because defendants can be successful even if the story is truthful in its entirety.[886] As well, false light requires the dissemination of offending content to a wide audience, whereas defamation claims can rest on the perceptions of a smaller number of recipients. The principal doctrinal difference rests in the interest the law seeks to protect: defamation protects the objective interest of reputation while false light protects the subjective interest of emotional injury causing personal embarrassment, helplessness or mere hurt feelings.[887] The conceptual vagueness of those terms, as well as of the reasonable person standard of proof, has prompted journalists to complain of the tort's chilling effect on their First Amendment protection.[888]

Daniel Solove's work builds on Prosser's taxonomy, emphasizing the variety of possible legal protection models beyond tort law that need addressing.[889] He observes that many jurists too readily rely on Prosser and avoid tackling the conceptual "muddle" that the law of privacy has become more recently.[890] Beyond Prosser's tort law, American privacy law extends to the jurisprudential right to privacy," Fourth Amendment law, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state privacy statutes.[891] With the "panoply of different privacy problems" arising with new technologies that do not fit readily into Prosser's categories, Solove calls for a new legal framework that more accurately recognizes *potential* risks of privacy harm: information collection, information processing, information dissemination, and

---

[886] *For e.g.* the case of *Anderson Columbia Co., Inc. v. Gannett Co., Inc.*, No. 2001 CA 001728, Fla. Cir. Ct. 1st Dist. (filed Aug. 28, 2001) (where the owner of a road-paving company was awarded $18.28 million for a true report that he had shot his wife but that failed to state that the authorities ruled the shooting accidental until two sentences after the original mention of the shooting, thereby putting his name in a false light. The decision was overturned on appeal (Florida Supreme Court No.sc06-2174 (October 23, 2008)).

[887] *Getting it right, but in a "false light",* Reporters Comm. Fr. Press, http://www.rcfp.org/browse-media-law-resources/digital-journalists-legal-guide/getting-it-right-false-light-0 (pointing out that some states hold that false light claims can concern untrue *implications*, not directly false statements.)

[888] Thereby offending the constitutional standard that "Congress shall make no law… abridging *the freedom of speech, or of the press*; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." [emphasis added].

[889] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 605 (2006) (Taxomony).

[890] Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy,* 44 S. DIEGO L. REV., 745, 754 (2007).

[891] Solove, Taxonomy *supra* fn 888 at 483.

invasion.[892] That organizational framework accommodates nicely the concept of reputational privacy (with its inclusion of data privacy) addressed throughout this paper.

Solove notes particular conceptual problems posed for personal privacy by the Internet, primarily consent[893] and increased accessibility.[894] Recognizing that there is no pan-American law of information privacy, unlike the uniformity achieved by the pan-European 95 Directive,[895] Solove argues for more nuanced categorization of harm, from methods of intrusion from gazes (surveillance) to official questioning (interrogation) to the imposition of one's presence into another's physical space as revealed in celebrity cases.

Regarding the latter, some US celebrities have taken the prying of the yellow press into their own hands: they have joined forces to argue for laws that prohibit paparazzi from photographing their children.[896] For celebrity targets of unwanted publicity, virtual intrusions magnify the ambit, speed, and constancy of exposure. YouTube videos and mobile phone photo capabilities provide a particular kind of

---

[892] *Id.* at 488ff.

[893] *Id.,* at fn 28 citing Julia Cohen (people are bad at predicting "the risk of future harms that might flow from piecemeal, otherwise consensual collection of their private data") and Paul Schwartz (who calls consent a legal fiction in the context of the Internet).

[894] *Id.* at 536.

[895] In the EU, two main legal instruments regulate the data protection in the information society. These legal instruments include the 95 Directive, *supra* fn 667, and the e-Privacy Directive 2002/58/EC *supra* fn 680.

[896] Laura Olson, *Paparazzi who harass stars' kids face tougher penalties*, CHICAGO SUN-TIMES (25 Sept. 2013), http://www.suntimes.com/news/nation/22779614-418/paparazzi-who-harass-stars-kids-face-tougher-penalties.html; Susan Rohwer, *Kristin Bell and Dax Shepard's scheme to sideline aggressive paparazzi,* L.A.TIMES (5 Mar. 2014), http://www.latimes.com/opinion/opinion-la/la-ol-kristen-bell-dax-shepard-aggressive-paparazzi-20140305-story.html - page=1; Anthony York, *Halle Berry, Jennifer Garner to urge crackdown on paparazzi*, L.A.TIMES (13 Aug. 2013), http://www.latimes.com/local/political/la-me-pc-halle-berry-jennifer-garner-paparazzi-crackdown-20130813,0,3748682.story - ax/ (commenting on NoKids Policy campaign created by celebrities to stop publication of images of their children); *California lawmakers pass bill to protect kids from paparazzi*, ABC NEWS (7 Sept. 2013), http://abclocal.go.com/kabc/story?id=9240150 (describing the 'de Leon' bill on privacy that would expand the definition of harassment to include photographing a child without the permission of a legal guardian, increase fines to $10,000, introduce incarceration as a sentence option, and allow civil lawsuits in cases where children are harassed because of their parents' occupation).

intrusive dissemination that tort and privacy laws fail to address.[897] By undertaking their own anti-paparazzi campaign, American celebrities are exhibiting the independence and autonomy of the self-regulatory model that US privacy policymakers prefer.

For EU Member States, two main legal instruments direct privacy legislation in the digital information society: the 95 Directive regarding data privacy of individuals[898] and the e-Privacy Directive regarding privacy rights of individuals and other legal persons for electronic communications, including oversight of the free movement of data, communications equipment, and services.[899] Both directives are persuasive, not mandatory, but portions of the 95 Directive will instantly become domestic law upon passage of the EUDR. Domestic criminal laws and the EU Convention on Cybercrime continue to address such violations as identity theft, the transmission of pornography, and cyberbullying.

The unsolicited commercial use of email addresses for marketing purposes is prohibited by the e-Privacy Directive[900] within the EU, unless consenting individuals choose to *opt-in* to such activities. That model contrasts with the traditional tenet of US Internet company terms of service where participation of consumers is accompanied with provisions for *opt out* choices. Those differences reflect US political support for the behavioral advertising regime that, as a consequence, makes the sale and transfer of personal data a flourishing industry in America. The emergence of *post facto* data breach notification laws in several US states marks a slight shift from the older US policy mindset of placing all data protection in the hands of the consumer.[901] The fact that breach notification was contained as early as 2002 in its e-Privacy Directive within the

---

[897] *See, for e.g.* Jaqueline Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video"*, 96 IOWA L. REV. 919 (2010).
[898] 95 Directive *supra* note 667, section 2.1.
[899] E-Privacy Directive, *supra* fn 680. pp. 37-47, section 2.2.
[900] Article 13. A natural or legal person who initially collects address data in connection with the sale of a product or service has the right to use it for commercial purposes provided the customers have a prior opportunity to reject such communication. Member States have the obligation to ensure that unsolicited communication will be prohibited, except in circumstances given in Article 13.
[901] Lei Shen & Rebecca Eisner, *New and Proposed US Data Breach Notification laws,* MONDAQ (9 July 2014), http://www.mondaq.com/unitedstates/x/326416/Data+Protection+Privacy/New+and+Proposed+US+Data+Breach+Notification+Laws.

EU indicates there is some cross-Atlantic influence of Europe's more paternalistic approach.[902]

A significant conceptual challenge posed by our participation in new media is whether we can claim any expectation of privacy when the very appeal of digital communications resides in the features that reduce our privacy. For example, we know that the personal cost of free entry and the convenience of the Web is the privacy invasion involved in commercial tracking of our online activities and consumer preferences.[903] While socialization has taken on a whole new visual appeal through the portability and immediate distribution of selfies and group photos, we have come to expect that our party antics are frequently tagged, posted, and widely disseminated through Facebook or Instagram, often without our knowledge. Potential employers, clients, and business prospects have access to legal, and illegal, spyware to learn more about such indiscretions.[904] On a broader scale, with each web search auto-correction suggestions are algorithmically determined from the most frequently entered search terms, a compendium to which we contribute with each entry online. We are coming to know, click by click, the privacy costs of our engagement.

iii Breach of Confidentiality

This subcategory of tort law has historical roots in Anglo-America to protect information conveyed within a confidential relationship.[905] It has maintained its usefulness within the UK to recognize expectations of trust within certain transactions, but has less currency in US legal practices due, primarily, to the other path taken by legislators responding to Warren and Brandeis, that of individual rights to privacy.[906]

---

[902] *See further,* European Union Agency for Network and Information Security (ENISA), Recommendations for the Technical Implementation of the Art of the E-Privacy Directive (2011), https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn.
[903] For further discussion of this legal dilemma, *see* Adam J. Tutaj, *Intrusion upon Seclusion: Bringing an "Otherwise" Valid Cause of action into the 21st Century,* 82 MARQ. L. REV. 655 (1999).
[904] Daniel Dimov, *Mobile Phone Spying Software: Legality, Symptoms, and Removal,* Infosec Inst. (8 Mar. 2013), http://resources.infosecinstitute.com/mobile-phone-spying-software-legality-symptoms-and-removal/. (giving examples such as SpyBubble, Mobile-Spy, and Stealthgenie whereby the owner can keep track of information exchanged over the tracked phone, including text messages and phone calls.)
[905] Geoffrey C. Hazard Jr., *An Historical Perspective on the Attorney-Client Privilege,* 66 CAL. REV. 1061, 1078 (1978).
[906] Richards & Solove, Privacy's Other Path, *supra* fn 883 at 123ff.

Communications within the confidential relationship are protected in a court of law through evidentiary privilege.[907] At earlier periods of history, communications through letters and literary expression were also respected as confidential, as were post office or telegraph office services.

Having existed in the shadow of tort law, the US breach of confidentiality action remains obscure and rarely invoked. In England, however, actions have been expanded to include cases where no prior relationship of confidence or trust existed but where an equivalent breach of privacy would be found in America.[908] An example is provided by the UK case of *Loreena McKennitt v. Ash*.[909] Canadian singer McKennitt sued in a breach of confidentiality action for a handful of references in a book by Ash, her former friend and confidante with whom no prior, legally-recognizable relationship of confidence existed.[910] Justice Buxton of the UK Court of Appeal found McKennitt's personal trust had been breached with the revelation of personal details. The cause of action has been similarly expanded over the past decade to include disclosure of personal information in such fields of practice as insurance, accountancy, social work, and education.[911]

Doctrinally the two causes of action are quite distinct. First, breach of confidentiality deals more with the *context* within which information is revealed, that of a relationship of trust and an understanding that certain information is of such a private nature as to be kept between those who originally shared it. With breach of privacy, the *content* is more the focus: the information must be sufficiently personal that its revelation causes humiliation and shame to the subject of the information. As one judgment

[907] For greater clarity, confidentiality is a broader ethical concept while privilege is an evidentiary matter. Examples include lawyer-client, priest-penitent, and doctor-patient relationships; they vary in .

[908] *See* section 4.2(b)(i) *supra* for a separate analysis of changes to the UK Defamation Act in 2013. *See also* Elizabeth Samson, *The Burden to Prove Libel: A Comparative Analysis of Traditional English and U.S. Defamation Laws and the Dawn of England's Modern Day*, 20 CARDOZO J. INT. & COMP. L. (JICL) (2012), http://ssrn.com/abstract=2170040.

[909] *McKennitt v Ash*, [2006] EWCA Civ. 1714. In *Mosley v United Kingdom infra*, Justice Eady extended the concept to find a confidential relationship between Mosley and the press despite the absence of any significant prior interrelation.

[910] The decision was one of the first libel cases that invoked the new *Human Rights Act* (1998) in the UK. Richards & Solove, Legacy, *supra* fn 880, suggest breach of confidence actions enable the UK to meet its obligations regarding privacy under that UK legislation and under the ECHR as a member state of the EU.

[911] *Id.* at 174.

determined, breach of confidence in the UK is more about the source of leaked information while the US privacy torts address the nature of the information itself.[912]

US and UK doctrine differ as well regarding the impact of the offending or leaked information. It is sufficient to make out a case of breach of confidentiality with few recipients of the news. With privacy invasion, however, an element of publicity must cause the plaintiff embarrassment and humiliation. The impact on reputation is much more profound. In addition, the information itself must be "highly offensive to a reasonable person"[913] whereas the confidence that is shared in a UK action need only be one that is preferred to be kept between the speaker and the confidante.

iv Data Disclosure

The genesis of modern legislation in this area can be traced to the first data protection law in the western world, enacted in the area of Hesse, Germany in 1970.[914] Such legislative development was reportedly prompted by an increased interest in rights to privacy with the advent of information technology in the 1960s and 1970s.[915] Similar data protection provisions followed in Sweden (1973),[916] the United States (1974)[917], Germany (1977)[918] and France (1978).[919] The Hesse data privacy legislation

[912] *McCormick v England*, 494 S.E. 2nd 431. (S. Ct. App. 1997) (which states "[A]n invasion of privacy claim narrowly proscribes the conduct to that which is 'highly offensive' and 'likely to cause serious mental injury.'"

[913] McCormick *id.*

[914] Hessisches Datenschutzgesetz (The Hesse Data Protection Act), Gesetz und Verordungsblatt I (1970), 625.

[915] *Data Protection and Privacy Laws*, Privacy International, https://www.privacyinternational.org/issues/data-protection-and-privacy-laws.

[916] The Swedish 1973 Data Act. *See* Soren Oman, *Implementing Data Protection in Law*, Stockholm Institute For Scandinavian Law, http://www.scandinavianlaw.se/pdf/47-18.pdf (advising that the Act only covered processing of personal data in traditional, computerized registers. The Act did not contain many material provisions on when and how the data should be processed, or general data protection principles.) According to David Wright, et al., *Are the OECD guidelines at 30 showing their age?* 54 Comm. Acm, 119 (February 2011), *Sweden's Data Act* of 1973 was the first comprehensive national act on privacy in the world.

[917] *Privacy Act of 1974*, *supra* fn 682.

[918] *German Federal Data Protection Act* of 1977 (BDSG), Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bun- desdatenschutzgesetz - BDSG) of 27 January 1977, BUNDESGESETZBLATT [BGBI] 1 201 (W. Ger.) [Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act - BDSG)].

was prompted by the power struggle that was developing between legislative and executive authorities.[920] The legislature sought to monitor the control the executive branches of local government would have over knowledge collection and retention.[921] As well, citizens began to worry about what would happen to their data and, more broadly, to their jobs as data collection became more widespread.[922]

The Hesse prototype contained basic themes that would influence most privacy and data protection legislation in Europe up to the present day: 1) the negative default rule (viewing the processing of personal data as interference *per se* that needed legitimization); 2) the idea that data subjects had a right of access to information relating to them without the need to show cause; 3) the omnibus approach (the *Hesse Act* could not cover the private sector and so it set out to regulate all of the state public sector within its competence); and 4) the establishing of a privacy protection institution (with the primarily European idea that you cannot regulate behavior through litigation but through highly structured organizations).[923]Today within the EU, the e-Privacy directive has been instrumental in introducing breach notification measures that can be taken within EU Member States once the damage of disclosure has occurred.[924]

---

[919] *Loi Informatique Et Libertes Act* N°78-17 (6 January 1978) On Information Technology, Data Files And Civil Liberties, as amended.

[920] Herbert Burkert, *Privacy – Data Protection: A German/European Perspective,* Max Planck Institute For Research, (nd), https://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf.

[921] *Id.,* at notes 4 & 5, p 45, (advising that "In the constitutional system of Germany after the war a new emphasis had been put on the executive and rule-making power of the local communities which carried the main burden of executing state and federal laws, as well as their local bye-laws. This role became expressly recognized in the German Basic Law [constitution]." The federal government had "only a relatively small administrative infrastructure of its own". The *Grundgesetz* or Basic Law functioned as a constitution for West Germany until the entire German people approved a constitution *(i.e.,* after reunification). It guaranteed the "dignity of the individual," and the right to the "free development" of one's personality.

[922] *Id.*

[923] *Id.,* at 46 (pointing out that *the Hesse Act* and many, but not all, subsequent laws in Germany tried to avoid "state association" by making the agency or commission directly responsible to Parliament).

[924] For practical ramifications and advice *see further,* Data Breach Notifications In The Eu, Full Report, European Network And Information Security Agency (ENISA) (2013), http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at.../.

Such principles differed widely from those that led to a much less centralized data protection regime in the US where the right to be left alone involved a freedom from state intrusion into one's private spaces. One German principle has influenced privacy policymaking in both Europe and US, however: the right to free development of the personality as the "highest constitutional value," existing within the "untouchable sphere of private life withdrawn from the influence of state power."[925] That goes back to that expressed by Justice Brandeis: the right to be let alone as against the government."[926]

Both EU and US jurisdictions have enacted legislation for the protection of personal data,[927] the central doctrinal concept that defines the scope and boundaries of many privacy statutes and regulations around the world.[928] As indicated above, in the 1990s the Clinton administration determined that the private sector should take the lead in global electronic development through self-regulation. As a result no single data protection law emerged in the US.[929] Consequently, electronic and digital innovation has produced such various pieces of federal legislation as the *Credit Reporting Act* of 1970, the *Privacy Act* of 1974, the *Video Privacy Protection Act* of 1988, and the *Cable Television Protection and Competition Act* of 1992.[930] In addition, individual states frequently pass their own versions of such legislation when local jurisprudence determines that portions of the federal acts are unconstitutional. An example can be found in the creation of the federal *Children's Internet Protection Act* of 2000 upon the

[925] Article 2(1) of the *Grundgesetz* provides: "Every person has the right to free development of his own personality, in so far as he does no damage to the rights of others, to the constitutional order, or the moral law." *Id.* The right to free development of the personality means, in the broadest sense, the right to act freely. (Judgment of 16 Jan. 1957 6 Bundesverfassungsgericht [BVerfG] 32, 36).

[926] *Olmstead v. United States*, supra fn 879, (dealing with the constitutional challenges to the US Fourth Amendment posed by wiretaps). This opinion is expressed in J. Lee Ricardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?* 6 Boston Col. Intl. & Comp. L. Rev., 243, 245.

[927] 'Personal data' is often referred to as 'personally identifiable information' and so are used interchangeably in this dissertation.

[928] Schwartz & Solove, Reconciling *supra* fn 676.

[929] William J. Clinton & Al Gore, A Framework For Global Electronic Commerce, (1 July 1997) http://www.technology.gov/digeconomy/framwrk.htm.

[930] For a comprehensive list of federal and state data privacy legislation *see United States Privacy Laws,* Information Shield, http://www.informationshield.com/usprivacylaws.html.

striking down by the US Supreme Court of certain provisions of the *Communications Decency Act* of 1995 dealing with Internet pornography.[931]

Cases of inadvertent data leakage by a public repository (such as a bank) or more deliberate or negligent disclosures at the hands of commercial entities (such as Internet companies and retail outlets) are an increasingly familiar occurrence worldwide. (click on Pictogram 2 in Appendix B). The case of Google's *Street View* mapping service demonstrates the litigious response such privacy invasions can ignite in concerned citizens on both sides of the Atlantic. From 2006 to 2010, Google Street View camera cars navigated city streets in more than thirty countries collecting over 600 gigabytes of personal data from citizens using unencrypted or public Wi-Fi services. No notifications went out to those residents or to the Wi-Fi stations involved.[932] The collection of video, audio, and other information bits only came to the attention of Google executives through queries by German regulators. The equipment used to photograph neighbourhoods around the world also picked up personal details of the Wi-Fi networks and coding from Wi-Fi routers, including usernames and passwords.[933] Google claimed its camera cars only picked up fragments of data due to their rapid movement through city streets. Several lawsuits ensued, including a class action heard in San Francisco that was decided for the plaintiffs and affirmed on appeal.[934]The case established that Wi-Fi operations do not come within the definition of "radio communication" under the federal *Wiretap Act*, an interpretation argued by Google Inc. to render all Wi-Fi data publicly accessible and hence to relieve them of charges of illicit interception of private data or communications.[935]

The 2013 *Google Spain* decision of the CJEU marked an expansion of individual rights over personal data collected by Internet companies for the retention and dissemination of inaccurate or irrelevant personal data. The decision's findings, while

---

[931] *Reno v. ACLU*, 521 U.S. 844 (1997) USSC.
[932] Michael Liedtke, *Google grabs personal info off of Wi-Fi networks,* Yahoo Finance, (May 28, 2010), http://web.archive.org/web/20100518095457/finance.yahoo.com/news/Google-grabs-personal-info-apf-2162289993.html?x=0.
[933] *Id.*
[934] *Google Inc v. Joffe et al*, 9th U.S. Circuit Court of Appeals, No. 11-17483 (10 Sept. 2013), on appeal from *Re Google Inc. Street View Electronic Communication Litigation,* U.S. Dist. Ct. for the N. Dist. CA, Case No. 5:10-MD-2184-JW 794 F.Supp.2d 1067, June 29, 2011.
[935] Statement of Defense, Google Inc. *See also* Jonathan Stempel, *Google loses appeal in privacy case,* Reuters (10 Sept. 2013), http://www.reuters.com/article/2013/09/10/us-google-view-lawsuit-idUSBRE98913D20130910.

focused on the 95 Directive, set the stage for acceptance of the provisions of its successor, the EUDR. The facts of the case are straightforward: A newspaper published a notice of auction in respect of the property of Mario Costeja González for unpaid debts in Spain. He subsequently paid the debts and the property was not auctioned. Ten years later Google searches on his name still brought up the newspaper advertisement. The Spanish courts did not agree that the newspaper archive should be amended and so González brought an action to require Google to suppress those results. Google appealed the lower court finding for the plaintiff to the National High Court that, in turn, sought a preliminary ruling from the CJEU on ISP liability (among other issues) as set out in the 95 Directive.

Google's principal argument was that search engines do not distinguish between data it carries that are protected by the 95 Directive (personal data) and other data, and that it has no control over the data or the selection of the data. It therefore argued that its role was not to "determine [...] the purposes and means of the processing of personal data" as required by the terms of the 95 Directive, and hence it was not a controller for purposes of the Directive. The CJEU rejected those arguments. Firstly it was not contested that the data included personal data that was processed: the fact that there was non-personal data in the search engine operations was deemed irrelevant. It was decided that:

> a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results'.[936]

The CJEU emphasized that a broad definition must be given to 'controller' to ensure complete protection for data subjects. In assessing this, the CJEU looked not only to what Google does in terms of the organization of the search engine but also its role in linking individuals to results.[937]

The decision establishes a system for data processing in the EU that gives the data subject certain rights to correct data and to object to its ongoing retention. The

[936] Google Spain, *supra* fn 401 at paras. 28-29.
[937] *See further,* Lorna Woods, *Google v Spain, landmark CJEU decision in relation to freedom of expression and the right to be forgotten,* Inforrm's Blog (13 May 2014) http://inforrm.wordpress.com/2014/05/13/news-google-v-spain-landmark-CJEU-decision-in-relation-to-freedom-of-expression-and-the-right-to-be-forgotten-lorna-woods/.

data subject thereby moves a step closer to garnering control over its online data presence. The case also raises important questions about the scope of the 95 Directive in its impact on non-EU resident processors who might be a 'controller'. It has repercussions for non-EU-based companies using data of EU citizens and exporting them across national borders. It also has implications beyond a first publisher of material to search engines and other entities that republish personal content and that might have more audience than first publishers of a webpage. Under all those scenarios, a search engine operator might be required to remove information at the request of the data subject.

With respect to the particular data rights of M. Gonzales that concern the right to be forgotten,[938] the CJEU held that:

> having regard to the sensitivity for the data subject's private life of the information … and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should *no longer be linked* to his name by means of such a list. [939] [emphasis added]

It is critical to remember in the ensuing discussions on the right to be forgotten that follow in Chapter IV that the Google Spain decision recognizes a right to request erasure of architecturally embedded *links* to one's non-consensual information, not a right to have the original information itself removed. Such a finding is always subject to the public interest in having access to the information.

c ISP Liability

There appears to be different judicial treatment emerging on each side of the Atlantic regarding the activities for which ISPs should be held legally accountable. US judges are less likely than their European counterparts to find Internet companies or Internet service providers (ISPs) liable for the hosting and distribution of defamatory content due to First Amendment protections and the sweeping immunity afforded by the *Communications Decency Act*.[940] Section 230 of that law states:

[938] As set out in Articles 12(b) and 14(a) of the Directive.
[939] Google Spain, *supra* fn 401 at para. 98.
[940] The *Communications Decency Act* of 1996, (47 U.S.C.) is a common name for Title V of the *Telecommunications Act* of the same year.

> No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider."[941]

Such wording suggests liability is restricted to active publishers or intermediaries, as the Matthew Drudge case illustrates.

The Internet gossip columnist Drudge,[942] most noted for breaking the President Clinton-Monica Lewinski story, was contracted to America On-Line (AOL) for a series of columns he posted on an AOL enabled website that were distributed by email to subscribers. The Drudge Report promoted itself as a particular species of new media: a US-based "news aggregator".[943] The AOL, as ISP for those columns, had the right to remove content under its standard terms of service, and arguably could be considered an editor or controller of content for its active involvement in the selection of posted material. Drudge physically posted the gossipy content, which provided links to other articles and sources of news. In one such column Drudge reported domestic abuse by Sidney Blumenthal, a prominent member of President Clinton's administration.[944] Blumenthal sued both Drudge and AOL for defamation. By invoking section 230 of the *Communications Decency Act* and disavowing any activities as publisher, AOL was successfully removed as a defendant, despite its input to content and the editorial oversight it provided.

In its deliberations over whether it held the judicial authority to impose a judgment in Blumenthal's suit for $30 million, however, the District Court of Columbia questioned the *carte blanche* extended to ISPs under the *Communications Decency Act*. It specifically addressed ISPs' freedom to "flaunt a rumormonger's ability to make rumors instantly accessible to its subscribers and then claim immunity" for any defamation claims that follow. The court upheld ISP immunity all the same,[945] and revealed in its judgment a misunderstanding of the technology of the Internet. The court suggested

---

[941] Section 230(c)(1).

[942] The Drudge Report provided links to upcoming political and entertainment stories and "predicted" the Monica Lewinsky scandal in 1996.

[943] Kaley Leetaru, *New media vs. Old media: A portrait of the Drudge Report* 2002-2008, 14 FIRST MONDAY (6 July 2009), http://journals.uic.edu/ojs/index.php/fm/article/view/2500/2235 (arguing that the *Drudge Report* relied heavily on wire services and obscure news outlets to find small stories that would break large in future days, making it highly dependent on mainstream "old media" sites.)

[944] *Blumenthal v Drudge and America On-Line Inc.*, 992 F. Supp. 44 (1998) (D.D.C.).

[945] *Id.*, at 51.

Drudge maintained a mailing list of email subscribers. Online authors like Drudge do not maintain email subscription lists that they service; they have no idea where, or from whom, their postings are transmitted from day to day. That service is provided autonomously in response to anonymous prompts from subscribers.

The ISP immunity provisions of the *Communications Decency Act* have been applied consistently by US jurists to defeat defamation or privacy claims provided three criteria are present: 1) the defendant must be an "interactive computer service";[946] 2) the plaintiff must allege the defendant I s a publisher or author of the material; and 3) the communication must have been provided by a third party "information content provider".[947] There has been a certain judicial willingness in recent decisions to use a more nuanced interpretation of the section 230 provisions.

EU case law has generally taken a stricter view of liability for ISPs than that of the US. Under EU law, a "service provider" is any person or entity providing an "information society service" which means any services provided for remuneration at a distance by electronic means.[948] The *eCommerce Directive*[949] affords an ISP immunity from liability only when it serves as a "mere conduit"[950] or provides "temporary caching"[951] for the sole purpose of making the transmission of content more efficient. The Directive is used in cases of copyright infringement, defamation, and invasion of privacy. Immunity is also provided if the ISP service is of a mere technical, automatic and

[946] In § 230(c)(1) the Act states: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." In § 230(f)(2) "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server. . . ."

[947] In " § 230(f)(3) "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."

[948] Article 1.2 of EU Directive 98/34/EC.

[949] Directive 2000/31/EC (8 June 2000) On Certain Legal Aspects Of Information Society Services, In Particular Electronic Commerce, In The Internal Market (eCommerce Directive). That approach is termed "horizontal" because it addresses liability regardless of the grounds of claim by a rights holder or injured party.

[950] Article 12.

[951] Article 13.

passive nature, and where the ISP has neither knowledge nor control over the content being transmitted or stored.[952]

Personal data retained by *telecom* service providers are regulated under a separate Telecom Directive.[953] Such laws requiring the retention for government purposes of location and traffic data of individual users were found to violate the ECHR according to the CJEU *Digital Rights Ireland* case in 2014.[954] Such service providers are thereby granted valid grounds to refuse to comply with national data retention obligations, although the decision is unclear as to which remedies are available to individual users whose personal data is disclosed. It is difficult to imagine such restriction on government surveillance practices in America.

Takedown requests by ISPs are of particular interest to courts in Europe. An oft-cited example involves the conviction for invasion of privacy and defamation of three Google executives at the hands of Italian courts in 2010. Residents of a small Italian town complained that a video of schoolmates taunting an autistic student lingered online for a couple of weeks before Google administration removed it.[955] The Milan court found that period of time sufficient for extensive access by countless online viewers. Google argued a guilty verdict might require it to filter content on YouTube before it was posted, which it claimed would be incompatible with the open spirit of the Internet, as well as the tenor of several European directives and guidelines. The executives were given a suspended sentence and fine.[956] The case is currently making its way through appellate levels of court, with the Google executives arguing the "mere conduit" defence.

The cases against Google's Street View mapping services in Europe, as

[952] Article 42. As affirmed in the CJEU decision of *Scarlet Extended SA v. SABAM (Societe belge des auteurs, compositeurs et editeurs,* C-70/10 (24 Nov. 2011).
[953] EU Data Retention Directive 2006/24/EC (eTelecom Directive). The Directive covers fixed telephony, mobile telephony, Internet access, Internet email and Internet telephony. All EU Member States have incorporated the Directive's provisions into their domestic laws except Belgium and Germany.
[954] Digital Rights Ireland, *supra* fn 681 .
[955] Loek Essers, *Google Video trial to continue to Italian supreme court*, PCWORLD (17 Apr. 2013), http://www.pcworld.com/article/2035387/google-video-trial-to-continue-to-italian-supreme-court.html. Three Google executives were handed 6-month suspended sentences in Milan in 2010, a decision that was reversed on appeal. The prosecutor has appealed that reversal in the highest Italian court, the Court of Cassation, arguing the executives deserve criminal sanctions for having knowledge of the continued posting.
[956] Privacy actions are addressed through the criminal law in Italy.

mentioned above, show how far some courts are willing to go to find ISP liability. Several EU countries have taken exception to the privacy invasion of Google's Street View cars and several German towns and cities have moved to block Google from taking pictures of storefronts and homes. In Switzerland, data protection authorities sued Google to press it to increase privacy protections.[957] The Swiss Data Protection laws extend privacy rights to images of a person's home and street view without express permission of the owner.[958] This is also the case for vehicle number plates and pictures of residences, gardens and other private spaces, all considered personal data because in such cases a personal connection can be established without difficulty. Public institutions housing individuals in need of privacy protection, such as hospitals and schools, are also protected. The rationale is that it takes little effort to identify specific persons and it must be assumed that third parties will take an interest in the data.[959]

The German decisions further rejected the claim of Google that the fact vehicles are clearly equipped with a rooftop camera meets its duty to provide information on what it is doing. People are simply not aware that the object of the exercise is to travel the roads, systematically photographing them to publish the images on the Internet without their consent. In Switzerland, advance notice in both the local and regional media and in particular in the print media must be given of Google Street View recording trips and of the activation of new images on the Internet. Clear notice must also be given of the right to object.[960]

There is increasing concern in the US over the lack of precision in defining the functions of ISPs for the purpose of determining legal liability. Such intermediaries as AOL, Prodigy, and Yahoo! have reportedly struggled with the issue of how much

---

[957] *FDPIC v. Google Inc.,* BGE 138 II 346 (31 May 2012). Note: Switzerland is not an EU member state so its relations with the EU Union membership is regulated through a series of bilateral agreements. Although it does not have a concrete legal framework dealing with rights and obligations of ISPs, legal doctrine and practice apply similar principles to those stated in the eCommerce Directive and the provisions of the 95 Directive concerning data protection more generally. *See further* Rolph H. Weber *Internet Service Provider Liability: The Swiss Perspective* (2010), https://www.jipitec.eu/issues/jipitec-1-3-2010/2793/Weber_ISP_Ch.pdf.

[958] *Swiss Federal Act on Data Protection* (FADP; SR 235.1).

[959] *Google Inc. und Google Switzerland,* BGE 138 II 346 E. 6. The only exception is when data is processed exclusively for personal use by a private individual who does not disclose the data to third parties.

[960] See further *Judgment of the Federal Supreme Court on Google Street View: Decisions on the processing of personal data,* Confederation Suisse, http://www.edoeb.admin.ch/datenschutz/00683/00690/00694/01109/index.html?lang=en.

control to exercise over their members and subscribers. By gearing its content to particular sectors, such as the family, Prodigy became known as a content-rich or content-specific site, thereby attracting liability for damages in the case of *Stratton Oakmont, Inc. v. Prodigy Services Co.*[961] Post-Stratton, ISPs have attempted to rely on safe harbour protections to avoid liability for content.[962] They argue they are passive intermediaries, although their provision of services and their insistence on subscriber compliance with terms of service indicates some *de facto* control over content. The posting of warnings by ISPs about compliance with certain laws, on auction sites for example, provide further indicia of control.

The more clear-cut intercontinental differences between European and American legal treatment of ISPs are beginning to shift as we experience the democratizing effects of online speech, become more aware of the existence of cached data, and ponder the implications of the *Google Spain* decision.[963] The issue of takedown requests is becoming the battleground for those shifting issues. Under the *Google Spain* ruling, individual users' takedown requests must be considered by Internet companies using a set list of criteria and, if denied, brought as of right before a "competent authority" for a decision. Within the EU that authority would be a Data Protection Authority once the EUDR is in effect. Within the US, that authority would be a court of competent jurisdiction.[964]

In a comment from France regarding take down requests discussed in the *Mosley* decision by the Court of First Instance in Paris (detailed below), we can see resistance based on privacy rights that involve cached or linked content that get transmitted to third parties and hence is claimed to be outside of Google's control.[965] The author

---

[961] *Stratton Oakmont, Inc. v. Prodigy Services Co.,* No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

[962] For an extended discussion of various methods of ISP control, see further Greenberg, *supra* fn 736 at 1195ff.

[963] Google Spain, *supra* fn 401.

[964] As stated in the Google Spain decision: '…if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results."

[965] *Mosley v. Google France,* Tribunal de Grande Instance de Paris file # 11/07970 (Nov. 2011) http://inforrm.files.wordpress.com/2013/11/mosley-v-google-france.pdf; Florain Martin-Bariteau, *The Mosley/Google Case: Why Privacy Can Not be Argued*, Droitdu.Net (17 Nov. 2013)

comments that Google has responded to each of Mosley's takedown requests, but the offending images are still accessible via video using a different search URL:

> Mosley asked Google to figure a way to automatically and permanently take them down. Google refused, arguing the company wasn't the Internet Police, and has no duty to watch the web content. [966]

Google's resistance to taking down any links to lingering images from Mosley's private party, particularly YouTube video footage that continues to be available through Google searches, has the Hamburg District Court characterizing the Internet company an "accomplice" to the *News of the World* whose story provoked Mosley's initial claim filed in the UK. As one commentator notes,

> The case strikes another blow at Google's continued resistance to the idea that it should play its part in preventing unlawful images from being published by way of image search results.[967]

The fact that Internet companies, as corporations, are not restrained by First or Fourth Amendment provisions, has resulted in executives for companies like Google wielding considerable autonomy regarding what content is posted, retained, or removed from their sites.

Facebook executives wield similar power: although its policy statements promote the democratic concept of its subscribers having a duty to invigilate offensive content, it is the upper management tier that makes final decisions.[968] Its current protocol is to ask its one billion subscribers to flag content that they believe violates Facebook's community standards as posted on its site. Such factors as "nudity, hate

---

http://droitdu.net/2013/11/the-mosley-case-paris-why-privacy-can-not-be-argued-for-notice-and-stay-down/.

[966] *Mosley v Google France,* Inforrm's Blog (Nov. 2013) http://inforrm.files.wordpress.com/2013/11/mosley-v-google-france.pdf (reporting that 'The publication of the images was held to be unlawful by Mr Justice Eady [2008] EWHC 1777 (QB) but video footage continues to be accessible via Google searches'.)

[967] Dominic Crossley, *Case Law: Hamburg District Court: Max Mosley v Google Inc., Google go down (again, this time) in Hamburg* Inforrm's Blog (5 Feb. 2014), https://inforrm.wordpress.com/2014/02/05/case-law-hamburg-district-court-max-mosley-v-google-inc-google-go-down-again-this-time-in-hamburg-dominic-crossley/.

[968] *Statement of Rights and Responsibilities,* Facebook, (15 Nov. 2013) https://www.facebook.com/legal/terms.

speech, bullying and pornography" are particularly targeted.[969] Facebook algorithms then sort the offending content into digital piles and Facebook employees around the world do a more detailed sorting and decide which content stays and which is deleted. Their word is the final arbiter.[970] There is an exception to such standards if content is group-posted on community pages, or involves humour.

Law professor Jeffrey Rosen objects to such "delete squads" or "deciders" wielding the power to determine community norms and to weed out comments that might be controversial and offensive, but still within legal limits.[971] Delete squads will be explored in section 5.3c(1) *infra*.

4.3 Outliers: Criminal Defamation, Insult Laws, Opinion, & Creepiness

a Criminal Defamation

While the focus of this paper is primarily on private law, defamation as a crime is still invoked in many countries in Europe and in some states of America. It is designed as either an alternative to, or in addition to, private law actions in defamation. More specifically still, the penal laws of several civil and common law states makes defamation of public officials, the nation, or government a discrete offense from laws addressing defamation of a private person. In the civil law jurisdiction of France, for example, the choice of law is left to the discretion of the prosecutor who bases such decisions on the degree of public interest that the facts attract.[972] Although framed as an offence related to the selling of prohibited goods rather than as defamation, the *LICRA v Yahoo!* decision of the Paris Tribunal de Grande Instance is an example of a high profile case where the court applied the French penal code to the streaming into France of Yahoo!

---

[969] *Id.*

[970] Stephen Henn, *Facebook's Online Speech Rules Keep Users on a Tight Leash,* NPR (3 Apr. 2013) http://www.npr.org/blogs/alltechconsidered/2013/04/03/176147408/facebooks-online-speech-rules-keep-users-on-a-tight-leash.

[971] Jeffrey Rosen, *The Delete Squad: Google, Twitter, and Facebook and the new global battle over the future of free speech* NEW REPUBLIC (29 Apr. 2013), http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules (Delete Squad). *See also* Jeffrey Rosen, The Deciders: Facebook, Google, and the Future of Privacy and Free Speech, in JEFFREY ROSEN & BENJAMIN WITTE, EDS, CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE, 69-82 (2011).

[972] *See further* Gerlind Berger-Walliser & Franck Valencia, *The Yahoo Case: How to Reconsider State Sovereignty in the Internet Age*, (1 Dec. 2008), http://ssrn.com/abstract=1927461.

auction websites advertising Nazi paraphernalia and links to holocaust denial literature.[973] The case was deemed of considerable public interest in that over 70% of French citizens were identified as Internet users that accessed the unlawful content, as determined by their digital tracks. The court had several criminal sanctions from which to choose: stiff fines, confiscation of offending materials, and the court appointment of technological experts to advise on the permanent removal of offending advertising from such websites.[974] The court chose the first and third options and issued an injunction to facilitate such removal within three months, failing which the defendant Yahoo! Corporation would be subject to a fine of 100,000 francs per day (about 16,500US).

In general, criminal defamation laws differ from those of civil defamation in their higher probative standards, penal sanctions, and more pervasive social stigma. Their chilling effect on dissidents, journalists, and political activists at the hands of state authorities and monarchs has led to repeated calls for repeal of such laws.[975] The power of criminal sanction has proven irresistible to leaders across time, even within democratic states, as an instrument to quell public criticism.

The first citizen to be convicted under the *1881 French Press Law* had called the French President a 'voyou profanateur' or profane thug and a 'goujat iconoclaste' or iconoclastic boor.[976] The last to be convicted was fined thirty euros[977] for holding up a cardboard sign at a 2008 rally telling then-President Nicolas Sarkozy to "Casse-toi pov'con," or get lost.[978] Critics of French Presidents, if convicted under insult laws, have

---

[973] Contrary to Article R645-1 of the French Criminal Code that prohibits the wearing or exhibiting of public uniforms, insignias and emblems which recall those used by any organization declared illegal by the Nuremberg Charter or by a person convicted of crimes against humanity under French law № 64-1326 of 1964-12-26.

[974] LICRA I *supra* fn 727.

[975] United States Helsinki Commission On Security And Cooperation In Europe, Memorandum On Defamation And Insult Laws, http://www.csce.gov (14 Dec. 2001).

[976] Max Fisher, *Yes, it really was a crime in France to insult the president until this week. Here's why*, WASH POST (26 July 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/07/26/yes-it-really-was-a-crime-in-france-to-insult-the-president-until-this-week-heres-why/.

[977] A typical fine for criminal defamation is $18,000 (US) or about 13,500 Euros.

[978] Fisher advises that "the expression literally translates to "break yourself off, poor jerk," but has a more colloquial meaning that is a profane (and unprintable) way of telling someone to go away." See further *European Court backs man against France over anti-Sarkozy insult,* BBC EUROPE (14 Mar. 2013), http://www.bbc.co.uk/news/world-europe-21783922. (offering the translation "Get lost, you sad prick", as reportedly used by Sarkozy himself to a rally member a few months earlier).

been sentenced to a year in jail; between 1881 and 1958, the law against presidential insults was used only nine times, but employed thereafter by President De Gaulle to convict 350 critics of his tactics in the war in Algeria.

It is a legal curiosity that such laws remain in force. A 2014 study of extant criminal defamation laws in Member States of the EU determined that only five of the 28 states have repealed general criminal defamation and insult laws, despite broad international consensus among legal experts and press freedom advocates that criminal punishments for defamation represent a disproportionate restriction on free expression.[979] The study has further determined that the laws of 20 EU Member States suggest imprisonment as a punishment for either defamation or insult, in contradiction of ECtHR rulings that imprisonment is, as a general rule, never an appropriate punishment for defamation. Fifteen states set maximum incarceration at two years, with eight years in one state.[980] Although international standards recommend against providing public officials with any special protection under defamation law, the laws of six EU states elevate criminal punishments for defamation when the offended party is a public official or public figure. In Appendix B, Chart 1, the distribution of criminal defamation laws within the EU is shown, indicating the ample provisions within EU states that have resisted pressure for repeal.

While the basic elements of defamation include a false statement about the person made to a third party that results in the lowering of his reputation in the esteem of his community, criminal defamation law additionally requires proof of intent to cause harm at a much higher probative standard than for civil actions.[981] In more autocratic regimes, the criminal law of defamation has become a weapon to rout out public discourse on controversial policies of the state.[982] Journalists and writers are specific

[979] Scott Griffin *et al., Out Of Balance: Defamation Law In The European Union And Its Effect On Press Freedom,* Report for International Press Institute, (July 2014) http://www.freemedia.at/fileadmin/uploads/pics/Out_of_Balance_OnDefamation_IPIJuly2014.pdf

[980] Slovakia sets a maximum of eight years' incarceration upon conviction for criminal defamation.

[981] Private law defamation traditionally only requires malice for the defamation of public figures and celebrities. Criminal defamation requires proof of intent to defame according to the penal standard of the particular state.

[982] The United Nations Commission on Human Rights determined in 2012 that the criminalization of libel violates freedom of expression and, in particular, Article 19 of the International Covenant on Civil and Political Rights.

targets of such laws and press councils and associations tirelessly promote the repeal of such laws.[983]

At times defamation laws, often in the form of "insult" provisions, are invoked simply to compensate for hurt feelings or indignation, without appreciation for the fact that in an open society, a person's sensibilities must be weighed against the right of others to freely express themselves.

In America, penal consequences can be quite harsh: in Colorado, for example, criminal libel was a felony carrying up to 18 months in prison and a $100,00 fine for a first offence. The libel law was quite broad: it was a crime to "knowingly publish or disseminate, either by written instrument, sign, pictures, or the like, any statement or object tending to blacken the memory of one who is dead, or to impeach the honesty, integrity, virtue, or reputation or expose the natural defects of one who is alive, and thereby to expose him to public hatred, contempt, or ridicule". [984]

Nearly all EU Member States retain criminal sanctions for defamation – with only Croatia, Cyprus, Ireland, Romania and the UK having repealed such laws.[985] The European Commission continues to call for a harmonization of libel laws across the EU,[986] and the Council of Europe called on states to repeal criminal sanctions for libel in 2007, as did both the Organization for Security and Co-operation in Europe (OSCE)[987]

---

[983] Examples include the International Press Institute, ARTICLE 19 within the EU, and the Electronic Frontier Foundation in the US.

[984] Criminal libel laws were repealed in Colorado in September of 2012.

[985] Council Of Europe, *Defamation And Freedom Of Expression: Selected Documents*, Directorate General of Human Rights (March 2003) (detailing the status of criminal defamation and insult laws in most EU Member States). *See also* Mike Harris, *The EU's commitment to free expression: libel and privacy*, X-Index (Jan. 2, 2014), http://www.indexoncensorship.org/2014/01/eus-commitments-free-expression-libel-privacy/ (suggesting a major variance in civil and criminal defamation laws and practices across the EU and referencing a 2008 Oxford University study that found costs of actions ranged from approximately 600 euros (claimant and defendant costs) in Cyprus and Bulgaria to over 1 million euros in Ireland and the UK. Defences varied widely as well: truth was commonplace, but a stand-along public interest defence was in more limited use).

[986] European Commission, *Comparative Study Of Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments*, Final Report JLS/2008/C4/011 – 30-CE-0219363/00-28 (Jan. 20, 2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

[987] *Ending the Chilling Effect: Working to Repeal Criminal Libel and Insult Laws*, OSCE (Nov. 25, 2004), http://www.osce.org/fom/13573 (detailing the censorship experienced by journalists for

and UN special rapporteurs on freedom of expression.[988] Non-governmental organizations that oppose their use include Amnesty International, Article 19, the Committee to Protect Journalists, the Helsinki Committees of Bulgaria, Croatian, Greece, Romania, and Slovakia, the International Helsinki Federation, the World Press Freedom Committee, the Norwegian Forum for Freedom of Expression; national chapters of PEN; and *Reporters Sans Frontières*. For many EU Member States, politicians and journalists receive tougher sanctions for criminal libel than ordinary citizens, even though the ECtHR ruled in 2006 that the limits of acceptable criticism (of the state and other citizens) are wider for a politician than a private citizen."[989]

In the US, criminal defamation remains on the books in seventeen states despite repeated calls for its repeal for the restrictions it places on First Amendment rights.[990] Journalism professor David Pritchard suggests that criminal libel can be a legitimate and hefty legal tool in the hands of state agents for 'expressive deviance' causing harm to private citizens, particularly victims with few resources for private lawyers, lengthy delays, and the unpredictability of private law outcomes.[991]

The reformation of criminal defamation (*desacato*) laws of OAS Member States has been a focus of the IACHR and, despite reports in 1998 and 2000 of its Special Rapporteur for Free Speech recommending their abolition across the OAS membership,[992] there is still wide usage of *desacato* laws to silence opinions against state authorities.[993] The basic constitutional argument of the IACHR is that *desacato* laws

---

criticisms of a ruling regime, but dealing very little with the experiences of non-journalistic critics of the state).

[988] *International Mechanisms for Promoting Freedom of Expression*, Joint Declaration By The UN Special Rapporteur On Freedom Of Opinion And Expression, The OSCE Representative On Freedom Of The Media And The OAS Special Rapporteur On Freedom Of Expression' (2002), http://www.oas.org/en/iachr/expression/showarticle.asp?artID=87&lID=1(stating in its preamble that the authors are "*Mindful* of the ongoing abuse of criminal defamation laws, including by politicians and other public figures".

[989] Lingens *supra* fn 644.

[990] Pritchard, *supra* fn 807, listing the following states: Colorado, Florida, Idaho, Kansas, Louisiana, Michigan, Minnesota, Montana, New Hampshire, New Mexico, North Carolina, North Dakota, Oklahoma, Utah, Virginia, Washington and Wisconsin, along with Puerto Rico and the U.S. Virgin Islands.

[991] Based on 61 trial-level prosecutions in Wisconsin from 1999 to 2007.

[992] *Annual Report Of The IACHR*, 1998 Volume III, Chapter IV A. –OEA/Ser.L/V/II.102 Doc.6 (rev. 16 April 1999); and *Annual Report Of The IACHR*, 2000 Volume III, Chapter III A.2. – OEA/Ser.L/V/II.111 Doc.20 (rev. 16 April 2001).

[993] *IACHR, Report On The Compatibility Of "Desacato" Laws With The American Convention On*

afford a higher level of protection to public officials than to private citizens. This is in direct contravention of the "fundamental principle in a democratic system that holds the government subject to controls in order to preclude abuse of its coercive powers."[994] It also offends the principle of US constitutional law that the state serves with the consent of the governed.

b Insult Laws

Insult laws differ from criminal defamation in that insults might be true but undesirable to public figures and heads of state; criminal defamation, in contrast, relates to false allegations involving either public or private citizens. Particularly disconcerting is the fact that insult laws remain in place in twelve EU Member States even though convictions have been consistently overturned by the ECtHR.[995] Even insult to national symbols, such as the flag, is criminalized in Austria, Germany and Poland.

Most European countries have domestic laws that accommodate actions in insult, a term so broad that it frequently covers expression that would be considered an opinion or value judgment.[996] Even countries regarded as having relatively strong media freedoms have statutes outlawing the insult of elected officials. For instance, the ECtHR has described Belgium's insult law as covering "gratuitously offensive terms or exaggerated expressions."[997]

Insult laws can cast a wide net and punishments can range from token to severe. For instance, until its repeal in 2013, France's *1881 Press Law* prescribed punishments for insult to the president, public officials and foreign dignitaries. At one time punishment included prison terms, but more recently "an insult to the president of France could see you smacked with a €45 000 fine."[998] Insult laws are frequently confused with criminal defamation laws, possibly because the procedural result is the same: hefty fines or incarceration, and the chill of expressive freedoms. For example,

---

Human Rights, OEA/Ser. L/V/II.88, doc. 9 rev., 17 February 1995, 197-212.

[994] *Id.*

[995] Swiss Data Protection and Privacy laws include a subcategory of "pillory" laws.

[996] Marlene Arnold Nicholson, *McLibel: A Case Study in English Defamation Law*, 18 WIS. INT. L. J., 1 at note 21 (2000).

[997] *De Haes and Gijsels v. Belgium*, 25 EUR. H.R. REP. 1, para 26 (1997).

[998] Nickolaus Bauer, *'Insult law' commonplace in many countries,* Mail & Guardian, (15 Nov. 2012).
http://mg.co.za/article/2012-11-15-insult-law-nothing-to-do-with-free-speech.

ARTICLE 19 as an organization of free speech activists complains that a number of countries across the world use defamation laws for the "ill-defined and stifling protection of 'feelings'"[999] where the plaintiffs' requisite standard of proof appears to be "that they feel offended."[1000] In some countries the term 'honour' is used instead of, or in addition to, reputation and humour and satire come within its prohibited actions.

c Opinion

Finally, much online invective that offends individuals has been determined by jurists in defamation cases to be opinion, not fact, and hence not actionable. Such speech can be "uninhibited, casual and ill thought-out" and it is often apparent to casual readers "that people are just saying the first thing that comes into their heads and reacting in the heat of the moment."[1001]

Internet scholar Yochai Benkler has emphasized that new methods of knowledge production on the Internet fundamentally alter the capacity of individuals to be active participants in the public sphere, from disparate corners of the world.[1002] Within that indeterminate community, the Internet confers

> entitlement to opinions and attitudes about me on persons who have never met me, likely do not speak my language, and who have the potential to do incalculable reputational damage through their online commentary.[1003]

While such opinions can cause loss of esteem and financial disaster, they escape legal remedy due to their unverifiable nature. Prosser took care to distinguish the defamatory *facts* that prompted legal defamation actions from the provocation of harmful *opinions* in a community of third parties.[1004]

---

[999] See further *Civil Defamation: Undermining Free Expression,* ARTICLE 19, http://www.article19.org/data/files/pdfs/publications/civil-defamation.pdf . The organization takes its name from article 19 of the ICCPR protecting freedom of expression.
[1000] *Id.*
[1001] *Smith v. Advfn Plc,* All E.R. 335 at paras 14-17 (Q.B.D.).
[1002] YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFERS MARKETS AND FREEDOM 212 (2006).
[1003] *Id. See further* Rodney W. Ott, *Fact and Opinion in Defamation: Recognizing the Formative Power of Context,* 58 FORD. L. REV. (1990) 761 (setting out the fact/opinion debate from the vantage of the First Amendment protections invoked by mass media journalists prior to Internet cases).
[1004] Prosser, *supra* fn 156 (noting "Defamation…tends to injure 'reputation' in the popular sense, to diminish the esteem, respect, good will or confidence in which the plaintiff is held, or to excite adverse, derogatory or unpleasant feelings or opinions against him.")

Online commentary, even if expressed in biting and devastatingly wounding terms, is not often legally actionable because it is not probative - it cannot be proven to be true or false. Courts have allowed that deciphering opinion is not always a clear-cut exercise, although a few have pronounced that statements posted on an Internet bulletin board or chat room are highly likely to be opinions or hyperbolic speech. Each remark must be examined in context. To criticize the Toronto Blue Jays as a defensively weak baseball team is more clearly a personal opinion than to couch that opinion in an assertion of fact, such as alleging that the Blue Jays' management is using deceptive trade practices in their recruitment from the minor leagues. The latter is still arguably an opinion, albeit dressed as fact that is unverifiable by the average individual.[1005]

US Courts' interpretation of what comprises opinion has not always been predictable; much is based on cultural context. For example, the following comments have been judged to constitute opinion: statements on a radio talk show that the plaintiff was a "chicken butt," "local loser" and "big skank", because they were too vague to be capable of being proven true or false and had "no generally accepted meaning";[1006] and email comments by a newspaper employee that a former publisher had displayed "abusive behavior" and "bizarre management style" and had damaged the paper's finances.[1007] Other examples of opinion include calling a political foe a "thief" and "liar"; calling someone a "bitch" or a "son of a bitch"; and changing a product code name from "Carl Sagan" to "Butt Head Astronomer".[1008] Examples found to be defamatory are: charging someone with being a communist in America in 1959; calling a lawyer a "crook"; accusing a minister of unethical conduct; or accusing a father of violating the confidence of his son.[1009] In Ireland, a former garda commissioner was awarded £30,000 in damages for the use of a graphic representation of his ears in a television program on corruption, and a senior barrister settled a High Court action against Irish television for an undisclosed amount for using an image of her car in a story about drunk drivers.[1010]

[1005] See further, *Online Defamation Law*, Electronic Frontier Foundation, https://www.eff.org/issues/bloggers/legal/liability/defamation (EEF Defamation).
[1006] *Seelig v Infinity Broadcasting*, 97 Cal. App. 4th 798 (Cal. Ct. App. 2002).
[1007] *Rose V. Hollinger International, Inc.*, 882 N.E.2d 596 (Ill. 2008).
[1008] EEF Defamation, *supra* fn 1005.
[1009] *Id.*
[1010] *Defamation Law in Ireland* Lawyer.IE, http://www.lawyer.ie/defamation .

Online comments found to be defamatory, even though not verifiable as fact, include those referring to a chief executive officer as "insane" with conduct similar "to that of Hitler, Saddam Hussein and Osama bin Laden."[1011] Linking a person's name to the website www.Satan.com however, was determined by a California court not to constitute defamation because "merely linking a plaintiff's name to the word "satan" conveys nothing more than the author's opinion that there is something devilish or evil about the plaintiff."[1012] Such examples illustrate courts are not always consistent and in many cases arbitrary.

More formalized opinions, such as those contained on professional performance rating sites like ratemyprof.com have become the target of teachers' unions due to their cyber-bullying potential. In 2007, delegates at a UK annual convention of the Professional Association of Teachers cited as defamatory such online activities as posting a doctored photograph of a headless teacher with the caption "You are dead". The organization approached the Internet company with a take-down request.[1013] In France matters have gone even further. When French entrepreneurs created the Note2be.com site, they encouraged students to grade teachers and discuss their teaching abilities. The SNES, a secondary school teachers' union backed by the Ministry of Education, immediately took the website to court, claiming the personal comments represented a breach of privacy and an incitement to public disorder. The judges agreed, ruling the website could no longer identify any teachers by name or risk a 1,000 euro fine for every infraction.[1014]

[1011] *Vaquero Energy Ltd. v. Weir,* 2004 ABQB 68, 352 A.R. 191.
[1012] EEF Defamation, *supra* fn 1004.
[1013] *Teachers in websites closure call,* BBC, (1 Aug. 2007), http://news.bbc.co.uk/2/hi/uk_news/scotland/6925444.stm.
[1014] *Don't complain about your teachers in France,* ARS TECH. (6 Mar. 2008), http://arstechnica.com/civis/viewtopic.php?f=23&t=137941. See also *French website Note2Be.com closed by court order,* 6 EDRI-GRAM (March 12, 2008), http://history.edri.org/book/export/html/1431, (reporting that the Commission nationale de l'informatique et des libertés (CNIL) also gave its verdict backing up the court ruling and considering the site as "illegitimate in relation to the personal data protection". CNIL considered that, on the basis of article 7 of the Information and Freedoms Law, the teachers should be given the option of giving their consent for the publication of information about them).

Such responses to individual commentary exist in a grey area between defamation, cyber-bullying, and opinion that, for the moment, look to the courts for a clear determination of individual privacy rights.

d Creepiness

Certain objectionable online behavior straddles the line between unethical or menacing behavior and overtly illegal acts. It might inflict alarm, discomfort, dread, or even apprehension of harm, but such creepiness lacks the proof of reasonableness that meets the legal test for reputational injury.[1015] It does, however, push the public-private boundaries of social interaction. Imagine, for example, standing at the bar for a professional social event and using your smart phone to access the name, musical tastes, and political convictions of an attractive individual you see standing across the room. You can equip yourself with immensely helpful background information before undergoing the risk of rejection involved in the more direct approach. That kind of social snooping does not incur legal liability; specific applications are even available to encourage the behavior. One such application, *Girls Around Me*, provided a profile of women within the user's geographic vicinity whenever they checked into their social networks on their mobile devices. While a definite social advantage at a nightclub, the passive collection of another's private actions is creepy and clandestine. [1016] Unsurprisingly, the application was withdrawn from the public market within hours of its launch in response to online critical reference to the "stalker app".[1017] A less sinister example, in that consent of subscribers is required, is the application *Highlight* that produces a profile (photos, name, likes and dislikes) on your mobile phone of someone standing near you whose phone also contains the application.[1018] This digital version of

[1015] Karniel, *supra* note 433 at 222 (noting that "frivolous" speech is non-actionable due to its spontaneous, general or unemotional nature).
[1016] Mark Sullivan, *SXSW Preview: The Year of 'Ambient Social' Apps?* PCWORLD (7 Mar. 2012), http://www.techhive.com/article/251455/sxsw_preview_the_year_of_ambient_social_apps_.html .
[1017] Damon Poeter, *Creepy 'Girls Around Me' App Delivers a Wake-Up Call,* PCWORLD (30 Mar. 2012), http://www.pcmag.com/article2/0,2817,2402457,00.asp.
[1018] *Highlight – Meet New People, Find and Connect with Friends Nearby,* ITunes Preview (9 July 2014), https://itunes.apple.com/us/app/highlight/id441534409?ls=1&mt=8.

speed dating is permissible under rules of privacy, but disturbing for the harassment potential it makes technologically possible.

Those devices illustrate that innovative technology does not guarantee ethical correctness.[1019] With social messaging comes ambiguity about the bounds of permissible online behavior. For example, is it acceptable to befriend your children, and their friends, on Facebook and to tag their photographs? What are the social rules for posting, or tagging, a friend's image on Instagram? How about a photograph of her infant children? As dana boyd warns, privacy in an age of social media is complicated. It is about "managing visibility, negotiating networks, and facing an ever-increasing flow of information."[1020]

4.4 Reputation Online: is digital speech different?

Given the democratization of online communications (free, spontaneous, and culturally open) there is some argument for allocating less weight and meaning to digital speech.[1021] Karniel maintains that a rumour does not have elevated status just because it is online: its reliability is still "restrained and incomplete".[1022] The credibility of sources, so critical to acceptance of traditional media accounts, is part of that status but often suppressed or absent in online accounts. Cues about authority and status of either the writer or sources can be hidden and footnotes and direct quotations suppressed. In online speech they seem to take second place to know-how and good ideas, as one psychological study of Internet behavior points out:

> Although one's identity in the outside world ultimately may shape power in cyberspace, what mostly determines the influence on others is one's skill in communicating (including writing skills), persistence, the quality of one's ideas, and technical know-how.[1023]

Commentary on the Internet is perceived as different than in more scrutinized traditional media in that "[h]yperbole and exaggeration are common and 'venting' is at

---

[1019] Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 11 YALE J. L. & TECH. 351 (Fall 2013).
[1020] Dana boyd *The Future of Privacy: Privacy Norms can Inform Regulation,* 32nd International Conference on Data Privacy & Privacy Commissioner. (29 Oct. 2010).
[1021] Karniel, *supra* fn 433 at 216, 219.
[1022] *Id.* at 231.
[1023] Suler, *supra* fn 434.

least as common as careful and considered argumentation."[1024] It is the side-by-side combination of both styles of speech, unmediated by editorial oversight, that creates discomfort about the verifiability of much online 'reporting'.

Online statements can be gossipy, grammatically creative, expletive, insulting, racist, politically incorrect, and contain only loosely connected thoughts. In the absence of editorial second thought for bloggers and tweeters, it becomes practically burdensome to authenticate and hence legally prove the reputational harm caused by such communications. It is because Internet content is "located in another time and zone", more anecdotal and immediate, that it is not subjected to the investigative rigours of traditional journalism.[1025] In the *Obsidian* decision, discussed above,[1026] the lower court found the language of blog posts contained "somewhat run-on" and "stream of consciousness-like sentences", reading more like a journal entry than assertions of fact.[1027] For example, Cox used such hyperbolic terms as "immoral," "thugs," and "evil doers."[1028] On the matter of proof of the truth of blog posts, Cox's assertions that "Padrick hired a 'hit man' to kill her" or "that the entire bankruptcy court system is corrupt" were found "not sufficiently factual to be proved true or false."[1029] The US appellate court of the 9th Circuit found that the very tenor of language used by the defendant Cox in her blog posts "negates the impression that she was asserting objective facts."[1030] The statements were posted on obsidianfinancesucks.com, a URL indicating that any reader would be

> predisposed to view them with a certain amount of scepticism and with an understanding that they will likely present one-sided viewpoints rather than assertions of provable facts.[1031]

Karniel takes the position that most digital speech cannot constitute a cause of action for defamation.[1032] He views the role of blogs, tweets, and other informal journalism as the preliminary flagging of issues that the mainstream offline press can

[1024] Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace* 49 DUKE L.J. 855, 862-63 (2000).
[1025] *Id.* at 218.
[1026] Obsidian I, *supra* fn 865.
[1027] Obsidian II, *supra* note 870 at 17.
[1028] *Id.* at 17.
[1029] *Id.*
[1030] *Id.* at 19.
[1031] *Id.* at 17.
[1032] *Id.* at 234.

then decide is worthy of further investigation, sober thought, and possible publication. Regarding the role of law to address defamatory remarks online, Karniel makes two proposals: either create a sub-category of law for virtual speech, with more lenient levels of proof, or remove online speech altogether from judicial scrutiny.[1033] We shall explore those options in Chapter V.

Yale University constitutional scholar Jack Balkin agrees that, while digital technologies have altered the social conditions of speech, the key transformation has been around the question of control.[1034] Online participation both widens our access to speech and diminishes our control over it. When we speak of freedom of speech, therefore, we must identify whose speech we are contemplating, the commercial speech of industry, the regulatory speech of government, individual speech, and so on. Balkin accepts that social networking speech is collaborative, interactive, and involves gossiping and shaming as much as supporting and praising.[1035] Internet speech intensifies all of those dynamics due to its unique architecture.

Law has a changed role in all of this, as Balkin promotes. Rather than the traditional US model, that is, the "judicial creation and protection of *individual* rights of free expression enforceable against state actors", he suggests we support individual privacy rights with various government programs and entitlements including, perhaps, requirements for technological design.[1036] The digital age makes the court model as important as ever, but aligned with technological and regulatory infrastructure.

4.5 Is the Bench Ready for Digital Speech?

A recent indication from the bench that jurists do not always understand digital science was provided by the *Aereo* case before the US Supreme Court. Technological confusion was indicated when Justice Sonia Sotomayor asked a lawyer to compare the services of his corporate client to "iDrop in the cloud", a non-existent data storage

[1033] Karniel *supra* fn 433 at 213 (rationalizing that most of us do not believe what we read online in any event).
[1034] Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society,* 79 NYU L. REV. 1 (2004).
[1035] *Id.,* (emphasizing that, "[a]lthough freedom of speech is deeply individual, it is at the same time deeply collective because it is deeply cultural") 5.
[1036] *Id.,* 47ff.

system.[1037] She also asked a question about the video streaming service "Netflick".[1038] Another example of technological confusion on the bench is provided by a class action against Google, brought in 2011, regarding its Street View geo-location service. Plaintiffs claimed privacy invasion under the *Electronic Communications Privacy Act*. The information collected, however, was from open Wi-Fi networks, requiring no special equipment. It was unencrypted information people were transmitting in the open, that is, data that was being broadcast. As one technology writer suggested,

> If you understand basic technology, you can understand what they were doing, and how it was almost certainly not to capture data from the network, but just to determine location info…This was data that was being *broadcast*.[1039]

Although not luddites, some judges ask questions in oral argument to more accurately understanding communications technology. In the 2010 case *City of Ontario v. Quon*, involving the issue of constitutional protection of California police communications sent by a paging system, US Supreme Court Chief Justice John G. Roberts asked "What's the difference between email and a pager?"[1040] Justice Anthony Kennedy asked how a text message could be sent to an officer at the same time he was sending one, showing a lack of knowledge of the existing technology. Justice Scalia asked, "Could Quon print these spicy little conversations and send them to his buddies?" [1041] In one court observer's assessment, "The implications are profound…[s]peech, expression, and living have become intertwined in technology. If we're ever to have a case involving Snapchat selfies and eDiscovery, we could be in

---

[1037] *American Broadcasting Companies, Inc. [ABC] et al., Petitioners v. Aereo, Incl, f.k.a. Bamboom Labs, Inc.,* 712 F. 3d 676 (25 June 2014). *See further* Timothy B. Lee, *The Supreme Court's technical cluelessness makes them better justices,* VOX (15 Oct. 2014), http://www.vox.com/2014/4/23/5644154/the-supreme-courts-technical-cluelessness-makes-them-better-justices (suggesting that US Supreme Court Justice Sonia Sotomayor confused the technologies of iCloud and Dropbox).

[1038] Lawrence Hurley, *In U.S., when high-tech meets high court, high jinks ensue,* Reuters (9 May 2014), http://www.reuters.com/article/2014/05/09/us-usa-court-tech-idUSBREA480N420140509.

[1039] *Vicki Van Valin v. Google Inc*. Class action complaint 18 U.S.C. §2511 et seq.; *see also* Mike Masnick, *Judge Who Doesn't Understand Technology Says Wi-Fi is Not Radio Communication,"* Techdirt (1 July 2011), https://www.techdirt.com/blog/wireless/articles/20110701/12225114934/judge-who-doesnt-understand-technology-says-Wi-Fi-is-not-radio-communication.shtml.

[1040] *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

[1041] Kimberly Atkins, *Technical difficulties at the Supreme Court*, DC Dicta (19 Apr. 2010), http://lawyersusaonline.com/dcdicta/2010/04/19/technical-difficulties-at-the-supreme-court-2/.

trouble."[1042] US Justice Scalia has publicly admitted to being "Mr. Clueless" when it comes to technology.[1043]

Similar concerns are expressed within the EU. As one Council of Europe report notes, "Experience suggests that *in most cases*, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world."[1044] One country, Japan, took the initiative of creating an Intellectual Property High Court in 2005 to hear cases of technological complexity. Justice Richard Posner doubts such a move would be well received in the US: "[T]he Supreme Court justices are unlikely to agree to any system which puts a focus on the technology, and likely will seek the safe harbor of focusing their decisions based on prior legal rulings and principles."[1045]

Part of that apprehension might be related to the fishbowl in which judges function today. Many judges display an acute awareness of "negative, even noxious gossip" that can erode *their* reputations and those of other officers of the court as proceedings are increasingly transcribed for online media.[1046] For example, judicial competence in online research that informs a judge's ruling can now be tracked, and results might in future be argued by counsel as leading to the judge's faulty decision making.[1047] The more technologically intrepid among judges are free to use the Internet and social media to monitor the past and current behavior of lawyers and defendants

---

[1042] *See further,* Mark Grabowski, *Are Technical Difficulties At The Supreme Court Causing A 'Disregard Of Duty?'* 3 J. L. TECH. & INTERNET, 1 (2011).

[1043] Jordan Fabian, *Chairman to Justices: "Have Either of Y'all Ever Considered Tweeting or Twitting?"* Hillicon Valley: The Hill's Tech. Blog (May 21, 2010), http://itk.thehill.com/policy/technology/99209-chairman-to-justices-have-either-of-yall-ever-considering-tweeting-or-twitting (quoting Justice Scalia's testimony at a House judiciary subcommittee hearing).

[1044] *Cybercrime training for judges and prosecutor: a concept*, Council Of Europe Project On Cybercrime And The Lisbon Network, (8 Oct. 2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf

[1045] Keith Kirkpatrick, *Technology Confounds the Judges,* 57 Communications Of The ACM, 27 (May 2014), http://cacm.acm.org/magazines/2014/5/174343-technology-confounds-the-courts/fulltext.

[1046] *See further* James G. Carr, *A Judge's Guide to Protecting Your Reputation,* 36, Truth Or Consequences, 26-30 (2014) American Bar Association, http://www.jstor.org/discover/10.2307/29760783?uid=3739448&uid=2129&uid=2&uid=70&uid=3737720&uid=4&sid=21104468347941 (recommending that "vigilant and constant probity and competence remain the best – and perhaps the only- defenses against the corrosive consequences of innuendo", 26.

[1047] *See further* Karen Eltis, *Does Avoiding Judicial Isolation Outweigh the Risks Related to 'Professional Death by Facebook?,* 3 LAWS (2014) 636, 639, www.mdpi.com/journal/laws/.

who appear before them, as well as judicial colleagues.[1048] As well, American judges use the Internet to promote and manage their election campaigns, an activity that has ethical implications for the appearance of impartiality.[1049] Both American and European judicial oversight bodies have expressed a need for judges to stay socially connected with their communities in order to gauge community standards, but within limits.[1050] For example, an ethics opinion from South Carolina found that judges could befriend on Facebook court employees and law enforcement personnel, so long as they avoided making reference to court matters.[1051] In a project on media relations for judges, the European Network of Councils for the Judiciary crafted guidelines in 2011 for use of social media and smart phones by the judiciary that would not compromise the appearance of judicial distance from the press.[1052]

The National Academy of Science as early as 2004 noted a lack of technological literacy amongst the general population in both America and European states.[1053] As juries for defamation and privacy litigation, as well as prosecutors and candidates for the bench, are selected from those populations, those findings are important indicators of how well (or poorly) scientific evidence is understood.[1054] More broadly, jurists offer

---

[1048] Kathleen Elliott Vinson, *The Blurred Boundaries of Social Networking in the Legal Field: Just "Face" it,* 41 U. MEMPHIS L. REV. 355, 399ff (2010).

[1049] Gena Slaughter and John G. Browning, *Social Networking Dos and Don'ts for Lawyers and Judges,* 73 TEX. B.J., 192 (2010) (reporting that the use of social networks by adults quadrupled between 2005-2008).

[1050] That policy has been supported in America by *Bland v. Roberts,* 57 F. Supp. 2d 599 (E.D. Va. 2012), rev'd in part, 730 F.3d 368 (4th Cir. 2013) (extending First Amendment protection to Facebook "liking").

[1051] Supreme Court Judicial Department Advisory Committee on Standards of Judicial Conduct, Op. 17-2009 (2009) as cited in John G. Browning, *Why Can't We Be Friends? Judges' Use of Social Media,* 68 U. MIAMI L. REV. 447 (2014).

[1052] *The Judiciary And The Media,* European Networks of Councils for the Judiciary http://www.encj.eu/index.php?option=com_content&view=category&layout=blog&id=21&Itemid=241&lang=en.

[1053] *Public Knowledge About S&T,* Ch. 7, Science And Technology: Public Attitudes And Understanding, NSF (2004), http://www.nsf.gov/statistics/seind04/c7/c7s2.htm - note29 (highlighting research that challenges, in light of digital technologies, the gatekeeper role of judges in admitting scientific evidence using the criteria of falsifiability, error rate, peer review, and general acceptance as set by the US Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals,* 509 U.S. 579 (1993). A study of 400 state trial court judges in 50 US states found that a majority clearly understood peer review but only a fraction clearly understood falsifiability and error rate.

[1054] A 2001 study concluded that "many judges may not be fully prepared to deal with the amount, diversity and complexity of the science presented in their courtrooms" and that "many

candid admissions that those who shape the law cannot always grasp its immediate or future applications. As cyberlaw scholar Michael Geist commented when Internet cases were beginning to appear on court dockets:

> [T]he technology involved in Internet publication is not a matter of judicial notice of knowledge. Many of the words used to describe what appears to be happening on the screen . . . are quite obviously metaphors and the Court cannot assume that they accurately describe what is actually taking place. [1055]

Hence they struggle to use technologically neutral language to avoid dating or over-particularizing their conclusions.[1056]

Judges are often tasked with using their imaginations to fashion new legal answers to problems arising from the functioning of new technology, all without overstepping their constitutionally designated functions. The judiciary must rework the materials of the common law to meet changed circumstances. Legal and institutional legitimacy in the face of such renewal depends, in large measure, on judges expanding the contours of law while "proclaiming fidelity to the past".[1057] Unlike Internet technology itself, developments in the law must be seen as continuous, not disruptive.[1058] Judges are also cautious when speaking of technology in order to prevent the need to revisit their prior decisions and preexisting doctrinal framework and often

---

judges did not recognize their [own] lack of understanding" (S.I. Gatowski, *et al., Asking The Gatekeepers: A National Survey Of Judges On Judging Expert Evidence In A Post-Daubert World*, 25 J. L. & HUMAN BEHAVIOR 433–58 (2001).

[1055] Michael Geist, *Cyberlaw shows its true colours,* Blog (6 Sept. 2001), http://www.michaelgeist.ca/resc/html_bkup/sept62001.html (citing the judge in the Federal Court of Canada case of *Guillot v Istek Corp*. [2001] F.C.J. No. 1165.

[1056] Rajab Ali, *Technological Neutrality,* 14 LEX ELECT. (Rev. du Centre de recherché en droid public) (Fall 2009) (citing the United National Convention On The Use Of Electronic Communications In International Contracts, para 5 of the Preamble, for the principle of technological neutrality as providing for the coverage of all factual situations where information is generated, stored or transmitted in electronic form, irrespective of the technology of the medium used) 2.

[1057] AUSTIN SARAT, LAWRENCE DOUGLAS & MARTHA MERRILL UMPHREY EDS, IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY, Introduction, 2 (2012), (suggesting law be an instrument of both continuity and change, all the while appearing unsettled, not reassured, by such change).

[1058] *Id.*

choose to issue more narrow decisions to avoid the difficult jurisprudential questions new technology can present."[1059]

4.6 Summary

As citizens of mature western democracies, we entrust our governments through our laws to balance our needs for liberty and security. However, false ideas or false facts by themselves are not illegal, and the dominant principle of the First Amendment is to treat falsehoods with "benign neglect".[1060] The US constitution does not offer a defence to defamation and American courts vary in opinion as to whether factual falsity is protected speech.[1061] For the most part the First Amendment shields people who make false statements, even intentionally, in the public sphere.[1062] Corporations like Google and Facebook take the position that, whether designated as carriers, controllers, accomplices or publishers in court decisions, they are engaged as innovators in the free market. Therefore, any government constraints on those activities must be authorized through the consent of the governed.[1063]

The constitutional framework of the EU, as embodied in the ECHR, similarly offers protection for freedom of speech but does not pronounce as illegal statements that are false or harmful *per se*.[1064]

The wider question addressed by this dissertation is whether the First Amendment or EU law can protect false statements in a public forum such as a new media site. One writer observes there exists very little public space online:

[1059] Mary-Rose Papandrea, *Moving Beyond Cameras in the Courtroom: Technology, the Media, and the Supreme Court*, 2012 BYU L. REV. 1901 (2012). http://digitalcommons.law.byu.edu/lawreview/vol2012/iss6/7

[1060] Alissa Ardito, *Social Media, Administrative Agencies, And The First Amendment,* 65 ADMIN. L. REV. 301, 378 (2013).

[1061] *Id.* Ardito suggests *Sullivan* implied it is; *Gertz* held it is not.

[1062] As seen in jurisprudence dealing with holocaust denial.

[1063] *Id.* at 379, (making the point that relying on government to distinguish truth from falsehood is at odds with the principles of popular government and robust deliberation at the heart of the First Amendment tradition).

[1064] Article 10 ECHR and various provisions of the TFEU (articles 49, 54, and 114) and as repeated in constitutions of individual Member States. A limited exception to harmful speech is child pornography, as addressed by the Child Pornography Directive, OJ L 335, 17.12.2011.

> Because the vast majority of websites and social media sites are in private hands, public space online, the equivalent of sidewalks and parks, which receive the highest level of First Amendment protection, is next to nonexistent.[1065]

We shall address that question in Chapter V. With respect to ISP liability discussed herein, those committed to reputational privacy are calling for a reconceptualising of free speech values to remedy the fact that "unregulated ISPs, free to engage in content discrimination or to steer user attention toward consumption, oversee nearly all online expression."[1066]

In summary, this chapter has shown that all levels of law are infused with challenges as raised by the presence of the Internet. The following broader conclusions relate those challenges to individual reputation: 1) the context of any impugned publication is critical to outcome; 2) the importance in pre-Internet law of the written/spoken distinction has become nuanced into a durability/ evanescence distinction; 3) at the heart of EU and US differences over rights to reputational privacy is the perception of individuals as either rights holders or as consumers; 4) increasingly, the binary discrepancies between offline/online and public/private activities are losing relevance when contemplating free speech or individual privacy;[1067] 5) Internet users have little *control* over third party damage to their reputations, but they have considerable *power* en masse when discrediting the reputation of others;[1068] 6) the legal infrastructure varies from one jurisdiction to the next, creating a legal balkanization of the Internet and frustrating attempts to formulate an international law of the Internet

---

[1065] Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace,* 20 BERK. TECH. L.J. 1115, 1116 (2005).

[1066] Ardito, *supra* fn 1060 at 307. Savin, *supra* fn 32 notes that the EU, through such initiatives as its Digital Agenda 2010-2020, COM(2010) 245, 19.5.2010, is focused on opening up access beyond national borders although, again, it does not constitutionally protect it.

[1067] Professor Laura Little of Temple University Beasley School of Law makes a similar observation: "To resolve personal jurisdiction and choice of law issues in internet defamation cases, U.S. courts have adapted rules from the non-internet context with relative ease. Reported cases tend to concern domestic internet disputes between U.S. entities, with few plaintiffs attracted to U.S. courts for the purpose of litigating cross-border defamation claims." *Supra* fn 757 at 2.

[1068] As Jon Ronson asks: *Do Twitter users have the right to ruin someone's life*? GUARDIAN (3 Mar. 2015) (regarding the length of alienation we judge appropriate for one reckless tweet, "It is up to us to decide: how merciless do we want to be?")

or even to enforce foreign judgments;[1069] 7) those discrepancies create expense, delay, uncertainty of outcome, and little vindication when using traditional defamation law; and 8) much of digital speech is so different in kind from offline expression that it is time to consider either a discrete legal process or extra-legal solutions.

Three broader observations relate to the cases chosen for analysis in this chapter: 1) private corporate action appears relatively immune from legal sanction as Internet companies view monetary sanctions as just another cost of doing business; 2) judiciaries on both sides of the Atlantic are struggling with the capabilities of new media and how to fashion judgments that do more than shoehorning digital speech into the timeworn legal categories created for an age of letters; and 3) despite a handful of international conventions that address reputation within the context of privacy and family life, those legal norms are not seeping down to regional or domestic judiciaries.

More specifically, in the sample cases considered, we have seen that 1) judges at the trial and first appellate levels tend not to invoke broader legal principles as contained in international legal instruments; 2) many older causes of action persist (such as criminal defamation and insult laws) that prevent development of a uniform or updated approach to reputational harm; 3) issues of jurisdiction and choice of law require up-front resources as well as emotional investment for the plaintiff even before the main contested principles can be heard; they also result in an uneven application of the law across geopolitical borders; and 4) judges and legislators are often under escalating pressure in both US and EU jurisdictions to recognize that digital speech is different that offline communications and hence it calls for more innovative or separate legal and extra-legal treatment.

[1069] The EU legal infrastructure (108 Convention, for example) has many directives that, in principle, direct activity involving the Internet. Practical enforcement is not robust, however.

CHAPTER 5 "NEW LEGALITIES" AND OTHER SOLUTIONS

5.0 Introduction

> There are calls to reconceptualize free speech values to remedy the fact that unregulated Internet service providers (ISPs), free to engage in content discrimination or to steer user attention toward consumption, oversee nearly all online expression. It may well be time for such sweeping changes.[1070]

We have seen that legal responses offered by western democracies like the US and EU have limited value in lowering our reputational risk. Like privacy, reputation is of profound personal concern but, unlike privacy, law cannot seem to close a door to the world and bring it back. Living online only complicates its vulnerability. While reputation forms our social currency without which our future is limited, legal minds cannot arrive at a remedy to guarantee its recapture. As Goffman suggests, once stigmatized, our social acceptance is permanently tarnished.[1071] In light of its complex nature (socially constructed but involving the private self, proprietary without meaningful control, reliant on trust from the very people who judge) perhaps the best law can do is to garner for us as much autonomy over its fate as society will allow, to provide a little vindication as we reorder our diminished opportunities.

We have also seen that, in Europe, the Web 2.0 is viewed as a highly regulable space; in America, it presents a mostly self-regulating marketplace for user-generated content and consumerism. Due to the spillover of online information from one geopolitical state to the next, those viewpoints must come to terms with one another and often clash. Efforts to resolve those differences are increasingly pressured by relentless technological innovation that keeps content control in the hands of Internet companies.

In this chapter I examine two such efforts, one originating in the US and the other within the EU, for the promise they hold for individuals to achieve meaningful

---

[1070] Ardito, *supra* fn 1060 at 307.

[1071] ERVING GOFFMAN, STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY, 87 (1990) (noting "The stigmatized individual is asked to act so as to imply neither that his burden is heavy nor that bearing it has made him different from us…he is advised to reciprocate naturally with an acceptance of himself and us, an acceptance of him that we have not quite extended to him in the first place.")

participation in that debate. I then move to other legal and extra legal suggestions for addressing reputational stigma and conclude with a consideration of a solution introduced in Chapter IV *supra:* whether digital speech might best be perceived as its own language, subject to its own rules.[1072]

5.1 User-Focused Legal Initiatives

Two new instruments, one remedial and one preventative, mark efforts by legislators in the EU and US to address another unique feature of Internet architecture, its persistent memory. Both models offer a user-centric tool for individual Internet users to control their online reputations. In the EU, the EUDR proposes erasure mechanisms whereby data subjects can order the take-down by Internet companies of content the data subject finds offensive or embarrassing, or the cessation of data collection and retention that no longer has their consent.[1073] In America, DNT legislation proposed in some US legislatures exhibits the more *ad hoc* and sectoral approach of US lawmakers and offers the Internet user (including children) the opportunity to proactively opt out of certain data mining and commercial access to their digital tracks by commercial agents. Those mechanisms will be compared for their effectiveness in addressing novel retention and tracking issues posed by Internet and web architecture.

a Erasure Laws: The European Harmonized Approach

i A Brief Legislative History

The most significant precursor to the EUDR is the 95 Directive, so called because of its introduction into the European Union in 1995, a time when both the political stability of the EU and individual use of the Internet were in much earlier states of their development. The total state membership of the EU was 15 that year, with Austria, Finland and Sweden having just acceded to the union.[1074] In 1995 "the Net" was an emerging technology, desktop computers were suitcase-sized and Compuserve was used to sign into USENET to get the daily news on the world wide

[1072] CH 4, section 4.4.
[1073] EC Communication To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions", Com 609, 8 (2010) (EC Communication).
[1074] Norway, after negotiations to accede, lacked the political majority in a national referendum to complete the process, as experienced by Switzerland three years earlier.

web: that dial-up process took about a minute.[1075] The principal social medium was email.

The 95 Directive was an important component of European privacy law and human rights law, but it dealt very little with the Internet. Its objective was to provide standardization of rules for all members of the EU regarding data collection by governmental, commercial and other interests that could identify individual citizens of the EU. That protection became particularly critical in the late 1990s as authorities sought to harmonize practices across all Member States in order to protect personal data as it was transmitted to any corner of the EU. To do so, the Directive set strict limits on the collection and use of personal data and demanded that each Member State set up an independent national body responsible for the protection of those data.[1076]

The 95 Directive, like all EU directives, was not a compulsory legal tool, but a guideline for crafting domestic legislation. Its provisions were sufficiently language-neutral to accommodate ICT evolution. As membership in the EU grew into the new millennium, and as collection and retransmission of personal data became more autonomous and more technologically sophisticated, EU authorities looked for a more effective regulatory tool that would reflect the two growing concerns of EU politicians: a strong digital economy for all commercial interests, and enhanced privacy protection for all EU citizens.

In January 2010, the European Commission proposed a reform of the EU's data protection rules to make them "fit for the 21st century" by addressing the vastly networked communications enabled by the Web, the Internet, and various applications such as social media.[1077] The EUDR sets out a general EU framework to meet that objective. It aims at data protection for purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

To become law, the proposed EUDR must meet the approval of four institutional authorities: the European Parliament, the European Commission, the

---

[1075] *This Was the Internet in 1995,* BUSINESS INSIDER, http://www.businessinsider.com/flashback-this-was-the-internet-in-1995-2013-4?op=1.
[1076] *Protection of Personal Data,* EUROPA, Legislation Summary, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.
[1077] EC Memorandum, Progress On EU Data Protection Reform Now Irreversible Following European Parliament Vote, Memo /14/186 (12 March 2014), http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (EC Memorandum)

European Council, and the Council of the EU.[1078] The European Parliament gave the regulation first reading on 14 March 2014 with 207 amendments to the original draft. Still outstanding at this writing is final ratification by the European Parliament and passage by the Council of the EU. The EUDR will crystalize into state law of the 28 EU Member States once approved, without need for further voting or ratification by the domestic parliaments. Although over 3,000 changes to the current Directive are under current review, the European Commission anticipates that it will be finalized and passed by the end of 2015. It is then expected to take two years from that date for the law to come into force.

In the interim, EU Member States are reviewing their data protection and privacy laws to ensure they do not conflict in principle with the proposed EUDR. All foreign countries and commercial interests that deal in any way with personal data of EU citizens are now challenged to review their data collection laws and policies to aim for compliance with the EUDR. The scope of the proposed legislation is very wide: it will affect public and private sector businesses, large and small, all of whom must have compliant in-house privacy and data protection regimes. Internet services are particularly involved, as online collection and storage is the dominant method to deal with personally identifying data.

ii Scope and Significance

The EUDR is promoted by the European Commission as the most comprehensive data protection tool in the world for meeting both individual and corporate needs.[1079] It deals with personal data that it defines as "any information relating to an identified or identifiable natural person" or "data subject ".[1080] More specifically, an "identifiable person" is one who can be identified, directly or indirectly,

[1078] The regulation requires final approval of the Council of the EU in which national Ministers sit as President on rotating basis for six months.
[1079] *Data Protection Day 2014: Full Speed on EU Data Protection Reform,* European Commission Press Release (27 January 2014), http://europa.eu/rapid/press-release_MEMO-14-60_en.htm (EC Press Release).
[1080] Proposal For A Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation) 2012/0011 (COD) (1 January 2013) Article 2a. (EUDR)

by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" such as a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."[1081] The regulation applies if the data controller or processor or the data subject is resident in the EU. Furthermore, and unlike the current 95 Directive, the Regulation applies to organizations based outside the EU if they process personal data of EU residents.

The EUDR states three policy objectives for businesses involved in the digital economy: 1) a single pan-European regime for data protection;[1082] 2) application to all foreign companies without preference;[1083] and 3) strong enforcement powers for European regulators.[1084] Compliance is the responsibility of the "controller" of a business, that is, the authority that determines the purposes and means of the processing of personal data.[1085] Small and medium sized businesses are predicted to draw particular benefit from cost savings available when dealing with one law and one data authority. Commercial interests will henceforth have a clear regulatory regime that should contribute to the health of the online global market.

Individual users, as data subjects, stand to benefit in significant ways as well. They include extended control of their own personal information once it is posted (or data collected) online, thereby resolving the issue of who owns content once it appears online. As well, in keeping with the principle of transparency, individuals' data can only be processed[1086] with their consent, to protect their vital interests as the data subject, for tasks carried out in the public interest, or in the exercise of official authority vested

---

[1081] EC Press Release *supra* fn 1078.
[1082] As was the case with the 95 Directive.
[1083] In accordance with the principle of harmonization that eliminates the need of external parties to deal with many different domestic laws. That aim necessitates the review of the current US Safe Harbor agreements.
[1084] EC Press Release, *supra* fn 1078. Fines have been projected to be 5% of yearly turnover of a data processing firm, up to 100m euros for major firms.
[1085] Draft EUDR, *supra* fn 1079, Article 2(d). All further references to 'article' in this section deal with the Draft EUDR.
[1086] Defined under Article 2(b) as ""any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

in the controller or in a third party to whom the data are disclosed.[1087] A controller is defined as the people or body, "which determines the purposes and the means of the processing" both in the public and in the private sector. A medical practitioner, for example, would routinely be the controller of the data processed on her clients that is stored within her own firm's medical record system; a company would be the controller of the data regarding its clients and employees. The *Google Spain* CJEU decision extends that responsibility to the Internet company that provides online access to such data or general information.

Very stringent rules apply to processing *sensitive* data, that is, data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs trade union membership, data concerning health or sexual preference. In principle, such data cannot be processed. Exemptions include historical and scientific research, health and other necessary institutional records, and journalistic coverage that serve the public interest.

Individual users are offered expanded rights of free erasure,[1088] rights of notification of when and how their personal data will be used including its transfer to third parties,[1089] rights to block contested data,[1090] restriction of the collection or lengthy retention of sensitive data in relation to fundamental rights of privacy,[1091] restriction of profiling,[1092] general access to their own data,[1093] its easy transfer between service providers,[1094] its general portability,[1095] and the right to be notified of any corporate data breaches in time to take appropriate action[1096] (*ie*, to cancel credit cards

---

[1087] Article 7.
[1088] Article 54. That right requires a controller to "take all necessary steps to have the data erased, including by third parties, without prejudice to the right of the data subject to claim compensation." The latter phrase retains the right of the data subject to commence a private action.
[1089] Article 48 (notification includes the existence of the processing operation, its purposes, the time the data will be likely stored for each purpose, and whether the data are to be transferred to third parties or third countries).
[1090] Article 54(a) ("Data that are contested by the data subject and whose accuracy or inaccuracy cannot be determined should be blocked until the issue is cleared.")
[1091] Article 41.
[1092] Article 58 ("Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject should only be allowed when expressly authorized by law").
[1093] Article 47.
[1094] Article 79.
[1095] Article 59.
[1096] Article 67 ("which should be presumed to be not later than 72 hours" after the breach).

or order new government licenses).[1097] A breach should be considered as adversely affecting a data subject "where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation".[1098]

Children merit particular attention when it comes to personal data, because "they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.[1099] A parent or legal guardian is required to authorize such use where the child is under the age of 13. Exceptions are made for matters of public interest, such as processing in the context of "preventative or counseling services offered directly to the child."[1100]

The enumerated rights of the data subjects are not absolute,[1101] but can only be suspended for the following purposes: to safeguard public security, including the protection of human life including response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences, for breaches of ethics for regulated professions, other specific and well-defined public interests of the EU or of a Member State such as its important economic or financial interest, or the protection of the data subject or the rights and freedoms of others. The EUDR notes that all such rights or restrictions should be in compliance with the ECHR. The EUDR would place a reverse onus on the data controller to establish why data cannot be erased.

Erasure rights extend the most direct control of users over their data and have created a great deal of media and academic interest.[1102] Known historically (and in

---

[1097] EC Memorandum, *supra* fn 1076.

[1098] Article 67 ("A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation.")

[1099] Article 29.

[1100] *Id.*

[1101] *Google Spain*, supra fn 401.

[1102] Meg Leta Ambrose, *et al., Seeking Digital Redemption: the Future of Forgiveness in the Internet Age*, 24 SANTA CLARA COMP. & HIGH TECH. L. J, 99 (2010); Steven C. Bennett, *The 'Right to be Forgotten': Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L., 161 (2012); Bernal, *A Right to Delete?' supra* fn 341; Blanchette & Johnson, *supra* fn 319. Chris Conley, *The Right to Delete*, Association for the Advancement of Artificial Intelligence, Spring Symposium Series, 8; Martin Dodge & Rob Kitchin, *Outlines of a World coming into Existence: Pervasive computing and the ethics of forgetting'*, 34 ENVIRONMENT AND PLANNING B: PLANNING AND DESIGN, 431-45; William H. Dutton, *The EU's Right to be Forgotten and Why it is Wrong,* Oxford Internet Institute (2010), http://www.oii.ox.ac.uk/people/?id=1; Karen Eltis, *Breaking through the 'Tower of Babel': A 'Right to be Forgotten' and How Trans-Systemic Thinking can help Reconceptualize Privacy Harm in the Age of Analytics*, 22 FORD. INTEL. PROP. MED. & ENT. L. J., 69; Bert-Jap Koops, *Forgetting*

earlier drafts of the EUDR) as the "right to be forgotten" or, more historically still, *le droit a l'oubli*, they are based on the data minimization principle that data controllers must keep compilations of personal data to a minimum and remove any data when it is not longer needed for the original purpose of its collection.[1103] The *Google Spain* decision particularizes that requirement to data that is inaccurate, inadequate, irrelevant, or excessive for the purpose of the data processing.[1104]The controller must respond to requests of the data subject within a *reasonable* deadline and give reasons if the request is denied. [1105] Permissible reasons include for the fulfillment of contract terms or other legal obligations.[1106]

The EUDR does not expressly define a right of erasure with respect to social media, including user generated content, false and anonymous social networking posts, or third party re-contextualized postings, that provoke reputational damage.[1107] Any mention of that aspect of forgetfulness is confined to explanatory notes in the many public speeches promoting the EUDR,[1108] in online news commentary,[1109] and through a growing interest on the part of academics.

In terms of the practical mechanics of asserting individual rights, erasure or rectification requests can be made directly to Internet companies. Those agencies must provide transparent and easily accessible and understandable information, including procedures for submitting deletion requests and reasons should those requests be

---

Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice, 8 SCRIPTed, 229-256 (2011).

[1103] EC Communication *supra* fn 1072.

[1104] *Google Spain*, *supra* n 401, para 93.

[1105] Article 47.

[1106] Article 53. Such legal reasons might include cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.

[1107] Google Spain *supra* fn 401.

[1108] Reding, *supra* fn 700.

[1109] *Private data, public rules*, ECONOMIST (28 Jan. 2012), http://www.economist.com/node/21543489; *'The Right to be Forgotten': US Lobbyists Face Off with EU on Data Privacy Proposal*, SPIEGEL (17 Oct. 2012), http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html; David Reid, *France ponders right-to-forget law*, BBC (8 Jan. 2010), http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm; *Is there a right to be forgotten on Google?* Freedom House (27 February 2013), https://freedomhouse.org/report/freedom-net/2013/france - .VRAFZUuGq1A.

refused.[1110] Data subjects hold a right of rectification of mistaken or otherwise faulty personal data or information[1111] either when (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or (b) the data subject withdraws consent for its collection or storage or the consent period has expired. [1112] Data transfers and processing by law enforcement and judicial authorities will have particularly strict guidelines,[1113] most notably in view of allegations by Edward Snowden in 2013 of spying activities of US intelligence agencies on EU high profile figures,[1114] and of other NSA activities.[1115]

There is promise of a significant impact on user rights made by the combined force of the 95 Directive, the clarification of its current scope in the *Google Spain* case, and the user-directed provisions of the EUDR. Their combination should aid in shaping an omnibus EU law with broad scope both inside and outside the EU that defines a European model of data protection and Internet company liability. The broad strokes of the EUDR are mostly backed up by domestic laws in each of the 28 Member States already in place as inspired by the 95 Directive.

iii Responses to EUDR with Respect to Reputation

Through the EUDR, the European Commission promotes three legal principles that underlie the legitimacy and stability of the EU: transparency, proportionality, and

[1110] Article 11.
[1111] Article 15(e).
[1112] A further elaboration of Article 12(b) of the 95 Directive.
[1113] *Fact Sheet: EU-US Negotiations on Data Protection,* IP/10/1661, EU-US "Umbrella Agreement" for transfers and processing of data in the context of police and judicial cooperation, http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf.
[1114] *Joint Press Statement* following the EU-US-Justice and Home Affairs Ministerial Meeting in Washington DC (18 Nov. 2013), http://europa.eu/rapid/press-release_MEMO-13-1010_de.htm. ("We together recognise that this has led to regrettable tensions in the transAtlantic relationship which we seek to lessen. In order to protect all our citizens, it is of the utmost importance to address these issues by restoring trust and reinforcing our cooperation on justice and home affairs issues.")
[1115] Kelly D. Dubacki, *Renewed Calls for Finalization of EU Data Protection Regulation by 2015,* FIRST ADVANTAGE (29 Sept. 2014), (noting that the EP Civil Liberties Members inserted increased safeguards in the draft EUDR for data transfers outside of the European Economic Area, including heftier fines, an explicit consent requirement, and a right to erasure, roughly 4,000 amendments in total.)

legitimate purpose.[1116] Within the context of data protection, the European Commission explains *transparency* as the right of every European citizen to know how the European institutions are collecting their data, who participates in that collection, and what documents are held or produced. The right extends to accessing those documents and making one's views known, either directly, or indirectly, through intermediaries.[1117] *Proportionality* generally involves regulating the exercise of powers by the EU. It seeks to set within specified boundaries the actions taken by the institutions of the EU. Under this principle, the involvement of the institutions must be limited to what is necessary to achieve the objectives of the Treaty on European Union.[1118] In other words, the content and form of the action must be in keeping with the aim pursued.[1119] *Legitimate purpose* assumes that personal data will only be processed in accord with the provisions of Article 7 of the 95 Directive.

Within the EU there is, predictably, resistance to the legislation as it is currently drafted. Jan Philipp Albrecht, as vice-chairman of the European Parliament's civil liberties committee, has identified Germany's concern with how the EUDR might erode the sovereignty of the country's powerful regions (Lander) in relation to the federal government.[1120] He notes both France and Germany are also sensitive to the idea that data issues could be decided in the smaller member states with less established data

---

[1116] *EU Data Protection Policy*, (asserting "personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose and proportionality.")

[1117] European Commission, *Transparency Portal*, http://europa.eu/rapid/press-release_MEMO-13-1010_de.htm.

[1118] Treaty On The Functioning Of The European Union (TFEU) C 83/49 1 December 2009, renamed, consolidated and amended by the Treaty of Lisbon (OJ C 326, 26 Oct. 2012), Article 5.

[1119] Europa: Synthèses de la Législation, http://europa.eu/legislation_summaries/glossary/proportionality_en.htm. In its decision in the case of *Digital Rights Ireland Ltd. (C–293/12) v. Minister for Communications, Marine and Natural Resources,* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1, the Grand Chamber of the CJEU determined that the EU had exceeded the limits of proportionality in drafting the 95 Directive.

[1120] Jan Philipp Albrecht, *Draft Report On General Data Protection Regulation*, COD 2012/0011 (12 Dec. 2012), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. *See also* Simon J. McMenemy, *Further Delay to the EU Data Protection Regulation,* Ogletree Deakins Blog (4 Mar. 2015), http://blog.ogletreedeakins.com/further-delay-to-the-eu-data-protection-regulation/ - sthash.u9gs6RSF.dpuf.

protection traditions. The United Kingdom is opposed to the entire EUDR document, preferring that the EU adopt a new directive with members states who will bring it into force in their own way similar to pending directives on nuisance callers and spammers.[1121]

For American businesses involved in the use of personal data of EU citizens, however, the EUDR provisions provide a considerable barrier to business as usual. Provisions that most affect US businesses include 1) specified fines for non-compliance;[1122] 2) inclusion of data processing of personal data regardless of whether the data belongs to persons EU citizens or residents and regardless of whether the controller is resident in the EU;[1123] 3) the need to report to EU data supervisory authorities any mass surveillance activities of the US government (as reported by Edward Snowden) to receive supervisory permission in order to transfer such data;[1124] and 4) the requirement that successful erasure requests are forwarded to third parties that might control replications of the data.[1125] The most controversial provision is (3) above regarding government surveillance.

US litigants are already engaged in disputes over court orders by US judges compelling the transfer of data out of the EU because one side argues that US law requires the provision of certain evidence, and the other argues that doing so would make its EU subsidiary or parent violate the applicable EU law. Such discrepancies are expensive and time consuming for litigants. EUDR provisions will need to be scrutinized to assure litigants that such procedural discrepancies are addressed. In this

---

[1121] *Anti-Spam Activities,* European Union Agency for Network and Information Security (ENISA) http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/anti-spam-measures.

[1122] Article 79. For example, Google announced $50 billion in revenue for 2012, meaning a maximum fine under the proposed EU data protection laws could total up to $2.5 billion.

[1123] Article 3. *See further,* Francois Gilbert, *A Legal Analysis of the updated EU General Data Protection Regulation*, ITLAW.com, http://searchcloudsecurity.techtarget.com/tip/A-legal-analysis-of-the-updated-EU-General-Data-Protection-Regulation (outlining such new provisions as Article 9 that establishes a new category of sensitive data known as "gender identity").

[1124] Article 43(a).

[1125] Article 17. Important limitations of the right to erasure include making it dependent upon the data controller's ability to verify that the person requesting the erasure is also the data subject; allowing companies to block, rather than erase, data where a particular technology does not allow erasure (article 17(4)); and exempting data needed to complete a contract or fulfill other legal obligations (article 53).

and a variety of other ways, American sources are the most vocal critics of the EUDR; then again, the US has the largest stake in the digital economy with respect to its Internet companies and collateral industries.

Regarding the practical details of individual take-down requests, an Internet company's procedure up to this point is to direct users with deletion requests to site operators. For example, educators concerned with the defamatory details of a posting on the Rate My Professors site would go to the "help" function on the <http://www.ratemyprofessors.com/help.jsp> site and follow the instructions under "Can I flag a comment or professor note that I think should be removed from your site?" They will be asked to report any postings that contain, 1) profanity, name-calling, derogatory remarks about religion, ethnicity or race, physical appearance, mental and/or physical disabilities; 2) references to a professor's sex life, including sexual innuendos; 3) claims that a professor shows bias for or against a student or specific group of students; 4) claims about a professor's employment status, including previous employment; 5) claims that a professor engages or has engaged in illegal activities; and 6) accusations that the professor is rating him/herself or his/her colleagues; [1126]

The website creators address liability for defamation to third parties with the statement that all postings are opinion, not fact.[1127] More recently, as the enactment of the EUDR with its right of erasure seems more certain, Google and its video arm YouTube are dedicating teams of administrators and paralegals to vet requests. Take down requests from government agencies are not processed automatically unless accompanied by court order.[1128] Google raises in defence of its decision to deny a take-down request that the applications lack important detail, or that complete erasure of content is technologically impossible or infeasible due to costs of tracking third party use.[1129] In general, Google staff review and categorize requests as defamation, copyright

[1126] Terms & Conditions, *Rate My Professor,* http://www.ratemyprofessors.com/TermsOfUse_us.jsp.
[1127] *Id.*
[1128] *Google refuses US request to video,* Alakhbar (16 Sept 2012. http://english.al-akhbar.com/node/12230 (Note: cut and paste: link does not respond to hyperlinking command).
[1129] See further *Access to Information,* Google Transparency Report, http://www.google.com/transparencyreport/. *See also* Don Reisninger, *Google: More government takedown requests than ever before,* CNET (25 Apr. 2013) at http://www.cnet.com/news/google-more-government-takedown-requests-than-ever-before/ (reporting Google received take

infringement, or violence, and appear prepared to reveal the number of successful requests but not the reasons.[1130]

As indicated earlier, the major concern over the EUDR provisions for erasure is the quasi-judicial role bestowed on the few largest Internet companies.[1131] Their staff function as the first layer of authority to vet erasure requests from individual users. The principle objection is that the key players in the Internet industry thereby become the first line arbiters of online content, a distribution of power in opposition to that anticipated by the promoters of the EUDR.[1132] The only guidance provided by the CJEU, through the *Google Spain* decision, is that the data subject's rights should override the interest of Internet users as a general rule, and that the balance of interests should be determined on a case-specific basis.

Academic response to the passage of the EUDR has been generally favourable,[1133] urging compliance by US Internet companies.[1134] Paul Schwartz criticizes the EUDR initiative for, among other things, heightening individual rights of privacy beyond those accepted in the US. Schwartz advocates diminishing the role of the European Commission as the final arbiter of information privacy disputes under the EUDR, primarily because of the US preference for self-regulation regarding transborder data transmission.[1135]

---

down requests for 24,179 pieces of content by government around the world between July and December of 2012).

[1130] Rebecca J. Rosen, *Google Refuses to Remove Police-Brutality Videos,* ATLANTIC (27 Oct. 2011), http://bangordailynews.com/2011/10/31/news/nation/google-refuses-to-remove-police-brutality-videos/ (note: the original link has been removed by content carrier).

[1131] For further discussion of Google take-down requests, *see* Rosen, Delete Squad, *supra* fn 970.

[1132] Most notably EC Commissioner and the EUDR's most vocal promoter, Vivienne Reding, FaceBook posting, (concluding that "Companies can no longer hide behind their servers being based in California or anywhere else in the world.") *See contra,* Meg Ambrose, *EU Right to be Forgotten Case: The Honorable Google Handed both Burden and Boon* (19 May 2014), http://playgiarizing.com (concluding that "the intention of the European Union to redistribute power away from companies and toward users backfired [because] Google gets to decide what the right to be forgotten means, because its interpretation of the right will be as good as anyone else's guess.")

[1133] For the European view, *see* Christopher Kuner, *The European Commissions' Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law,* Bloomberg BNA PROV. & SEC. L. REP. (6 Feb. 2012) 1-15.

[1134] Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV L. REV. 1966 (2013).

[1135] *Id.,* at 1968.

In preparation for the EUDR, the current US-EU agreements concerning data export involving EU residents are under review. The Safe Harbor provisions; Model Contractual Clauses;[1136] and Binding Corporate Rules[1137] only require proof of 'adequate' data protection, a standard much lower than for other exporting countries.[1138] For its part, the US has maintained that a combination of policy responses do provide adequate data protection by combining to provide a type of collaborative 'lawmaking', with compliance overseen by the FTC.[1139]

b Do Not Track Laws: The US Sectoral Approach

The Do Not Track (DNT) policies in the US represent a different approach to individual control over one's online content: injecting FTC oversight into unauthorized commercial access to a person's digital tracks. Interestingly, the original guidelines drafted for US government agencies in the 1970s were very similar to the current EUDR provisions.

i A Brief Legislative History

DNT policies were created to provide an easy mechanism for consumers to opt

[1136] The current framework makes each party responsible for any damage it causes to the data subject (*see* Schwartz, *supra* fn 1133).
[1137] Under current agreements, data export is permitted if exporters can prove the data will receive 'adequate' privacy protections while in transit. It has been the opinion of the EU that US privacy legislation did not meet that standard, although neither side has requested a clear definition of 'adequacy'. The ARTICLE 29 Working Party, a group of European data protection officials, was of the opinion in 1999 that the "patchwork of narrowly focused sectoral laws and voluntary self regulation [of US data transmissions] cannot…be relied upon to provide adequate protection in all cases for personal data transferred from the European Union." *Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 1/99* concerning the level of Data Protection in the United States and the Ongoing Discussion between the European Commission and the United States Government, at p. 4, DG MARKT DOC 5098, WP 15 (26 Jan 1999).
[1138] 95 Directive, fn 667, Article 25(1). The EUDR will require a level of data protection "equivalent" to that provided for internal data transfers between Member States.
[1139] Schwartz, supra fn 1133 at 1980; *See* Issuance Of Safe Harbor Principles And Transmission To European Commission, 65 Fed. Reg. 45,666 (24 July 2000); EU Commission Decision 2000/520/EC (26 JULY 2000) Pursuant To Directive 95/46/EC Of The European Parliament And Of The Council On The Adequacy Of The Protection Provided By The Safe Harbor Privacy Principles And Related Frequently Asked Questions, US Department Of Commerce, 2000 O.J. (L215) 7.

out of online tracking that led to targeted or behavioral advertising.[1140] As indicated in Chapter 3, tracking of our online activity involves targeters or advertising companies contracting with online publishers to place a piece of tracking code on its site that, when you visit the site, will inject cookies into your computer that enables digital tracking of all the sites you visit or browse online.[1141]

In 2010, the FTC endorsed the concept of a universal browser-based DNT signal that could be inserted into online services and programs. Much earlier, in the 1970s, the DNT concept was raised on a formal governmental basis by the US Department of Health, Education, and Welfare. At that time a voluntary *Code of Fair Information Practices* was devised to form the backbone of a US privacy law model that included data collection and use. The key policy points of the code were openness (no secret personal data record keeping systems); disclosure to data subjects; no secondary use of data without full disclosure to the data subject; ability of the data subjects to correct false or outdated data; and assurance by collectors of the security of the stored data against third party unconsented use. Many of those policies reflect provisions of the draft EUDR.

While those principles were influential in formation of some state laws, no overarching federal privacy law was ever developed covering public and private sector data collection. Neither was there created a federal privacy commission unlike in the EU and may commonwealth jurisdictions. The result has been a patchwork of laws with many gaps.[1142] For example, the federal *Do Not Track Me Online Act*,[1143] introduced into Congress in February of 2011 but never passed, was specifically targeting the blocking of all collection of personal data for behavioral advertising purposes, with an exception for fraud prevention and inventory control. The bill also authorized the FTC to create nationwide regulations that required DNT technologies to be implanted into devices, and to use random audits of web publishers as an enforcement mechanism. Five

---

[1140] Laura Drell, *4 Ways Behavioral Targeting is Changing the Web,* Mashable (26 APR. 2011), http://mashable.com/2011/04/26/behavioral-targeting/.
[1141] Ch. 3, section 3.3(iv) *infra.*
[1142] Beth Givens & Sen. Steve Peace, *A Review of State and Federal Privacy Laws,* Testimony To The California Legislature Joint Task Force On Personal Information And Privacy, Privacy Rights Clearinghouse (1997-2014), https://www.privacyrights.org/ar/jttaskap.htm.
[1143] House of Representatives 654 (112th), introduced into the US Congress by Representative Jackie Speier for the 112th session and referred to Committee.

additional attempts have been made in the US to introduce similar legislation, most invoking the FTC to set an 'opt out' regime for online tracking as well as other user-directed mechanisms to discourage third party tracking.[1144]

ii Scope and Significance

Unlike the uniform approach to data protection and user control envisioned by the EUDR, American DNT policy and legislative tools regarding information privacy have proceeded in a much more *ad hoc* fashion. For example, there is one set of statutes for the public sector and another for the private one. Further, US private sector legislation distinguishes between types of data. The variety of US legislation governing the regulation of data collection and transfer just at the federal level is wide: it could involve the *Sarbanes-Oxley Act of 2002*[1145] for the financial sector;[1146] the *Financial Modernization Act of 1999* (Gramm-Leach-Bliley Act)[1147] to protect the privacy of consumer information held by financial institutions; or the *Economic Espionage Act of 1996*.[1148]

On the state level, the passage of the California DNT legislation, *The California Online Privacy Protection Act*, marks the first successful codification of DNT policies in any US jurisdiction.[1149] It requires any operator of a website, online service, or mobile

---

[1144] *California Senate Bill 761* (14 March 2011), http://info.sen.ca.gov/pub/11-12/bill/sen/sb_0751, (Lowenthal Bill on computer spyware); *Consumer Privacy Protection Act Of 2011,* (14 March 2014), http://www.gpo.gov/fdsys/pkg/BILLS-112hr1528ih.pdf (introduced by House Representatives Stearns and Matheson); *A New Commercial Privacy Bill Of Rights,* (14 March 2014), http://www.kerry.senate.gov/imo/media/doc/Commercial (introduced by Senators Kerry and McCain); *Do Not Track Online Act Of 2011* (14 March 2014), http://commerce.senate.gov/public/?a=Files.Serve&File_id=85b45cce-63b3-4241-99f1-Obc57c5c1cff (introduced by Senator Rockefeller); *Do Not Track Kids Act Of 2011,* (14 March 2014), http://online.wsj.com/public/resources/documents/billdreaft050 (introduced by House Representative Markey).

[1145] *Sarbanes-Oxley Act of 2002,* PL 107-204, 116 Stat 745 (July 2002) (Devised to regulate corporate financial reporting following the Enron and WorldCom scandals).

[1146] *What is the Sarbanes-Oxley Act?* Legislative And Governance Fact Sheets (2005), http://www.securit.com/legislative/sarbanesOxley.pdf.

[1147] *Financial Modernization Act of 1999,* Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 1999).

[1148] *Economic Espionage Act of 1996,* 18 U.S.C. 1831 (theft for the benefit of a foreign entity) and 18 U.S.C. 1832 (theft for pecuniary gain). (Oct. 1996). Both encompass electronic storage.

[1149] *The California Online Privacy Protection Act,* A.B. 370 (CalOPPA as amended); *See background,* Ivan Rothman & Philip Zender, *California passes the first "Do-Not-Track" legislation in the US,* ITCAN LEXOLOGY (24 October 2013)

application that collects personally identifiable information about California residents to include DNT disclosures in its privacy policy. That disclosure would reveal any third party tracking activities on the operator's website and explain how the operator responds to web browser DNT signals or other mechanisms used by individuals to stop such tracking.[1150] The Act does not require website operators to incorporate DNT technologies into their sites or services nor does it require operators to respond to DNT signals used by data subjects in a certain manner. If an operator does not respond to such signals, it will suffice merely to indicate this fact in its privacy policy. The legislation limits operator responsibility to setting forth its privacy policy in a separate online location accessible by hyperlink. Once again, any active opting in or out is left to the individual user. Should the operator violate any terms, it has 30 days from the time of notice of the violation to comply or be subject to fines of up to $2500 per violation.[1151] That fine is often justified by operators as the cost of doing business, so the California Attorney General has clarified that each download of a non-compliant mobile application constitutes a single violation.[1152]

A similar first step has been taken through the California *The Student Online Personal Information Protection Act*[1153] regarding children's rights of online erasure, dubbed by the press as a youth "erasure button".[1154] The draft law stipulates that websites and applications directed at children under 18 must allow registered users to remove publicly posted content and make certain disclosures to those users.[1155] A

---

http://www.lexology.com/library/detail.aspx?g=a51c3fe0-98b8-4c2d-9035-01e32f2576e2. The act is in the form of an amendment to the California Online Privacy Protection Act of 2003 (CaIOPPA).

[1150] *Id,* s.1. The legislation amends the *Business and Professions Code*, s. 22575, and only required the operator to 'describe',' identify', and 'disclose' certain third party practices involving PPI of users.

[1151] Cal. Bus. & Prof. Code § 17206(a).

[1152] *AB370: California's "Do Not Track" Law,* Cooley LLP, http://www.cooley.com/ab370-californias-do-not-track-law.

[1153] *The Student Online Personal Information Protection Act* – Sb 1177 (in force 1 Jan 2016) (Student Online Act). The Act amends s. 22581 of the California Business And Professions Code and becomes effective 1 January 2015. US congressman Edward Markey spearheaded the initiative, calling for technological adaptation of website access to enable erasure of search histories that reveal personal information of child Internet users.

[1154] Mike Reicher, *State law allows kids to clean their digital past",* Orange County Register (24 SEPT 2013), http://www.ocregister.com/articles/online-527862-companies-law.html (arguing adults would benefit from a similar law in America).

[1155] Or ask the provider to remove or anonymize.

website or application is directed to a minor (under 18) when it is "created for the purpose of reaching an audience that is predominately comprised of minors, and is not intended for a more general audience comprised of adults."[1156] A complete expunging is not required: deleting the requested content from viewer accessible websites will suffice, even though it remains on the operator's servers in some form.[1157]

iii Responses to DNT with Respect to Reputation

Internet researcher Adam Thierer characterizes the DNT mechanism as "a browser-based tool that tells advertisers and other third parties not to follow us around the Internet".[1158] In policy terms, he suggests the anti-tracking device transports the EU data minimization principle to the US. Thierer warns, however, that such technology proposed for California minors opens a back door for hackers or "others with malicious intentions". The uneven history of data protection in the US might be attributed in some regards to the lack of uniform definition of online "tracking" as well as government policy concerns about undermining commercial entities that rely on behavioral tracking and subsequent advertising for economic survival.[1159]

As most online activities are free to the consumer, commercial interests argue that behavioral advertising is carrying the weight of the digital economy. That pull between individual privacy expectations and the economic wisdom of the market overshadows transnational efforts to reach agreement on the legal efficacy of anti-tracking. A prominent example is the lack of direction in the wake of the 2012 meeting in Amsterdam between the European Commission's top privacy panel, the Article 29 Working Group, and the World Wide Web Consortium (W3C) a global standards group that promotes good governance of the Internet.[1160] The talks foundered on what types of user data advertisers should be allowed to collect while respecting the right of

[1156] Student Online Act, *supra fn* 1153, s. 22581(a)(1) to (4).
[1157] *Id.,* s. 22581(d).
[1158], Pursuit of Privacy *supra* fn 160 at 413.
[1159] *Id.* at 414.
[1160] Kevin O'Brien, *Privacy Advocates and Advertisers at Odds Over Web Tracking,* NYTIMES (4 Oct. 2012), http://www.nytimes.com/2012/10/05/technology/privacy-advocates-and-advertisers-at-odds-over-web-tracking.html?pagewanted=all&_r=0. (W3C was founded 20 years ago by Web inventor Tim Berners-Lee to garner support for an open Web).

consumers to "simply and effectively declare their 'do not track' preferences on Web sites."[1161]

Advertisers express concern that EU regulation could diminish the amount of free information that users access on the Internet and could "create incentives for online companies to erect pay walls and lead to more shotgun forms of advertising."[1162] As US data collection regulator, the FTC has contributed to the conflict by exempting Internet companies, including Google, Facebook, Microsoft and Apple, from tracking oversight in 2011, arguing consumers gave implicit consent to data collection by signing up for their services. In the EU, regulators perceive that tracking is illicit in any form without the data subject's consent. Such discrepancies could lead to a "two-track do-not-track system" which makes cross-Atlantic compliance costly and perpetuates choice of jurisdiction issues – none of which helps either side.[1163]

A critical impediment to the success of DNT policies is public confusion or ignorance regarding tracking policies. Two studies have found that individual users are not aware of such data protection measures in the US. The Hoofnagle study found that almost 66% of American Internet users have never heard of DNT.[1164] The 2012 study additionally determined that a significant number believed their activities online were protected by strong privacy laws, but could not provide details when asked, a failing that raises doubt about the viability of the notice-and-choice process and the ability (or willingness) of individual users to make informed opt out choices.

An earlier US study by McDonald and Peha similarly reported that a wide gap existed between the capabilities of DNT technology and the expectations of users.[1165] While users currently have a choice of total blocking of all advertising data collection

---

[1161] Advertisers' interests in the DNT debate are represented internationally by the Digital Advertising Alliance, the lead organization representing online advertisers, within the US by the Association of National Advertisers, and in the EU by the International Advertising Bureau, among others.

[1162] O'Brien, *supra* fn 1159.

[1163] *Id.*, as per Jeffrey Chester, Center for Digital Democracy.

[1164] Chris Hoofnagle, Jeff Urban & Su Li, *Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection of Data About their Online Activities*, Berkeley Consumer Privacy Survey & Research Paper, (8 Oct., 2012) http://ssrn.com/abstract=2152135.

[1165] Aleecia McDonald & Jon Peha, *Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature*, Tracking Position Working Group, SSRN, http://ssrn.com/abstract=1993133 (2011) (McDonald Study). Online survey April 22-29, 2011, n=293.

(opt out) or only those selected by the user (HTTP cookies), most participants of the McDonald study were unaware of the difference, and believed if they chose a DNT option all of their personally identifying information was deleted all of the time. McDonald found participants to be naïve about more aggressive data mining technologies as well, such as flash cookies[1166] (that evade the opt-out settings) and cache cookies (that store webpage history for fast retrieval).[1167] As users become more knowledgeable about DNT technologies, advertisers become more creative in their innovations for data collection, igniting the semblance of a virtual "arms race".[1168]

The key concern for researchers was the users' imbalance of technological savvy. For example, when users delete cookies believing they are erasing data collection capabilities of advertisers, the McDonald study determined that they are often deleting the opt-out function instead.[1169] The study concluded that users do not have a nuanced understanding of DNT technology; about 25% expected they would be exempt from all commercial tracking by merely clicking a DNT option and a further 50% believed they were completely exempt from any tracking (commercial or government or private) simply by choosing one of the options available. When informed such expectations were not valid, those users displayed a general distrust so eroded in the opinion of the researchers that "there may not be many options for engagement left."[1170]

Public ignorance of DNT capabilities is troubling, particularly to the FTC. In 2010 it promoted three priorities its staff determined would move users closer to informed choices for protection: greater industry transparency, privacy by design at every stage of product development, and implementation of greater consumer choice

---

[1166] Tanzina Vega, *Code Known as Flash Cookies Raises Privacy Concerns*, NY TIMES (20 Sept. 2010), http://www.nytimes.com/2010/09/21/technology/21cookie.html?_r=3& (noting that at issue is "a little-known piece of computer code placed on hard drives by the Flash program from Adobe when users watch videos on popular Web sites like YouTube and Hulu.")
[1167] John Herrman, *What are Flash Cookies and How Can You Stop Them*? POP. MECH. (23 Sept. 2010) http://www.popularmechanics.com/technology/how-to/computer-security/what-are-flash-cookies-and-how-can-you-stop-them (advising that "Every time you surf the Internet, your browser collects bits and pieces of information from the sites you visit, either in the form of cache, which stores photos and site data on your hard drive to help speed up page loading, or cookies, which are small files deposited on your computer so Websites can remember certain things about you" such as shopping preferences).
[1168] McDonald, *supra* fn 1164 at 2.
[1169] *Id.*
[1170] *Id.* at 30.

and hence control through such mechanisms as DNT tools.[1171] In a follow-up report in 2012, the FTC reported have brought enforcement actions against 1) Google and Facebook for failing to gain express consent of users before changing their data practices;[1172] 2) online advertising networks that failed to honor opt outs; 3) mobile applications that violated the *Children's Online Privacy Protection Act*; 4) applications that set privacy settings in a way to cause consumers to unwittingly share their personal data; and 5) companies that sold consumer lists to advertisers in violation of the *Fair Credit Reporting Act*.[1173] The FTC further announced it would increase vigilance against de-anonymizing activities of companies, and against information brokers who buy, compile, and sell highly personal information about consumers but never interact with them.[1174] The 2012 Report sets the following future goals: intensified DNT implementation; increased privacy initiatives by mobile service companies; increased access by consumers to information about them held by data brokers; and the creation of sector-specific privacy codes of conduct.[1175]

Not all major browsers and web servers are on board, however, foretelling a possible regulator-industry clash. Yahoo! announced in May 2014 its intention not to honour DNT customer requests, and to disable web browser DNT settings, primarily due a lack of a single, easy-to-use standard that has been adopted "by the broader tech industry."[1176] Google has "opted out" of DNT policies as well.[1177] Facebook similarly announced its decision to dishonour DNT browser settings in June of 2014, except for iOS (Apple) and Android devices, and to employ its 'like' function for subscriber tracking- all because of a lack of industry consensus.[1178] AOL followed in August of

---

[1171] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* (December 2010), http://www.ftc.gov/opa/2010/12/privacyreport/shtm.
[1172] The FTC reported over 1 billion users of both online services.
[1173] FTC 2010 Report, *supra* fn 1171 at iii.
[1174] *Id.,* at iv.
[1175] *Id.,* at ix.
[1176] *Yahoo's Default = a Personalized Experience,* Yahoo Privacy Team, (30 April 2014), http://yahoopolicy.tumblr.com/post/84363620568/yahoos-default-a-personalized-experience.
[1177] Zach Minors, *How bickering and greed neutered the 'Do Not Track' privacy initiative,* PC WORLD (22 May 2014), http://www.pcworld.com/article/2158220/do-not-track-oh-what-the-heck-go-ahead.html.
[1178] Cotton Delo, *Facebook to Use Web Browsing History for Ad Targetting,* Digital Advertising Age (12 June 2014), http://adage.com/article/digital/facebook-web-browsing-history-ad-targeting/293656/.

2014.[1179] Other industry leaders are more compliant: one source reports that 12 percent of Firefox users around the world have opted into Mozilla's DNT program, that Microsoft's Internet Explorer and Apple's Safari now block many cookies by default, and that most mobile devices, including the iPhone, don't allow use of cookies in its applications.[1180] The initiative taken by Microsoft and Apple raises the stakes in the debate, accelerating protests from advertising industry associations. Those actions nevertheless fall far below the expectations of the FTC for a nationwide program to gain some control over behavioral tracking.

The principal advantage for industry (and challenge for the FTC) is that, in the legislative vacuum created by the inability of Congress to agree on a uniform DNT law, major Web companies and intrepid start-ups are offering "personalized services" that streamline web searches and allow portability between personal devices,[1181] generally through cookie alternatives that are getting smarter and more difficult to spot or disable.[1182] Start-up companies add new meaning to the word "interoperability" by selling tracking devices that can link smartphones, tablets, personal computers and even Internet-connect televisions to an autonomous entity that uses algorithms to sift through their programs for IP addresses, browsing patterns, and buying preferences.[1183] The resultant cross-device advertising illustrates the relentless surge of innovation when regulation falters or becomes entrenched in only one game plan.

c. Can the EU and US Agree on Data Protection Mechanisms?

Unlike the influence US policies confer in the areas of copyright, net neutrality, and cybercrime, information privacy policies are being set by a combination of US and EU initiatives. The good news about both the EU and US mechanisms is in its message to legal, political, and civic sectors that governments are proactive in their response to

[1179] Wendy Davis, *AOL Won't Honor Do-Not-Track Requests,* MEDIA POST (19 Aug. 2014), http://www.mediapost.com/publications/article/232394/aol-wont-honor-do-not-track-requests.html.
[1180] Olga Kharif, *The Cookies You Can't Crumble,* BLOOMBERG BUSINESS WEEK (21 Aug 2014), http://www.businessweek.com/articles/2014-08-21/facebook-google-go-beyond-cookies-to-reap-data-for-advertisers.
[1181] Yahoo, *supra* fn 1175.
[1182] *Id.*
[1183] Daposh Dutta Roy, *Changing trends in Marketing,* LinkedIn (2 Sept. 2014), https://www.linkedin.com/today/post/article/20140902140606-616354-changing-trends-in-marketing.

digital invasive practices. Policy setters have erected privacy infrastructures that, in principle, provide a backdrop against which Internet users can react. Until recent successes with movement towards some consensus over passage of the EUDR, the gap in cooperation between EU and US authorities did not look likely. Industry leaders have begun to comply with the implementation of the EU model, however, due in large measure to their impatience with the lack of progress with the federal US model, coupled with the forceful *Google Spain* characterization of Internet companies as "controllers" with direct liability.

One potential outcome of the EU-US differences in data protection policies is for each jurisdiction to go its own way. That do-nothing option appears practically unworkable for a few reasons. One of the practical impediments to perpetuating the *status quo* involves the expense and frustration of the simple act of getting disclosure for litigation. In cases involving the cross border transmission of personal data, US requirements are much wider, calling on litigants to produce any requested information under their control without regard to whether the information originated in the US or elsewhere or to whose private information they are disclosing.[1184] EU regulations, meanwhile, prohibit the transfer to the US of data on its citizens that originates within its borders because it has determined that the US lacks adequate data protection standards.[1185] The resulting EU-US safe harbor arrangement,[1186] by which US companies may voluntarily increase their level of data protection in order to conduct data exports involving EU citizens, creates problems for a smooth and predictable sharing of disclosure. Legal compliance in one jurisdiction means noncompliance in the other.

Another impediment is the difference in evidence gathering for private law cases. Under the common law (US), evidence is gathered by both parties and presented to the opponents during pre-trial discovery. In civil law jurisdictions, including many EU Member States, the judge determines which evidence is necessary and collects that evidence, including taking witness statements. While those differences are not

---

[1184] Carla L. Reyes *The U.S. Discovery –EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy,* 19 DUKE J. COMP. & INT'L L. 359 (2009).
[1185] 95 Directive, *supra* fn 667.
[1186] U.S. Dep't Of Commerce, Safe Harbor Privacy Principles (July 21, 2000), http://www.export.gov/safeharbor/SH_Privacy.asp.

insurmountable, they give fundamental messages about who conducts the release of personal information in each legal system and call on special procedures that are not automatic and hence that create uncertainty, additional costs, and frustration for the parties.

US adoption of the EU model would clearly provide the least expensive answer to the compliance issue. The EUDR is in the final preparatory stages: it has been approved by the European Parliament and awaits final amendments. One proposed change by the Italian EU Presidency that is being given serious consideration adds further enticement for US authorities to consider adopting more EU-like practices. It involves the granting of binding decision-making to a centralized EU data protection Board with arbitration powers if data protection measures cannot be worked out at the local level by Member State authorities.[1187] US Internet industries look upon this as streamlining their information flow activities into "one stop shopping". That means businesses operating across the 28-nation EU would have to deal only with the data protection authority in the country where they are headquartered, even if alleged mishandling of data affects citizens in another country. That new feature makes the EUDR more palatable to US companies in terms of cost in data mobility, a factor that could be quite persuasive as the US DNT model founders.[1188].

In introducing its *Privacy Bill of Rights* in 2012 that urged a comprehensive nationwide DNT program, the White House indicated America's intention of pursuing its own course in regulating the flow of personal data.[1189] Less than two years later, the

---

[1187] Julia Fioretti, *EU mulls conferring binding powers on body of data privacy regulators,* REUTERS (14 Nov. 2014), http://www.reuters.com/article/2014/11/14/us-eu-dataprotection-idUSKCN0IY1LR20141114.

[1188] US Consumer Bill of Rights, Draft 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (upholding ISP exemptions stated in s. 230 of Communications Decency Act); *Editorial: Should US Adopt the Right to be Forgotten Electronic Data Collection Raises Privacy Issues,* Conn. L. Trib. (3 Oct. 2014), http://www.ctlawtribune.com/id=1202672292749/Editorial-Should-US-Adopt-the-Right-to-Be-Forgotten-Electronic-Data-Collection-Raises-Privacy-Issues?slreturn=20141014150309.

[1189] *We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online,* Press Release, White House Office Of The Press Secretary (23 Feb. 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

program is perceived as seriously log-jammed.[1190] The formal mechanisms are in place: the Commerce Department has been tasked with creating enforceable policies, the FTC has queued up as nationwide enforcer, and the advertising industry has agreed to support DNT.[1191] The inherent flaw in moving DNT forward is that, even with DNT technology as part of online systems, users might still need to initiate them, a requirement that calls for user understanding of the basic mechanics of opting out and privacy settings. In some ways we are back to the notice and choice model whose uneven application led to the formation of DNT policies in the first place. In the vacuum created by the slow development of a federal DNT regime, state legislators are devising their own privacy laws in many sectors, a development that localizes the law on data privacy in the US, just as national laws in EU Member States have threatened to 'balkanize' Internet regulation across the EU.[1192]

As Thierer observes more broadly, "information control has always been complex and costly",[1193] increasingly so as expanding ways to steal, invade, and manipulate stores of personal data or posted content challenge government efforts to maintain free access and minimum regulation of online spaces.

5.2 New Legal Responses

a Internet Companies as Controllers: *Google Spain*

With the long-awaited *Google Spain* decision, the CJEU achieved two things that had a major impact on individual control of online personal information. It judged Internet companies to be "controllers" of such information with respect to data

---

[1190] Sandra Fulton, *One Year Later, Consumers are Still Waiting on a Do Not Track Standard,* ACLU.org (24 Apr. 2013), https://www.aclu.org/blog/technology-and-liberty/one-year-later-consumers-are-still-waiting-do-not-track-standard; Somini Sengupta, *No U. S. Action, So States Move on Privacy Law,* NYTIMES (30 Oct. 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?pagewanted=all&_r=0;

[1191] *Id.*

[1192] *State Laws Related to Internet Privacy,* National Conference Of State Legislatures (NCSL) (23 Jan. 2014) http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (outlining how schools can collect student data, how websites post privacy policies, how to protect readers' online purchasing choices, how to get personal information held by ISPs, how to require employers to give notice before monitoring employee email, and tightening up warrantless police searches of cellphone contents.)

[1193] *Id.*

involving EU citizens or for Internet companies offering services in EU Member States. Being identified as a controller meant liability for data misuse that threatened individual user's reputational privacy. It also granted unprecedented autonomy to individuals regarding the collection, processing, leakage, and mobility of that information.

Prior to the CJEU decision, take-down requests were limited. The head of Google in the United Kingdom admits they were only successful if they referred to information deemed illegal by a court (such as defamation), pirated content (once Google was notified by the right's holder), malware, child sexual abuse imagery and other things prohibited by local law (such as material that glorifies Nazism in Germany).[1194] The large number of US victims of data mishandling had no recourse; FTC sanctions against major offenders did not have any impact on individual cases of exposure and litigation would have been far too expensive unless class actions were pursued, a long and costly undertaking with uncertain outcomes.

Control of the individual over her personal information was limited in other ways. People did not know what data identifying them was being collected, profiled, or shared with other institutional third parties. For example, medical information from laboratory tests or clinical trials is frequently sold to pharmaceutical companies in formats that can be de-anonymized. That practice has received legal recognition by the US Supreme Court in its 2014 *Sorrell* decision.[1195] People also were unaware of all the agencies and businesses that were collecting their data or when their stored data was subjected to hacking, loss, negligent handling, or other activities that jeopardized their privacy. If leaks, exposure or loss occurred, there was little recourse that compensated the data subject. If a victim of negligent or ruthless data use became aware of such exposure, there were no intermediaries she could appeal to for information, damage control, or compensation.

This lack of transparency hid the extent and acceleration of the exposure problem: an IBM study in 2013 revealed that American companies are attacked an average of 16,856 times a year, and that many of those attacks result in a quantifiable

[1194] David Drummond, *We need to talk about the right to be forgotten,* GUARDIAN (10 July 2014), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate.

[1195] *Sorrell v. IMS Health Inc.,* 131 S.Ct. 2653 (2011), where the US Supreme Court held that a Vermont statute that restricted the sale, disclosure, and use of records that revealed the prescribing practices of individual doctors violated the First Amendment.

data breach.[1196] A pictograph of the world's biggest breaches and hacks (*see* APPENDIX B, pictogram 2) indicates the size of such breaches in 2014 alone: Adobe (152 billion accounts); JP Morgan Chase (76 billion); Ebay (145 billion); Target (70 billion); Gmail (5 billion); and AOL (2.4 million).[1197] With today's data moving freely between corporate networks, mobile devices, and the cloud, data breach statistics show this disturbing trend is rapidly accelerating. Affixing ISP and Internet company liability, along with a more structured and international data collection regulatory regime, is one answer being pursued on the international level.

b Reputational Injury as a Tort

The creation of a new tort of reputational injury has definite appeal. It might more adequately provide remedies for personal exposures.[1198] A new reputation law might serve several needs: 1) it could force courts to clarify reputation as a societal value and a legal concept; 2) it would sharpen distinctions between various types of reputational harm (exposure versus disclosure) so that suitable remedies might be more adequately fashioned; 3) it would allow courts to more closely monitor the means-end relationship between harm and liability; 4) it might clarify the distinction, if any, between defamation and the false light privacy cause of action. The latter would particularly reduce the amount of claims pleaded in the alternative and hence reduce court costs and delays. Such a proposal could also increase the seriousness with which reputational suits are perceived and call for clearer thinking on the discrete nature of online reputational damage. A new law of reputational injury could also expand legal analysis on how the First Amendment might be modified in its application for new media cases in view of a lack of institutional mediation and other indications that digital speech might be a unique species of communication.

[1196] *1.5 million monitored cyber attacks in the United States in 2013,* IBM Data Breach Statistics, (April 2014), http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/.

[1197] *World's Biggest Data Breaches,* Information Is Beautiful pictogram, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[1198] Heymann, *supra* fn 174 at 1424 (suggesting such a tort could clarify the overlap between defamation claims and those brought using the false light privacy tort.)

c A Discrete Law for Digital Speech

i A Critical Need

Creating a separate legal space for digital speech is another response that addresses the unique ability of online messaging to put another person's reputation at risk. Such a proposal recalls the contrary opinions of Justice Frank Easterbrook of the US Court of Appeals[1199] upon the emergence of the law of the Internet: that it made about as much sense as creating a law of the horse.[1200] He found such a proposal frivolous because the need would be based on technology, not on norms or industry.[1201] Easterbrook's objection was the unattainability of legal principles for a subject that is so rapidly evolving:

> [W]hat I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile.[1202]

He also objected on the grounds that the law of the computer smacked of dilettantism: it was without serious subject matter and was an attempt to use clairvoyance to decipher the future: [1203]

> Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.[1204]

Lawrence Lessig rebutted Easterbrook's objections stating that, essentially, cyberspace was a discrete entity and the need for cyberlaw an example of legal exceptionalism as

---

[1199] Frank Hoover Easterbrook has been a Judge of the United States Court of Appeals for the Seventh Circuit since 1985. The US Courts of Appeals are considered among the most powerful and influential courts in the United States; only 1% of their decisions are heard by the US Supreme Court.

[1200] Cyberlaw, IT law, computer law and the law of Internet have been used interchangeably in this dissertation.

[1201] Frank H. Easterbrook, *Cyberspace and the Law of the Horse,* 1996 U. CHI. LEGAL F. 207 (1996); *see also*; Andrew Murray, *Looking Back at the Law of the Horse: Why Cyberlaw and the Rule of Law are Important,* 10 SCRIPTed 310 (2013), http://script-ed.org/?p=1157. Examples of law based on industry are space law or railroad law.

[1202] As cited in Murray, *id.* at 313.

[1203] Later developing into cyberlaw.

[1204] Murray, *supra* fn 1200 at 313.

determined by the intricacies of computer code and the digital market.[1205] Andrew Murray of the London School of Economics believes we have not met Easterbrook's objections head on because we continue to use "the language and rhetoric of social policy, sociology and political philosophy," such as the literature of communications theorists like Manuel Castells and the philosophical thinking of Michel Foucault. In other words, "[w]e become social scientists not lawyers." [1206]

Despite those objections, the Internet has several idiosyncrasies that recommend separate legal treatment for the language used in digital spaces, most of which reference technological capacity but all of which shape human behavior online. New media communications can be, for example, immediate and spontaneous; truncated and filled with digital semaphore, [1207] unmediated; internationally accessible; consensually anonymous and interactive;[1208] archived in perpetuity and with no entry costs.[1209] Of those qualities, three particularly raise issues of free speech – the spontaneity of messaging that results in fragmented speech; the anonymity of messages that encourages incivility; and the ability for permanent archiving with indeterminate third party access. All three factors can exacerbate our reputational risks that warrant direct legal protection. For example, posted or texted content can inform, alert, persuade, or convert. Those are positive attributes that advertisers and reputational management firms count on. On the other hand, content can confound the recipient or judge in that translation is needed to decode the cryptic terms of regular users. It is its own language.

The very complexity of determining whether offending content is defamatory, a breach of confidentiality, or a privacy offence within traditional categories of law illustrates the non-traditional nature of online communications. For example, is a YouTube video that harms your good name actionable as libel or slander? What about the reader commentary displayed below the video? If you did not post the video but are the subject of its contents, can you claim a proprietary interest in the video? Is texting an abbreviated form of writing or speaking?

[1205] Lawrence Lessig, *The Law of the Horse: What Cyberlaw might Teach,* HARV. L. REV. (1999)
[1206] *Id.*
[1207] Employing terms such as "btw" or "by the way", lmao or "laughing my ass off", all of which need context and cultural cues to determine intent.
[1208] Karniel, *supra* fn 433 at 220 confirms anonymity is well accepted by cyber culture.
[1209] This paragraph is an expansion of ideas introduced in section 4.4 *supra.*

Linguist John McWhorter of Columbia University suggests texting and other digital messaging is more speaking than writing. "Texting isn't written language," he claims, "[i]t much more closely resembles the kind of language we've had for so many more years: spoken language."[1210] Why not write like we speak, McWhorter proposes, — looser, more casual, telegraphic, and less reflective? Primarily, he answers, because we haven't had the right tools. Pencils, typewriters, even computers were too slow to keep up with the pace of human speech. The speed and convenience of the mobile phone or tablets could achieve it. "Fingered speech" is developing its own form and vocabulary; it does not measure a decline in written speech but an evolution of a new means of communication. McWhorter gives as example the changing nuances of the acronym "lol". Its original literal translation was "laughing out loud," but with use it has adopted a subtler meaning as demonstrated in a texting exchange McWhorter observed between two 20-something college students:

> Susan: lol thanks gmail is being slow right now
> Julie: lol, i know
> Susan: i just sent you an email
> Julie: lol, i see it [1211]

McWhorter sees "lol" becoming something far subtler than laughing out loud or "loving you lots". "It's a marker of empathy of accommodation," he notes, what linguists call a "pragmatic particle," like the word "yo." Another practicality is the recently minted acronym "TLDR" which is a disclaimer-type reference to a text that is "too long, didn't read" or the use of a forward slash (/) to indicate the author is changing topic. In some ways, texting resembles Pitman shorthand, an American transcribing system from the 1950s that few would argue should be taken for a written code, not a standard form of communication. It was semaphoric in style and economic in its abbreviation of words through symbols. For judges or jurors to be tasked with finding criminal intent or the civil standard of liability in such fragments would seem akin to deciphering a unique code or language.

As well as exhibiting a different form and more nuanced messaging, digital speech contains its own *cultural* coding. Words or images that might not offend in one

---

[1210] Michael V. Copeland, *Texting isn't Writing; it's Fingered Speech',* WIRED (1 Mar. 2013) http://www.wired.com/2013/03/texting-isnt-writing-its-fingered-speech/.
[1211] *Txting is killing language. JK!!* TED2013 YouTube (Feb. 2013), http://www.ted.com/talks/john_mcwhorter_txtng_is_killing_language_jk?language=en.

culture or religion could vilify in another. That provides another challenge for anyone who attempts a legal response to impulsive, emotionally charged digital speech. Take-down requests of Internet companies track that standard setting most frequently. For example, the Turkish government demanded YouTube remove videos posted by Greek soccer fans who claimed Turkish player Kemal Ataturk was gay; YouTube agreed to its removal from Turkish access but allowed its dissemination in other countries where wider tolerance of sexual practices is the norm. France and Germany outlaw any speech that even hints at holocaust denial or that promotes Nazism; America seems more tolerant of hate speech as long as it is not dangerous or incites violent behavior. As Jeffrey Rosen summarizes,

> the American First Amendment tradition…allows speech to be banned only when it is intended—and likely—to incite imminent violence or lawless action. By contrast…European law draws a tighter line, prohibiting so-called group libel, or speech that offends the dignity of members of a protected class and lowers their standing in society.[1212]

Rosen characterizes decisions regarding protected online speech differently from one side of the Atlantic to the other: Americans, he observes, are guided by democracy, Europeans by civility.

As pointed out earlier in this chapter, the provision in the EUDR that places erasure decisions in the hands of Internet company staffers effectively bestows judicial-like power. Such "delete squads"[1213] are tasked with vetting takedown requests primarily by studying the language used in all its nuances and interpretations.[1214] Jeffrey Rosen has studied the basis for such takedown decisions and has determined they are based on arbitrary criteria that are not necessarily conveyed to the individual applicant. He reveals that delete squads have settled on accepting content that targets institutions, such as churches and governments, but not groups or their members. To

[1212] Rosen, Delete Squad, *supra* fn 970.
[1213] *Id.* Jonathan Zittrain sees the self-appointment of Google staff to vet deletion requests as usurping the sovereignty of European powers and suggests the task is better placed with EU Data Protection Authorities: "It turns a rights problem into a customer service issue, and one that Google and others in its position no doubt rightly disdain. If Google can process 70,000 requests, so can and should the data protection authorities." *See further* Jonathan Zittrain, *The Right to be Forgotten Ruling Leaves Nagging Doubts,* FINANCIAL TIMES (13 July 2014).
[1214] *Google Transparency Report*, (14 Nov. 2014) http://www.google.com/transparencyreport/removals/copyright/ (claiming it receives over 12 million URL takedown requests from its search engine each week).

state "I hate the Pope" is acceptable under those guidelines; to say "I hate Muslims or Jehovah's Witnesses" is not.[1215] In essence and practice, then, those new delete squads are a law unto themselves.[1216] Further, they need not give reasons for their decisions, other than to ensure that they align with internal policies and data retention laws.

Devising a law of digital speech would mean expanding on all of the above possibilities of language, a feat that could call on linguists and other language specialists. It would find resources in a variety of experiences, from UN debates to cryptography practices, from those who analyze hate speech to interpreters of signing or online flaming. All participants in such a legal system would need to keep an open mind regarding the cultural histories that certain words carry. As the ECtHR advised in the 1976 British obscenity case, *Handyside v. United Kingdom*,

> Freedom of expression...is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.[1217]

A law of digital speech might be as obscure as a law of the horse. In the spirit of innovation that spawned the cyberworld, however, we could engage those in the emerging field of social media studies with constitutional experts, linguists, systems languages, and others with a professional interest in decoding social media speech. An auspicious starting place would be the Universal Declaration of Human Rights for its pronouncement that,

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media* and regardless of frontiers." (emphasis added)[1218]

[1215] *Id.*

[1216] With the exception of executive or court orders, with which they must comply.

[1217] *Handyside v. United Kingdom,* 1 Eur. Ct. H.R. (Ser. A) *737* (1979), para *49*. The court did not, however, decide for Handyside who was charged with publishing obscene materials in *The Little Red Schoolbook*.

[1218] Universal Declaration Of Human Rights, *supra* fn 619.

ii Aim, Scope, and Form of Digital Law

If we were to design a law to deal with digital speech *vis a vis* the protection of reputation, what features would it have? We would have to ensure, firstly, that such a law acknowledges that individual reputation has social capital, that is, worth in the eyes of one's entire community and that its misuse would have has implications both societal and personal. In terms of the scope of the law, the model would focus on human activity, not technological possibilities. Unlike the myriad EU regulations and directives, as well as the various national and state laws in the US that focus on digital technologies, a critical feature of a Digital Speech Law would be its regard for individual rights (to Internet access, to free speech online, to speech format) while setting out responsibilities (to self-educate regarding the legal limits of self speech, to consider digital spaces in the spirit of community stewardship, etc). It would address conduct beyond what ethical guidelines would do but would stop short of regulating the particularities of speech defined by culture or geography. Available defences or excuses would arise from those limits. Such a law could incorporate national, regional, and international laws addressing those rights and responsibilities.

In terms of the particular aim and scope of the law, the mandate of judges, mediators or other directing figures would be to seek a deeper understanding of what constitutes a welcoming and respectful online communicative environment, to place that determination as much as possible in the hands of the individual participants, and to create a tone of edification and leniency, not one of exacting retribution so prevalent in today's private law solutions. They could achieve this objective by pursuing clarity of meaning over certainty of word choice.[1219] Context would be critical. In order to avoid dictating that context, lawmakers would need to take a page from their policymaking colleagues who strive for technologically neutral language when drafting technology-

[1219] *cf.* Chris Reed, *How to Make Bad Law: Lessons from Cyberspace,* 73 MOD. L. REV. 903-932 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1696691 (promoting a law that encourages individual inhabitants of cyberspace to determine whether their behaviors have met limits set by computer and communications law). A program of research to tap the precise capabilities of each media is also critical: *see, for example,* Dhiraj Murthy, *Twitter and elections: are tweets predictive, reactive, or a form of buzz?* 18 INF. COMM. & SOC. 816 (2015), (examining almost 350,000 tweets about the 2010 US primaries and found they served a 'buzz' or reactive rather than a predictive function.)

focused law: they would use "linguistically neutral" or "culturally neutral" language as much as possible. This law would foster a certain expertise in digital speech for judges, mediators, or other facilitators who direct the process. There is precedent in arbitrators of labour disputes or jurists involved in drug courts or mental health courts who accrue special knowledge. This law, and those professionals, would not address immoral or treasonous acts already captured through criminal laws or insult laws. They would not concern themselves with reputational risks posed by government institutions that are already addressed by government oversight bodies. They would deal with offending behavior between individuals, not between individuals and commercial entities as is the object of data protection and anti-tracking laws. In furtherance of that aim, the law would be silent on the role of Internet or Web companies regarding their respective liability for the content they transmit.[1220] That would avoid a judge or mediator having to deal with duties to disclose anonymous contributions and sources.

In terms of procedure, the model would require cheap and quick entry into the legal process so that reputational damage could be speedily suppressed to stem unending or unquantifiable third party regeneration online. We would frame the problem within the private law system, distinct from so-called cybercrimes against the state that are already addressed by national laws in western states. Determination of choice of law and jurisdiction issues up front would be important in reducing uncertainty and expense. A hierarchy of non-acceptable online behavior might be devised, correlated with the risk or loss to which the plaintiff has been subjected. Alternatively, the judge or mediator could work in each case to have the parties determine their own hierarchy within their particular normative circumstances.

Remedies would incorporate the reasonable wishes of the plaintiff, modified by input from community sources or other expertise. While aiming for a speedy resolution to diminish cost and the further publicity affecting reputation, the law would canvass a variety of remedies that do not commodify reputation by placing a dollar on one's good name. There would be the recognition of aggravating circumstances for a defendant trying the plaintiff in the court of public opinion prior to legal process. One innovative remedy would be to have the defendant pay for reputational management services of the

[1220] That issue is currently addressed through the *Communications Act* in the US and the 95 Directive within the EU as interpreted by the *Google Spain* decision of the CJEU.

plaintiff if the online damages so warranted. Another would be to order the defendant to produce an online posting that not only recanted his offending accusations but that extolled the particular virtues or successes of the maligned plaintiff, all subject to the plaintiff's consent and review. Such remedy would meet the concern of privacy scholar Helen Nissenbaum that personal information ought to be distributed and protected according to norms governing distinct social contexts, whether it be workplace, health care, schools, or among family and friends.[1221]

With respect to the function of the law in relation to other laws involving cyberspace, the lawmakers might consider Karniel's more liberalist position that the Internet is a new playing field for freedom of expression and such spontaneous, anonymous expression has very little significance or reliability in proving harm to one's reputation in the absence of a consideration of the "totality of circumstances".[1222]

5.3 Extra-legal Responses

a Online Civic Monitoring

Ideally, Internet content hosts could serve a function similar to real time social conveners or impresarios of information. University of Cornell communications professor Tarleton Gillespie is advancing a similar idea when he speaks of Google and MySpace as "curators of public discourse" in that their technologies mediate between various sectors of online community. Those sectors include individual users, advertisers, major media producers it hopes to have as partners, and policymakers.[1223] "Community" is used here in its broadest sense to indicate an interacting population of various kinds of individuals considered collectively, especially in the context of social values and responsibilities. [1224] Content hosts serve as intermediaries in assembling those communities, by intervening in the delivery of content, cultivating relationships,

---

[1221] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).
[1222] Karniel, *supra* fn 433 at 232.
[1223] Tarleton Gillespie, *The Politics of Platforms,* 12 NEW MEDIA & SOC. 347-364 (2010) https://dspace.library.cornell.edu/bitstream/1813/12774/1/pop.pdf ; *see also* Ardia *supra* note 10 at 321 (suggesting that the term 'platform' has a variety of context-dependent meanings including computational (something to build upon), architectural (open and egalitarian, not an elitist gatekeeper of expression), figurative (accommodating abstract ideas), and political (providing a podium from which to be heard) 3.
[1224] Oxford Dictionary Online.

serving advertisers, and distinguishing between user generated content and advertising content - all the while striving to remain neutral.[1225] Its services must be simultaneously specific and flexible, "anticipatory but not causal",[1226] and must appeal to all users as egalitarian and democratizing in order to garner wide participation.[1227] It is that neutral, anticipatory role that web hosts can fulfill by monitoring what serves civic interests without defaming them or exposing their most personal data.

Alternatively, web hosts can provide a platform for such communities to comingle amongst those of like interest without host intervention. Ardia points out that, even in the absence of legal liability, many online communities are "experimenting with various forms of dispute resolution procedures and reputation management systems".[1228] No longer confined to a shared space or time, but acting in a decentralized and independent manner to safeguard a shared value, such community members need not know one another, subscribe to larger ideologies, share a language, or identify themselves to each other in order to effectively monitor online space to protect reputations. Communities can also be fluid, coming together once, over one issue, and then dissolving.

A prominent example of such *ad hoc* communities is a large group of Facebook subscribers who united online to protest changes to privacy terms of service by both Facebook and the photo sharing website Instagram.[1229] Those two companies had introduced into their privacy policies their intention to connect users with each other, or with advertisers, in order to promote wider advertising potential.[1230] In 2009, without forewarning subscribers, Facebook executives decided to advance that scheme by claiming ownership of personal content posted on its site that had been provided by subscribers when they first created a personal profile.[1231] Facebook justified its move as

---

[1225] Gillespie, *supra* fn 1222 at 3.
[1226] *Id.*
[1227] Yochai Benkler, *Freedom in the Commons: Towards a Political Economy of Information,* 52 DUKE L. J. 1245-1276 (2003).
[1228] Ardia, *supra* fn 10 at 321.
[1229] A photo sharing site.
[1230] Kevin Systrom, *Thank you, and we're listening,* Instagram Blog, http://blog.instagram.com/post/38252135408/thank-you-and-were-listening.
[1231] Marshall Kirkpatrick, *Facebook Management Has Lost its Grip on Reality,* Readwrite.Com, (26 Feb. 2009), http://readwrite.com/2009/02/26/facebook_managment_has_lost_it; *see also* dana boyd, *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*, 14 CONVERGENCE 13, 13-14 (2008), http://www.danah.org/papers/FacebookAndPrivacy.html (explaining the

an attempt to intensify subscribers' social networking by linking users who shared interests, birthplaces, consumer tastes, and other indicators of community. The *ad hoc* community of protesters held Facebook to account for invasion of privacy and manipulation of its informational property.[1232] Facebook retreated under that community's pressure.

Instagram, now owned by Facebook, tried a more far-reaching strategy in 2012 when it sold images posted by its subscribers to advertisers without users' consent. Many photographs contained images of children. Users objected to the loss of privacy and disclosure of personal information.[1233] In response, Instagram initiated an opt-out privacy setting that relied on user initiative to set privacy boundaries. Instagram CEO Kevin Systrom explained the company's strategy through an example: Instagram might promote a brand X and show Facebook visitors which of their friends already follow Brand X, blurbs that could include their user name and avatar. Systrom reassured Instagram subscribers that they still "own their content and Instagram does not claim any ownership rights over your photos."[1234] Instagram followed that gaffe with a verification scheme in 2014: subscribers were notified that, unless their posted photographs were to be accompanied by an arrow, they would be deleted. The arrow of "verification" was obtained by clicking on an icon that, when clicked to reveal a drop down page, displayed accounts similar to theirs. That scheme appeared to have little to do with deletion prevention and much to do with trying to generate a list of users with shared interests, presumably to sell to advertisers.[1235]

Both examples illustrate the potential of communities to change industry practices where their privacy is concerned. Such communities of power might be

---

2009 virtual assembly of interest groups like "Students Against Facebook News Feeds" that totaled 700,000 Internet users to protest Facebook's launch of News Feeds. That feature presented a start page listing of every act undertaken by a Facebook subscriber's friends each time the subscriber logged on to the system.)

[1232] Juan Carlos Perez, *Facebook tweaks Beacon again, Zuckerberg apologizes,* Computerworld UK, (7 Dec. 2007), http://www.computerworlduk.com/news/security/6592/facebook-tweaks-beacon-again-zuckerberg-apologises/.

[1233] Jenna Wortham, *Facebook responds to anger over proposed Instagram changes,* NYTIMES (18 Dec. 2012), http://www.nytimes.com/2012/12/19/technology/facebook-responds-to-anger-over-proposed-instagram-changes.html?_r=0.

[1234] *Id.*

[1235] Christopher Boyd, *January 1st Instagram Profile Deletion Hoax,* Malwarebytes (30 Dec. 2014) https://blog.malwarebytes.org/fraud-scam/2014/12/january-1st-instagram-profile-deletion-hoax/

limited in their influence, however, due to economies of scale. As an analyst with a private research group advising on disruptive technologies comments, "There's not a lot of portability. Where would you go?"[1236] To its credit, Facebook is presenting the incident as a learning moment, and has committed to a set of Principles it created and submitted to subscribers for comment. The company pledges to let its community of members vote on contentious practices that affect them.[1237]

Former Microsoft social media researcher dana boyd sees these movements as far more complex and involving several communities of interest. In the following excerpt, for example, she identifies *five* such communities that have been affected by Facebook's 2009 gaffe:

> The disconnect between average users [*community #1*] and the elite [*community #2*] is what makes this situation different, what makes this issue messier. Because the issue comes down to corporate transparency, informed consent, and choice…I think that it's important that the techno-elite and the bloggers [*community #3*] and the journalists [*community #4*] keep covering this topic…[W]e also have to contend with the fact that most people being screwed don't speak English [*community #5*] and have no idea this conversation is even happening. Especially when privacy features are only explained in English. [content in brackets added][1238]

Boyd makes a call to arms to each of the above communities to "challenge Facebook to live up to a higher standard, regardless of what we as individuals may gain or lose from their choices."[1239] She also takes it upon herself as an elite user "to make sure that everyone is informed and actively engaged in a discussion about the future of privacy."[1240]

The community David Ardia envisions has no need of a formal legal apparatus to protect online reputation. Community players assume a central role in community governance because they are often in a position to recognize and respond to reputational harms, a more engaged and influential force than individual subscribers acting alone. Ardia suggests that we enlist their help, through social incentives, to mitigate

---

[1236] Rebecca Lieb as cited in Wortham, *supra* fn 1232.
[1237] Tom Spring, *Dawn of a Facebook Democracy? Users Invited to Shape Site's Policies,* PCWORLD, (26 Feb. 2009) http://www.pcworld.com/article/160314/facebook.html.
[1238] Dana boyd, *Quitting Facebook is pointless: challenging them to do better is not,* Apophenia Blog (23 May 2010) http://www.zephoria.org/thoughts/archives/2010/05/23/quitting-facebook-is-pointless-challenging-them-to-do-better-is-not.html/comment-page-1.
[1239] *Id.*
[1240] *Id.*

reputational harm while maintaining an environment "conducive to public engagement and vigorous debate."[1241]

b Online Reputation Ranking Systems

Another community-based approach to safeguarding reputation is to ensure the reliability of reputational information we read online rather than trying to impose legal liability. There exists a community of websites devoted to that task: large-scale word-of-mouth networks.[1242] EBay, for example, was designed with a built-in review system so that its buyers and sellers could review or assess each other and hence build trust in certain participants and in various products.[1243] Within that system, by adding commentary as either buyer or seller, we designate select websites as our online communities for that particular purpose. Amazon, another reputational rating system, goes one step further by permitting buyers to rate the choices of others. Netflix provides similar rating opportunities, for either one's own movie choices or for those of other users within the same household. Xbox Live, a gaming site, rates gamers against the performance of other gamers using scoreboards in order to reward them and help them find opponents with similar skill levels. Until the summer of 2014, the website Technorati served as a rating system for blogs in various subject areas.[1244] Rating systems have been democratized in the sense that many online activities in which we participate call for user ratings: examples include rating requests (Rate and Review your shopping experience, service experience, viewing experience, etc.) sent to purchasers of e-books through Google and Amazon, recipients of online technical help at Apple, and online conferences, podcasts, or courses we experience.

Chrisanthos Dellarocas of Boston University's School of Management suggests such reputation management systems fulfill four primary roles: 1) they build trust in the reputation of another person by encouraging positive behaviors and discouraging

[1241] Ardia, *supra* fn 10 at 264.
[1242] Chrisanthos Dellarocas, *The Digitization of work-of-Mouth: Promise and Challenges of Online Feedback Mechanisms,* 49 MGMT SC. 1407-1424 (Oct. 2003).
[1243] *E.g.* The Technorati system of ranking weblogs as outlined by Ardia, *supra* fn 10 at 321, note 393.
[1244] Greg Finn, *RIP Technorati Blog Search & Rankings: The Once Popular Blog Tools Have been Sunset,* Search Engine (26 June 2014), http://searchengineland.com/rip-technorati-blog-search-rankings-popular-blog-tools-sunset-195186 (A decline in blogging and a concurrent rise in social media use forced its demise.)

negative ones within a site; 2) they filter high quality content from lesser content; 3) they attempt to neutralize or even out a wide array of subjective contributions or products; and 4) they "lock in" users who have established a reputation and loyalty through their contributions to a particular site.[1245] A reputation system must decide which behaviors it wishes to feature; that will determine the information it will collect to promote that message. For a professor, for example, those behaviors relate to the three components considered for promotion and tenure: teaching, research, and service.

Institutions such as universities employ websites to build both institutional and individual reputations. They participate in a reputation system that evaluates their ranking and value system among professors. The choice and placement of information on faculty websites signal what factors are of most value to the university or faculty. For example, a professor's degrees are usually listed prominently on her homepage, as are areas of research and courses taught. Should the professor hold a particular research chair or have been granted a major funding allocation, additional esteem is signaled within the professional community by announcements on the website. Individual faculty webpages list a professor's publications; research areas are also listed. Both build the professor's scholarly reputation while building institutional reputation. Similar benefits accrue from lists of industry and professional awards, scholarship funds, and endowments. Faculties frequently post the rankings of their school in comparison to others if favourable (QS World University Rankings, for example). Teaching awards bestow additional prestige, indicating an elevated trust component amongst students. By posting such achievements on the institutional website, school and faculty receive reciprocal benefit.

The home page of the law faculty at Stanford University is exemplary of those features.[1246] It presents, at center page, a column of most recent publishing contributions from the entire pool of faculty. While building institutional reputation, that listing also elevates a particular professor above her peers and serves to urge others to follow suit that, in turn, will build the institutional reputation even higher. Faculty are also encouraged to tweet about publications authored by themselves and their colleagues and include a link for a more interactive experience.

[1245] Chrisanthos Dellarocas, *Designing Reputation Systems for the Social Web,* Boston U. School Management Research Paper 2010-18, (June 13, 2010) http://ssrn.com/abstract=1624697.
[1246] *Stanford University,* Home Page, https://www.law.stanford.edu/.

Customer or peer ratings, another online reputational measurement, can work either for or against an individual or institution and so calls for serious deliberation before choices are made. Review of a professor's work for example, by publishers or colleagues or students, can bolster her reputation; it can also carry bias or inaccuracies that will persist and be globally available. One way to reduce those risks is to implement a rate-the-rater mechanism into the system, as is used in restaurant or book reviews where readers of reviews comment on their usefulness or credibility. One can usually "game the system" as was revealed at an American university where a professor was found to have negatively rated a colleague on the <ratemyprofessor.com> website whom he found particularly threatening due to his comparatively greater achievements.[1247]

A prominent reputation system for the academic world is offered by the Social Science Research Network (SSRN), an online publishing and rating service. All submissions are made available to anonymous readers despite the article's publication history. A reputation service is provided through the compilation of statistics that track the number of times the abstract has been accessed, the number of downloads of the full article, and how that statistic ranks with other downloads. The number of footnotes is provided, as well as the number of citations from those sources. Similar works of other authors are promoted in a sidebar. A feedback function allows users to make suggestions regarding their selections. The contact information of each author is provided, as well as the institution where she teaches. A "top paper" and "top author" ranking is also provided, as is a listing of "top organizations" that rates universities and law schools by country and on an international scale. Authors, in turn, are encouraged to email or tweet announcements of upcoming publications, an endeavor that can boost both individual and institutional reputation. The concept of rating systems for law practitioners is receiving academic interest; one such article points out the additional layer of complexity brought to the reputational issue when considering the professional obligation of confidentiality.[1248]

[1247] Mike Resnick, *Professor Fired for Trashing Colleagues on Professor Ratings Site,* Techdirt, (22 Feb. 2006), https://www.techdirt.com/articles/20060222/221239.shtml.

[1248] Angela Goodrum, *How to Maneuver in the World of Negative Online Reviews, the Important Ethical Considerations for Attorneys, and Changes Needed to Protect the Legal Profession,* Expresso (2015) http://works.bepress.com/angela_goodrum/ .

The above discussion establishes that design choices for a reputational system can profoundly affect a community's culture, with potential to make either a collaborative and cordial community or "a competitive and even combative space."[1249] If used with careful deliberation, however, it can also generate user loyalty, mutual respect, institutional pride, and lasting impressions for the reader.

c) Expiry Dates

In 2009, Victor Mayer-Schönberger offered expiry dates as an extra-legal solution for users' data protection online.[1250] This technical default system would trigger the dissolution of personal information at a user's pre-set date. Such external mechanisms would remind us of the "finiteness of information",[1251] hone our skills at data conservation, and instill an appreciation for the data minimization thinking akin to that promoted by the EU agenda for harmonization. Mayer-Schonberger maintains such a technological solution would compel us to decide how long our information remains relevant and valuable. He urges that data cleaning, just like fridge cleaning of foods past their expiry dates, reinforces the importance of forgetting: it "shifts the default back from pervasive remembering to human-controlled forgetting."[1252]

The debate over the technological realities of the persistence of data is not resolved and provides a complication to Mayer-Schonberger's practical suggestion.[1253] Jeffrey Rosen warned in 2010: "[T]he Internet records everything and forgets nothing … every online photo, status update, Twitter post and blog entry by and about us can be stored forever."[1254] As discussed earlier, several Internet scholars point out that, if only through a plethora of technological glitches and errors, online content does have a

[1249] Dellarocas, *supra* fn 1244 at 8.
[1250] Mayer-Schonberger, *supra* fn 161 at 171.
[1251] *Id.*
[1252] *Id* at 172.
[1253] Meg Ambrose, *It's about Time: Privacy, Information Life Cycles, and the Right to be Forgotten,* 16 STAN. TECH. L. REV. (Winter 2013), 121-125 (ably setting out both sides of the permanence/ephemerality debate).
[1254] Jeffrey Rosen, Forgetting, *supra* fn 172.

life span. The permanence argument might just have met its match in the data ephemerality discourse.[1255]

d A Bifurcated Space for Online Speech

One high-risk feature of the Internet is its ability to take gossip that is scattered, forgettable, and localized and transform it into a form that is permanent and infinitely searchable.[1256] The defining attributes of gossip are that it is conversational, often unattributed, casual or unconstrained, and about other members of our community. Due to its details that cannot be confirmed as true or false, gossip cannot become the subject of a legal action such as defamation or breach of confidence.[1257] Nor does it rank as opinion, because gossip is a social currency I pass to others, not a commodity I routinely create. As gossiper, my function would be to merely keep it in social circulation. Synonyms such as rumours, tittle-tattle, whispers, carnards, scandal, hearsay, dirt, buzz or scuttlebutt suggest that, while neither good nor evil, gossip is still unfavourable to its subject and hence potentially harmful to reputation.[1258]

In democratic regimes, the law takes only a tangential interest in gossip. It is concerned with protecting speech but only to the extent it does not wipe out any future chance I have for advancement or social engagement.[1259] The rationale is to avoid one of two extremes: the triggering of a chill of expression if too harsh, or the enabling of circulation of one's secrets if too lenient. If the latter, the gossip subject might find it harder to engage in self-exploration if "every false step and foolish act is chronicled

[1255] Ambrose, *supra* fn 1252; *see* also Mary Rumsey, *Runaway Train: Problems of Permanence, Accessibility, and Stability in the Use of Web Resources in law Review Citations,* 94 LAW LIBR. J. 27, 35 (2002); Mary K. Taylor & Diane Hudson, *"Linkrot" and the Usefulness of Web Site Bibliographies,* 39 REF. & USER SERVICES Q. 273 (2000); ROY ROSENZWEIG, CLIO WIRED: THE FUTURE OF THE PAST IN THE DIGITAL AGE, 8 (2011).
[1256] Solove, Future supra fn 97 at 4.
[1257] Oxford English Dictionary (2014), http://www.oxforddictionaries.com/us/definition/american_english/gossip. Truth is an absolute defence to defamation but not to gossip: the nature of gossip denies the speaker the ability to confirm its truth or falsehood.
[1258] *Id.*
[1259] Daniel Solove, *A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere,* 84 WASH. U. L. REV. 1195, 1198 (2006) (Two Bloggers).

forever in a permanent record."[1260] US First Amendment law is clear that not all speech is deserving of equal protection.[1261] As expresses by the US Supreme Court, as a society we have determined that speech of private concern should merit less protection than speech of public concern.[1262]

One solution to the dual nature of online speech, ie speech that contains references that are more reliable in one space and spontaneous, emotional, graffiti-like speech in the other, is to create a bifurcated online space. As such, one space would foster the perpetuating of good speech and articulate debate while the other would be more of a verbal mosh pit or gossip fest. Both spaces would call for some sort of standard of care, a measurement of responsibility to one's neighbor under privacy law. Using false names and locations, for example, when engaging in either space would have to be agreed upon or eliminated. While the notion of regulation of the spaces would be discouraged as defeating the objective of free expression, creators and users of each space would have to reach consensus on the gradients of speech permitted: hate speech would not be treated in the same way as extortion or blackmail; gossip might be redefined or lower standards of proof required. Any disputes would call on more "nimble remedies" as Solove suggests.[1263] Particularly for digital natives who have experienced the freedoms of online speech without the censures of defamation, a process of accountability could be created, in the vein of ethical review that would generate a spirit of responsible stewardship towards a shared digital environment.

Anonymous defamation is an online behavior that ethical review could effectively address. Blogging that has an anonymous author/publisher or that does not identify the target of a defamatory remark is particularly menacing because it implants cues to guarantee identification of the target by the viewer but escapes judicial review for three main reasons: 1) most bloggers lack deep pockets; 2) actual malice is difficult to prove, and 3) speedy corrections are more easily achieved in blogs than in other

---

[1260] *Id.*

[1261] In fact, the *Fair Credit Reporting Act* was devised to address the unreliable, salacious material that was contained in credit rating agencies without official substantiation.

[1262] *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.* 472 U.S. 749 (1985).

[1263] Solove, Two Bloggers, *supra* fn 1258 at 1199 (noting current laws addressing Internet speech lack "nimble ways to resolve disputes.")

media.[1264] One legal approach is to treat blogging as its own culture and hence deserving of more lenient court treatment.[1265] Dr. Glenn Reynolds recommends litigation but with a higher standard of proof for claimants of anonymous defamatory blogs, taking into account the context and highly idiosyncratic speech they use.[1266] Daniel Solove argues a counter view, that bloggers should have *greater* accountability because, although we tend to think of blogs as "something that enhances the freedom of the little guy", the countervailing freedom from privacy invasion is equally important.[1267] That view is supported by S. Elizabeth Malloy of the University of Cincinnati who cites the permanence of such online postings and the lack of Internet regulation that could be of assistance to the defamed plaintiff.[1268] This chapter argues that a bifurcated space with extra-legal, ethical review could address the vulnerability of defamation victims to anonymously generated content that can undeservedly destroy their carefully maintained reputation.

In the concluding chapter I examine how the introduction of man-machine interoperability in the new Web 3.0 era affects some of those important concerns about reputational privacy.

5.4 Conclusion

Previous chapters have analyzed the most prominent discrepancies between the policies of the EU and US regarding informational privacy. In this chapter we have examined two initiatives that expose those differences in *haut relief*: the EUDR represents a European-led, uniformly enforced, institutional approach to privacy protections that, with the accelerating penetration of the Internet market calls for a meeting of minds and political will in order for the digital economy to thrive. It is

---

[1264] Glenn Harlan Reynolds, *Libel in the Blogosphere: Some Preliminary Thoughts,* 84 WASH. U. L. REV. 1157 (2006).
[1265] *Id.*
[1266] *Id* at 1187.
[1267] Solove, Two Bloggers, *supra* fn 1258, 1195.
[1268] S. Elizabeth Malloy, *Anonymous Bloggers and Defamation: Balancing Interests on the Internet,* 84 WASH. U. L. REV. 1187 (2006) (criticizing the case of *Doe v. Cahill* 884 A. 2d 451 (Del. 2005) for setting too high the requisite proof for disclosure of the name of the defendant blogger: that the claim is brought in good faith; that attribution is materially related to their claim; and that disclosure could not be obtained from any other source.)

crafted as a protectionist and punitive legal mechanism to provide EU residents with higher standards of protection than those of 'adequacy' accepted under the previous US Safe Harbor agreements. EU legislators aim to balance protecting the individual with generating a vibrant digital economy that includes digital access in all its benign uses. The result of such harmonization will be predictably beneficial for one-stop-shopping compliance for industry as well as the development of human rights to access, erasure, and transparency of data handling. Enforcement of such rights has been promoted by the European Commission as swift and effective.

For America, policy aims are more industry driven and constitutionally focused on free speech including economic speech. Data protection and privacy legislative initiatives are sectoral, decentralized, and based on a self regulatory, user notice-and-choice model. Data minimization objectives held by EU regulators do not fit ideologically with commercial tracking practices of US Internet companies that generate and foster behavioural advertising. Recent efforts by the FTC to bring a federal hand to personal data protection have met with considerable industry resistance.

Despite such protectionist steps as the US *Speech Act* to shield journalists from US enforcement of foreign libel judgments, and the finding in the *Google Spain* decision that Internet companies are data controllers with respect to information involving EU citizens, there is considerable interest and effort at higher levels in collaborating on what all western states agree is a privacy crisis. As suggested elsewhere in this dissertation, precedent for EU/US collaboration exists in the Hague Conference on Private International Law, a regime of bilateral consensus on trade, and agreements to share information systems between states to facilitate the digital compatibility of the flow of data, money, and goods. Transnational and international organizations continue to meet and debate the contours of an Internet future, particularly as defined by the pressing Internet governance issue, including the World Summit on Information Society (WSIS+10), Article 29, Transparency International, and the Internet Society. For the most part, participation is voluntary and enforcement potential is sorely lacking.

Several quasi-judicial or extra-legal systems are emerging to deal with data breaches and reputational harms that are escalating at an alarming rate, if takedown requests of Internet companies are any indication. One such judicial-type authority is

the administrative staff of Web and Internet companies like Google and LinkedIn that autonomously devise their takedown standards. Another is the corps of legal experts who craft terms of use contracts between social media providers and subscribers that comprises a mini-system of obligations and liabilities all its own.

Of increasing promise for addressing reputational protections are extra legal activities such as the *ad hoc* assemblage of online communities to lobby for user interests where unilateral actions by companies and institutions threaten reputational privacy. Another emerging practice is that of online review and ranking systems where positive accomplishments or services of individuals can be promoted and false claims can be unearthed. This chapter has also proposed a more formal adjudicatory two-tiered system addressing harms caused by social media language that is stripped of context and body cues to assist interpretation.

In the concluding chapter, I consider those dynamics in light of the web 3.0 era of man-machine co-functioning that is already making our lives easier but culturally, ethically, legally, and socially more complex.

CHAPTER VI CONCLUSION & FUTURE DIRECTIONS

6.0 Summary of Major Findings

This chapter concludes this study and makes recommendations for further research. In this dissertation, I have examined the effectiveness of legal and extra legal responses to breaches of what I call reputational privacy in the current era of new media. This era is comprised of both web 2.0 uses of digital media (marked by human generated communications) and web 3.0 uses (integrating human communications with computers, sensors, and other non-human elements). Both web uses are evolving simultaneously, web 2.0 primarily for interpersonal and informational exchange, and web 3.0 for 'smart' technological functions such as efficient heating of our homes, driverless vehicles, and automatic piloting of aircraft. As I shall discuss in this closing chapter, however, Web 3.0 technology is evolving so quickly that the automation it provides is moving well beyond inter-human communications and further into the inter-functioning of human and computer cognition. That development will call for even more finely tuned legal and extra-legal responses for tomorrow's intellectual and technological academies.

I have organized the inquiry of this dissertation around three research questions: 1) how well do existing legal mechanisms address loss of reputation and informational privacy in the new media environment; 2) can new legal or extra-legal solutions fill any gaps; and 3) how is the role of law pertaining to reputation affected by the man-computer interoperability emerging as the Internet of Things. I will summarize my findings under each title.

1) *how well do existing legal mechanisms address loss of reputation and informational privacy in the new media environment?*

We have seen that there exists a distinct gap between the broad ranging stigma we can suffer to our reputations through posted content and online data leaks and the effectiveness of extant legal responses. One reason is that many of our laws are designed to respond to real world time, geolocations, political boundaries, and physiologically identifiable persons, all the while dealing with intangible property that ignores those constraints. For example, in order to make a property claim for lost reputation, our common law system still requires some element of control over that

property by the claimant. Proof of content or data control is often unsuited to digital behaviour around reputation because it is the societal nature of reputation to reside in the control of others. Our social, financial, and professional worth can be magnified or reduced through our own actions, but its ultimate measure is out of our hands. That situation can be distinguished from copyright law where control over intellectual property *is the critical element of the claim.* As well, law cannot deliver the satisfaction of recovery in the straightforward manner of intellectual property claims: a stained reputation can rarely be exchanged for a sterling one, a fundamental shortcoming that removes much reputational injury from law's purview.

For the persistent litigant in a defamation or breach of privacy suit, challenges also arise with the cross-jurisdictional unevenness of laws, legal definitions and standards of proof. Litigants must choose a system of law and a jurisdiction most historically sympathetic to their case, a need that drives libel tourism. Those additional procedural steps increase the uncertainty of outcome and compound the time, cost, and emotional freight of litigation for the individual.

With new media, we are in unexplored legal terrain where every user can be a generator and publisher of her own content, where publisher or reader or both prefer anonymity that defies attribution, and where the reflexive state response is to tighten local laws regarding access to online content, thereby exacerbating our sense of vulnerability by increasing the sheer quantum of proof we must marshal in our case. Such national laws produce a "balkanization" of the Internet, an insertion of legal and code-architectured firewalls around individual jurisdictions to enable distinct real world societies to deal with Internet exposure as their political ideologies dictate. [1269] As a result, jurisprudence tends to follow national precedent, and be influenced by cultural distinctions, rather than reaching across jurisdictions for collaboration.[1270]

I have noted that a significant number of international legal conventions, like the UNDR and the ICCPR, are rich in their references to reputation rights in the context of family life and privacy. My review of particular cases, sadly, reveals a lack of

---

[1269] The term is used by Marshall W. Van Alstyne & Erik Brynjolfsson, *Global Village or CyberBalkans: Modeling and Measuring the Integration of Electronic Communities,* MGT. SCI. (forthcoming), http://ssrn.com/abstract=756445; *see also* David Kurt Herold, *An Inter*-nation-*al Internet: China's Contribution to global internet governance?* SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1922725.

[1270] Herold, *id.*

reference of those instruments in regional and domestic law (EU) or federal and state law (US). Their influence on local legal norms as revealed in judicial decision making is therefore much diminished.

I also note that judges, primarily in the US, are cautious and sometimes uninformed regarding new media; they often prefer to resolve a case focusing on traditional legal principles that do not consider new conditions of sociality brought about by emerging communications technologies and our interaction with them. I have noted the challenge to judges of learning about the disruptive realities of such technologies and attempting to balance their capabilities with legal principles that evolve incrementally. I observe their preference for technologically neutral language in order to appear consistent with what has gone before and to avoid having to revisit their decisions in the future. I conclude, in terms of judicial practice, that there is a judicial preference for cobbling traditional reasoning onto new media issues without thinking further about how digital technology actually works or whether certain principles of law have any utility or relevance in cyberspace at all.

Such findings are particularly apt for defamation claims. One example is the preference of judges to look for the same elements of proof, to the same standards, when dealing with cryptic, almost fractured, social media speech. Another is applying literary or grammatical standards of interpretation for written correspondence to spontaneous and ephemeral digital messaging. I suggest that digital speech might be a discrete form of communication requiring a unique branch or system of law, or at minimum a separate court staffed with new media experts, such as the Tokyo IP model or the historic equity court based on fairness rather than on black letter law. I further note cases involving defamation being framed in breach of confidentiality, insult or criminal defamation law or other obliquely related causes of action, a practice that further muddles the conceptual and procedural patchwork of legal reasoning regarding individual reputation.

More promising, however, is the emergence of cross-Atlantic interest in new mechanisms to address reputational privacy: a focus in Europe on gatekeeper liability (ISPs primarily) to give individual Internet users control of what gets collected and disseminated online (through the EUDR) and a reworking in the US of the light regulatory approach to user protection through do not track policies. Countering those

initiatives are prominent examples of the nationalization trend, such as the new *Speech Act* in America to protect US journalists and online publishers from the enforcement of foreign judgments in defamation, and the strong data protectionism for EU residents offered by the EUDR. I will follow a description of the *Speech Act* with a discussion of political initiatives that indicate growing international interest in more open but informal collaborations regarding reputational challenges for individuals.

The 2010 *Speech Act* renders unenforceable any foreign defamation judgments against US journalists, unless they are consistent with US laws and procedures, including the US Constitution (including the First Amendment), section 230 of the *Communications Decency Act*,[1271] and US standards of due process.[1272] In other words, foreign judgments must be "consistent with that which a U.S. court would have reached on the facts, if the defamation had been in the United States."[1273] "Defamation" is defined in the Act as "any action or other proceeding for defamation, libel, slander, or similar claim alleging that forms of speech are false, have caused damage to reputation or emotional distress, have presented any person in a false light, ***or*** have resulted in criticism, dishonor, or condemnation of any person."[1274] That definition incorporates traditional torts of privacy, infliction of emotional harm, and defamation. Reference to the *Communications Decency Act* [1275] exempts from legal liability any online intermediaries such as individual users, ISPs, and publishers who post third party content as journalists, ie stories of public interest. In theory the legislation and policy framework exempts from enforcement US citizen publishers who post news stories on YouTube, their own blogs, third party blogs as guest contributors, and even social media sites like Facebook if the general public has access to such sources. The Speech Act does not cover other user generated content.[1276] The *Speech Act* applies to both state and federal

[1271] *Communications Act Of 1934, 47* U.S.C. 230 (as amended and called *Communications Decency Act Of 1996), supra* fn 939 (providing immunity for online web host services regarding content created by other companies.)
[1272] *Securing The Protection Of Our Enduring And Established Constitutional Heritage (Speech) Act,* Part VI, Title 28, (Pub. L. No. 111-223), 124 Stat. 2480 (10 Aug. 2010). (SPEECH Act).
[1273] Emily C. Barbour, *The SPEECH Act: The Federal Response to 'Libel Tourism',* CRS Report For Congress 7-5700 (16 Sept. 2010, https://fas.org/sgp/crs/misc/R41417.pdf
[1274] S. 4101(1) [emphasis added].
[1275] S. 230 states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".
[1276] *Section 230 of the Communications Decency Act,* Electronic Frontier Foundation, https://www.eff.org/issues/cda230.

courts and marks a rigorous policy objective of creating a uniform national response to foreign judgments involving the issue of journalistic free speech.[1277]

Contrasting sharply with the wide berth granted free speech in the *US Speech Act* and *Communications Decency Act* is the *Google Spain* decision. As discussed in earlier chapters, the CJEU decision identified ISPs and Internet content hosts as controllers of content with legal liability and pro-active responsibilities to individual data subjects regarding privacy-sensitive content. The ruling was specific to the Spanish context in which the facts unfolded, although legal principles regarding rights of erasure, for example, are instructive for other Member States. One analyst of the CJEU decision concluded that, "America is rigidly ideological about free speech, while Europe is pragmatic and flexible."[1278] That conclusion might be too categorical for these digital times, as we have seen in the conclusions to Chapters IV and V that the controversy raised by *Google Spain* and its implications for reputational privacy are generating robust debate in both EU Member States and in the US. Those jurisdictions are coming closer to consensus regarding the two initiatives that will change the laws on personal and data privacy as it affects reputation: DNT policies[1279] and the EUDR.[1280]

On the macro stage, there is ongoing dialogue at high levels: the Hague

---

[1277] Barbour, *supra* fn 1273 at 14 (arguing that "Although the SPEECH Act lacks an explicit pre-emption provision, it applies to all "domestic" courts and defines a "domestic court" to include both state and federal courts, notwithstanding any other provision of state law.")

[1278] Eric Posner, *We all have the right to be forgotten,* SLATE (14 May 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html (commenting that the judgment is "hugely more protective of privacy interests than American law, which nearly always prevents people from winning anything from search engines and publishers who have spread personal information about them far and wide.")

[1279] Neelie Kroes, *Why we need a sound Do-Not-Track standard for privacy online,* Europa.eu, (11 Mar. 2014), http://ec.europa.eu/archives/commission_2010-2014/kroes/en/blog/donottrack.html; *see contra,* Richard Beaumont, *Do Not Track Gets Thumbs Down from EU,* The Cookie Collective (12 June 2014), http://www.cookielaw.org/blog/2014/6/12/do-not-track-gets-thumbs-down-from-eu/ (reporting that the Article 29 Working Party with EU Data Protection Authorities could not agree on its European adoption that balanced user control and business interests).

[1280] *See*, for example, *Should the US Adopt the Right to be Forgotten?* Video Debate, Berkman Center For Internet & Society At Harvard University (11 Mar. 2015), http://intelligencesquaredus.org/debates/past-debates/item/1252-the-u-s-should-adopt-the-right-to-be-forgotten-online (featuring Paul Nemitz and Eric Posner arguing for adoption and Jonathan Zittrain and Andrew McLaughlin arguing against. The latter team won the debate.)

Conference on the role of private international law in cross border data flows;[1281] the *UN Resolution on a Global Agenda for Dialogue among Civilizations*;[1282] the *Declaration Of Principles By The World Summit On The Information Society (WSIS)*;[1283] as well as the creation of privacy principles by the Asia-Pacific Economic Cooperation organization (APEC).[1284]

Despite the lack of enforcement bite of international legal conventions, there has been a show of faith in the worth of the individual through broader recognition of a human right to Internet access. For example, the parliament of Estonia passed legislation in 2000 declaring Internet access a basic human right;[1285] the Constitutional Council of France effectively declared Internet access a fundamental right in 2009;[1286] the constitution of Greece acknowledges the duty of the state to facilitate digitally transmitted information;[1287] Finland's Ministry of Communications and Transportation passed a decree in 2009 setting minimum standards of user access;[1288] the special rapporteur to the UN, Frank Le Rue, designated Internet access a human right in

[1281] *Cross-border Data Flows and Protection of Privacy,* Report, Hague Conference On Private International Law (March 2010), http://www.hcch.net/upload/wop/genaff2010pd13e.pdf.
[1282] Global Agenda For Dialogue Among Civilizations, G.A. Res. 56-6, U.N.Doc. A/56/L.3 and Add/ 1, Nov. 21, 2001, Article 9: "Utilization of communication technologies, including audio, video, printed press, multimedia and the *Internet, to disseminate the message of dialogue and understanding throughout the globe* and depict and publicize historical instances of constructive interaction among different civilizations". [emphasis added]
[1283] Declaration Of Principles By The World Summit On The Information Society, WSIS-03/GENEVA/DOC/4-E (Paris: UNESCO & Geneva ITU (Dec. 12, 2003) (to build "a people-centered, inclusive, and development-oriented Information Society").
[1284] APEC Privacy Framework, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx .
[1285] Colin Woodward, *Estonia, where being wired is a human right*, CHRISTIAN SCI. MON., (1 July 2003) http://www.csmonitor.com/2003/0701/p07s01-woeu.html .
[1286] Ian Sparks, *Internet access is a fundamental human right, rules French court*, DAILY MAIL (12 June 2009) http://www.dailymail.co.uk/news/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html.
[1287] Hellenic Viii Revisionary Parliament, Constitution Of Greece, Article 5A, as revised by parliamentary resolution (27 May 2008), http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156aggliko.pdf.
[1288] Decree Of The Ministry Of Transport And Communications On The Minimum Rate Of A Functional Internet Access As A Universal Service," FINLEX, 732/2009, (22 Oct. 2009), http://www.finlex.fi/en/laki/kaannokset/2009/en20090732 (emphasizing that "Every Internet connection within the country must have a broadband speed of at least one megabit per second, increasing to a speed of 100 megabits per second by 2015").

2011;[1289] and a survey by the British Broadcasting Corporation (BBC) in March 2010 determined that almost 80% of participants from 26 countries believe that Internet access is an inherent fundamental human right.[1290] In a separate calculation, 85% of BBC participants who do not have Internet access believe it *should* be a protected human right.[1291] Each of those activities could lead to lobbying at high levels for more dedication of resources to the digital divide problem.[1292]

In his 2011 report to the UN Council on Human Rights, Frank La Rue identified the Internet as an enabler of other human rights because it "vastly expands the capacity of individuals to enjoy their right to freedom of opinion and expression", and it boosts economic, social and political development, "thereby contributing to the progress of humankind as a whole".[1293] One of those "other human rights", the right to communicate, was promoted by former UN Secretary-General Kofi Anan in his message on World Telecommunication Day:[1294] he reminded the international community of the millions of people in the poorest countries who are still victimized by the digital divide.[1295]

The above illustrations support our ideological intention, as an international community, to promote our human entitlement to reputational protection through our

---

[1289] Frank La Rue, *Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression*, UN Council on Human Rights, 17th Sess. agenda item 3, 28-59, UN Doc./A/HRC/17/27 (2011) 28-59, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. *See also* Nicolas Jackson, *United Nations Declares Internet Access a Basic Human Right*, ATLANTIC (3 June, 2011), http://www.theatlantic.com/technology/archive/2011/06/united-nations-declares-internet-access-a-basic-human-right/239911/.

[1290] *Four in five regard Internet access as a fundamental right: global poll,* BBC NEWS (8 Mar 2010), http://www.bbc.co.uk/pressoffice/pressreleases/stories/2010/03_march/07/poll.shtml (explaining there were 27,973 adult participants including 14,306 Internet users, ethnology included face-to-face or telephone interviews between 30 November 2009 and 7 February 2010 or urban samples, and polling was conducted for BBC World Service by GlobeScan.)

[1291] *Id.*

[1292] 'Digital divide' can be defined as 'inequality of access to the Internet'. Manuel Castells, The Internet Galaxy 248 (2001).

[1293] La Rue, *supra* fn 1289 at para 67.

[1294] 17 May 2003.

[1295] Bruce Girard, Sean O Siochru, *Communicating in the Information Society,* Paper for Information Technologies and Social Development Project, United Nations Research Institute for Social Development (Nov. 2003), http://www.unrisd.org/80256B3C005BCCF9/(httpAuxPages)/B6020CCE9EBC00FCC1256E550059CB34?OpenDocument.

our Internet access. In practice, however, more violent or physically damaging acts against human rights garner the headlines and the attention of those who apply the UNDR and the ICCPR. Although technological innovation promises democratic participation in the digital economy through education and healthcare, this dissertation has identified several factors that create a risk of exclusion from those conversations: state censorship;[1296] realistic fears of cyber-terrorism and digital attacks; and the perceived tyranny of aggressive surveillance techniques by the state in the name of national security. Each of those risks soundly affects the participation of the individual in life online.

2) C*an new legal or extra-legal solutions fill any gaps?*

In response to this research question, I have provided several tenable possibilities such as emerging legal initiatives or less formal responses altogether. I have reviewed the proposed EUDR that will require all exporters of personal data of EU citizens to comply with stringent guidelines regarding the cross-border use of individual personal data. That regime calls for closer collaboration between US Internet companies and EU data authorities.

I have compared the EUDR regime with the US policy agenda for do not track mechanisms that could become law for all Internet content carriers. At present, DNT initiatives work on a notice-and-choice basis that requires the active decision making of individual users. American regulatory agenda, steer-headed by the FTC, would see all US-based Internet companies embed DNT mechanisms into its designs, thereby taking the initiative for non tracking policies off the shoulders of individual users by creating a federal regime. The active interest of the European Commission and Article 29 Working Party of data retention authorities suggests trans-Atlantic collaboration over DNT policies is possible.

I have also proposed several extra-legal responses to protect reputational privacy. Those suggestions include creating 1) project-specific monitoring communities,

[1296] *See further* Aendrew Rininsland, *Internet censorship listed: how does each country compare?* GUARDIAN (16 Apr 2012) http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list (indicating which national governments are involved in filtering and the different levels of formal activity).

such as Facebook subscribers, to address intrusive practices of industry; 2) reputational rating and review systems that build individual and institutional reputations and informally weed out harms by unfounded attacks on reputation;[1297] 3) educational programs for new media users regarding online citizenship, beginning with pro-active self-regulation;[1298] and 5) an inter-disciplinary mechanism for the ongoing study of the epistemological nature of digital speech to more accurately distinguish risk causing verbal behavior from mere socially offensive conduct.

I propose that legal and extra-legal solutions are not mutually exclusive but collaborative; some of the latter already exist as suffers of reputational stigma take re-building into their own hands. There is a need for more individual awareness of the Internet industry's own system of reputational privacy law: its Terms of Use provisions. I suggest a formalized study of those terms might reveal a layer of legality for individual Internet use that provides additional issues regarding reputational control or that suggests areas of consensus. Similarly, access to the criteria for successful take down requests devised by Internet companies like Google could assist in arriving at a list of 'fair practices' for removing harmful content. In that way, industry need not always be an adversary in our quest for reputational integrity.

3) *How is the role of law pertaining to reputation affected by the man-computer interoperability emerging as the Internet of Things?*

This dissertation has shown how not all reputational effects relate to the privacy of our home and family life. Much exposure of the identifying data we leave behind during our online activities renders us vulnerable to its collection, retention, sale, and analysis by authorities or commercial entities without our consent or even knowledge. Those activities are included in this dissertation because, as I have illustrated, their manipulation robs us of the control over our reputations that we need in order to maintain the high esteem of our society.

The theme of user control gains complexity with our entry into the age of human-computer integration, what we increasingly refer to as the Internet of Things. or the connection through the Internet of devices or sensors that are sold to consumers

[1297] As first proposed by Ardia *supra* fn 10 at 321.
[1298] *See further* Gillespie, *supra* fn 1222.

to communicate information between them.[1299] When computers are connected to sensors and activators in order to assist human comfort, security, health, mobility or access to information, data and images are produced that threaten to expose our reputations and self-presentation in a host of new ways. Such augmentation of our human capabilities poses questions regarding the role of law that we have only begun to ponder. Future research, therefore, is needed to extend beyond this exploratory study and develop recommendations for dealing with those increasing risks to reputation, as accelerated by our entry into the era of the Internet of Things. [1300]

[1299] *See further* Tim O'Reilly, *IoTH: The Internet of Things and Humans,* Oreilly.Com YouTube video, http://radar.oreilly.com/2014/04/ioth-the-internet-of-things-and-humans.html (suggesting the more inclusive descriptor 'human-computer' to replace more historical references to 'man-computer'.)

[1300] *See further Internet Of Things: Privacy And Security In A Connected World,* FTC (Jan. 2015), https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world; *and also The Internet of Things is transforming everything from Formula One to driverless cars,* Internet Of Things Council, http://business.financialpost.com/2015/03/11/how-the-internet-of-things-is-transforming-everything-from-formula-one-to-driverless-cars/.

6.1 Future Research

One place to start is to develop research threads introduced in this paper, such as the construction of a methodology for measuring and comparing reputational harm. While this dissertation has illustrated the intangible aspects of such injury, it has also shown how those harms can be translated into loss of opportunity in the economic, social, and professional sense. Those opportunities enable our contributions to the society we entrust with our reputations. Unlike in Brandeis and Warren's time, we now recognize intangible harms in many areas of law. By devising a gradient of expressible harms, for example, we could work towards recommendations for law reform that would deliver more effective legal responses to personal reputational injury. Once harm can be systematically measured, we can begin to assess the adequacy of our existing responses through laws of defamation, privacy invasion, and data retention. Another fertile area of research includes deconstructing digital speech to test this paper's proposal for a bifurcated space of legal and non-legal responses to communications that result in online reputational damage. Further development of the quasi-adjudicative function of Google personnel regarding take-down requests is warranted as well in light of mounting pressure by US and EU authorities to formalize such processes. All of those topics hold promise for more clearly defining the control of the individual over personal reputation as we move into the human-machine interconnectedness of the Web 3.0 era.

Bibliography

1 Legislation

A Constitutions

United States:

United States Constitution (4 March 1789) as amended.

Cal. Const. Art. I, § 1.

Conn. Gen. Statute §54-142a

Mont. Const. Art. 2 § 10.

European Union:

Constitution of Greece, Hellenic VIII Revisionary Parliament, rev'd (27 May 2008).

B International Treaties & Conventions

American Convention On Human Rights, Organization of American States [OAS], American Convention on Human Rights, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123 (22 Nov. 1969).

American Declaration Of The Rights And Duties Of Man, Inter-American Commission On Human Rights, Basic Documents Pertaining To Human Rights In The Inter-American System, (2 May 1948) OEA/ser. L/V/II.82, Doc. 6 Rev. 1 (1992) (IACHR).

Convention ETS 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, (28 Jan. 1981).

Convention For The Protection Of Human Rights And Fundamental Freedoms, 213 U.N.T.S. 221, E.T.S. 5 (3 Sept. 1953), as amended by Protocols 3, 5, 8, and 11 (entered into force 21 Sept. 1970; 20 Dec. 1971; 1 Jan 1990, and 1 Oct. 1994) (ECHR).

Convention On The Rights Of The Child, 1577 U.N.T.S. 3 (20 Nov. 1989).

Convention On The Rights Of Persons With Disabilities, 2515 U.N.T.S. 3 (13 Dec. 2006).

Global Agenda For Dialogue Among Civilizations, G.A. Res. 56-6, U.N.Doc. A/56/L.3 and Add/ 1 (21 Nov. 2001).

International Convention On The Protection Of The Rights Of All Migrant Workers And Members Of Their Families, G.A. Res. 45-158, U.N.P.M. 69 (18 Dec. 1990).

International Covenant On Civil And Political Rights, S. Exec. Rep. 102-23, 999 U.N.T.S. 171 (16 Dec. 1966) (ICCPR).

Protocol 14 to the Convention For The Protection Of Human Rights And Fundamental Freedoms, amending Convention CETS No. 194 CE/ (1 June 2010).

UN, Declaration Of Principles By The World Summit On The Information Society, WSIS-03/GENEVA/DOC/4-E, Paris: UNESCO & Geneva ITU (12 Dec. 2003).

UN Universal Declaration Of Human Rights, UNGA Res 217 A Iii (10 Dec. 1948) (UDHR).

C Statutes

United States: Federal

Cable Communications Policy Act of 1984, 66 U.S.C. Title 47 (Pub. L. No. 98-549), 98 Stat. 1984 (26 January 1983).

Cable Television Protection and Competition Act, 102 Stat. § 1992 (Pub. L. No. 102-385) (1 May 1991).

Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (Pub. L. No. 105-277), 112 Stat. 2681-728 (21 October 21 1998).

Communications Decency Act of 1996, 47 U.S.C. § 230 (Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996).

Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1001 (Pub. L. No. 99-474, 100 Stat. 1213 (16 Oct. 1986), am. 18 U.S.C. §1030.

Digital Millennium Copyright Act, 17 U.S.C. § 512 (Pub. L. 105-304) 112 Stat. 2860 (28 Oct. 1998).

Economic Espionage Act of 1996, 18 U.S.C. 1831 (economic espionage), 1832 (theft of trade secrets) (Pub. L. 113-234) 114 Stat. 3488, (11 Oct. 1996).

Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2701 et seq. (Pub. L. 95-108) 100 Stat. 1848 [21 Oct. 1986).

Fair Credit Reporting Act, 1970, 15 U.S.C. 1681 (Pub. L. No. 91-508), §601, 84 Stat. 1128, codified as amended, 15 U.S.C. §1681-1681x (26 Oct. 1970).

Financial Modernization Act of 1999, 106 U.S.C. (Pub. L. No. 106-102) 113 Stat. 1338 (12 Nov. 1999) (Gramm-Leach-Bliley Act)

Health Insurance Portability and Accountability Act, 42 U.S.C. §§300 & 29 U.S.C. §§1181 *et seq (*Pub. L. No. 104-191), 110 Stat. 1936 (1996).

Privacy Act of 1974, 5 U.S.C. §552a (Publ. L. No. 93-579), 88 Stat. 1896 (31 Dec. 1974).

Sarbanes-Oxley Act of 2002, 18 U.S.C. (Pub. L. No. 107-204), 116 Stat 745 (30 July 2002) (An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes).

Securing the Protection of our Enduring and Established Constitutional Heritage Act, Part VI, Title 28, (Pub. L. No. 111-223), 124 Stat. 2480 (10 Aug. 2010) (SPEECH ACT).

United States: State

The California Online Privacy Protection Act, 370 A.B. (CalOPPA) as amended 27 Sept 2013.

California Student Online Personal Information Protection Act – SB 1177 (effective 1 Jan 2016).

International: European Union

European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02.

Treaty on the Functioning of the European Union (TFEU) C 83/49 1 December 2009, renamed, consolidated and amended by the Treaty of Lisbon (OJ C 326, 26 Oct. 2012).

Directive 06/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention Of Data Generated Or Processed In Connection With The Provision Of Publicly Available Electronic Communications Services Or Of Public Communications Networks and amending Directive 2002/58/EC (Doc. 32006L0024).

Directive 02/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector (Document 32002L0058).

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a Procedure For The Provision Of Information in the Field of Technical Standards and Regulations (Doc. 31998L0034).

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection Of Consumers In Respect Of Distance Contracts, Statement by the Council and the Parliament re Article 6 (1) - Statement by the Commission re Article 3 (1), first indent (Doc. 31997L0007).

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection Of Databases (Doc. 31996L0009).

Directive 00/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, In Particular Electronic Commerce, in the Internal Market (Doc. 32000L0031) (e-commerce directive).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection Of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data Access To, And Interconnection Of, Electronic Communications Networks, Domain Name Regulation (Doc. 31995L0046).

Proposal For A Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation) 2012/0011 (COD) (1 January 2013).

Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the Law Applicable To Non-Contractual Obligations [Rome II].

Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the Implementation Of The EU Top Level Domain (Text with EEA relevance) (Doc. 32002R-733).

Regulation (EC) No 44/2001 of the European Parliament and of the Council of 22 December 2000 on Jurisdiction And The Recognition And Enforcement Of Judgments In Civil And Commercial Matters (Brussels I).

Uniform Benelux Law on Marks (amended by the Protocol of November 10, 1983, amending the Uniform Benelux Law on Trademarks and by the Protocol of December 2, 1992, amending the Uniform Benelux Law on Marks).

Domestic: EU Member States

Bulgaria

Code Penal (C. Pen.) art. 146 and 147, art. R.645-1.

Finland

Code Penal (C. Pen.) 39/1889 as amended, ch 24(9).

Decree Of The Ministry Of Transport And Communications (Finland) On The Minimum Rate Of A Functional Internet Access As A Universal Service, of 22 October 2009, FINLEX.

France

Code Penal de France, Art. R.645-1.

Press Freedom Act of 29 July 1881 (Loi Du 29 Juillet 1881 Sur La Liberté De La Presse).

Law On Information Technology, Data Files And Civil Liberties of 6 January 1978 (Loi Informatique Et Libertes), Act N°78-17, as amended.

Germany

The Hesse Data Protection Act 1970 (Hessisches Datenschutzgesetz) , Gesetz und Verordungsblatt I (1970), 625 (Hesse, Ger.).

German Federal Data Protection Act of 1977 (BDSG), Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bun- desdatenschutzgesetz - BDSG) of 27 January 1977, BUNDESGESETZBLATT [BGBI] 1 201 (Ger.).

Sweden

Swedish Data Act 1973 (*Datalagen* [1973] Svensk For-Fattningssamling, 11 May 1973, 289) (Swe).

Switzerland

Swiss Federal Act on Data Protection (FADP; SR 235.1) (19 June 1992) (Status as of 1 January 2014), *Fed. Ass. Swiss Conf.*, based on Articles 95, 122 and 173 paragraph 2 of the Federal Constitution.

United Kingdom

UK Defamation Act 2013 (England And Wales) No. 3027 (C. 125).

UK Human Rights Act 1998, c. 42.

d Jurisprudence

United States:

American Broadcasting Companies, Inc. [ABC] et al., Petitioners v. Aereo, Incl, f.k.a. Bamboom Labs, Inc., 712 F. 3d 676 (2014).

Anderson Columbia Co., Inc. v. Gannett Co., Inc., No. 2001 CA 001728, 1st Cir. Fla, filed Aug. 28, 2001; ot'd by the Fla S. Ct in No.sc06-2174 (Oct. 23, 2008).

Apex Tech. Grp. Inc. v Doe, No. MID-L-7878-09 (N.J. Sup. Ct. Law Div. Dec. 23, 2009).

Bland v. Roberts, 857 F. Supp. 2d 599 (E.D. Va. 2012), rev'd in part, 730 F.3d 368(4th Cir. 2013).

Blumenthal v Drudge and America On-Line Inc., 992 F. Supp. 44 (D.D.C. 1998).

Calder v. Jones 465 U.S. 783 (1984).

Citizens United v. Federal Election Commission 558 U.S. 310, 352 (2010).

City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

Cochran v. Tory, (No. BC239405, 2002 WL 33966354 (Cal. Sup. Ct. Apr. 24, 2002), vacated 544 U.S. 734 (2005).

Cooper v. Greeley, 1 Denio 347, 358 (N.Y.Sup.Ct.1845)

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Doninger v. Niehoff (2d Cir. Apr. 25, 2011).

Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 784 (1985)

eDate Advertising v X and *Olivier Martinez & Robert Martinez v MGN Limited*, [2011] EUCJEU C-509/09 & C-161/10, [2012] QB 654.

EF Cultural Travel v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

Re Google Inc. Gmail Litigation, Case No. 13-md-02430, U.S. Dist. Ct., N. Dist. CA (San Jose 2014).

Gertz v. Robert Welch, Inc., 418 U.S. 323, 350 (1974).

Google Inc v. Joffe et al, 9th U.S. Cir. C.A. No. 11-17483 (Sept. 10, 2013).

Re Google Inc. Street View Electronic Communication Litigation, U.S. Dist. Ct. for the N. Dist. CA, F.Supp.2d 1067, (2011).

Gordon & Holmes et al. v. Love, Motion for Summary Judgment BC462438, Sup. Ct Cal. (Dec. 29, 2013)

Griswold v Connecticut, 381 U.S. 479 (1975).

J.S. ex rel. Snyder v. Blue Mountain Sch. Dist. No. 3:07-cv-585, 2007 WL 954245 (M.D. Pa. Mar. 29, 2007)

Kowalski v. Berkeley County Sch., No. 1098 (4th Cir. 2011).

Lawrence v Texas, 539 U.S. 558 (2003).

Layshock v. Hermitage Sch. Dist., No. 07-4465 (3d Cir. Jun. 13, 2011).

Lorraine Martin v. Hearst Corp. et al., Dist. Conn. No. 3:12-cv-01023-MPS, doc 58, U.S. Dist. Ct, Dist. Conn. (2013).

Lorraine Martin v. Hearst Corporation Case 13-3315, filed 17 March 2014, US Ct App.2nd Circ.

New York Times Co. v Sullivan, 376 U.S. (1964).
Obsidian Financial Group., LLC v. Cox, 812 F. Supp. 2d 1220, 1232–34 (D. Or. 2011)

Obsidian Finance Group v Cox, Case §12-35238, C.A. 9th Cir. Dist. Ct Ore. (Nov. 6, 2013).

Paul v Davis, 424 U.S. 693, 96 S. Ct. 1155, 47 L. Ed. 2d 405, (1976)

Olmstead v. United States, 277 U.S. 438, 478 (1927).

Perkins v. LinkedIn Corp., Case No. 13-cv-04303, U.S. Dist. Ct., N. Dist. Ca (San Jose).

Reno v. ACLU, 521 U.S. 844 (1997).

Reynolds v. Times Newspapers Ltd [2001] 2 A.C. 127 (HL).

Roe v Wade, 410 U.S. 113 (1973).

Rose v. Hollinger International, Inc., 882 N.E.2d 596 (Ill. 2008).

Rosenblatt v. Baer, 383 U.S. 75 (1966).

Search King, Inc. v. Google Technology, Inc. No. CIV-02-1457-M, 2003 WL 21464568, at§4 (W.D. Okla. May 27, 2003).

Seelig v Infinity Broadcasting, 97 Cal. App. 4th 798 (Cal. Ct. App. 2002).

Shea on Behalf of American Reporter v. Reno, 930 F. Supp. 915, 925-26 (S.D.N.Y. 1996).

Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995).

Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969).

United States v. Anthony Douglas Elonis, Case No. 12-3798 (US App. Ct. 3rd Cir. 2013).

United States v. Google Buzz (FTC File 102 3136)

United States v. Snapchat (FTC file 132 3078).

United States v. Google Inc. (No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012).

Vicki Van Valin v. Google Inc. Class action complaint 18 U.S.C. §2511 et seq.

Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisdmitisme (LICRA), Plaintiff's Application for Declaratory Relief, 169 F. Supp. 2d. 1181(N.D. Cal. 2001).

Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168, 1171 (N.D. Cal. 2001).

Youssoupoff v Metro Goldwyn-Mayer Pictures Limited [1934] 50 TLR 581, CA.

Zippo Manufacturing Co. v. Zippo Dot Com Inc. 952 F. Supp. 1119 (W.D. Pa. 1997).

European Union Member States

Belgium
De Haes and Gijsels v. Belgium, 25 Eur. H.R. Rep. 1 (1997).

England
Case de Libellis Famosis, 77 Eng. Rep. 250 (1606).

Cooper v. Greeley, 1 Denio 347, 358 (N.Y.Sup.Ct.1845)

Gee v. Pritchard 36 ER 670 (Chancery Ct 1818)

Max Mosley v. News Group Newspapers Limited, [2008] EWHC 1777 (QB).

McCormick v England, 494 S.E. 2nd 431. (S.C.Ct.App. 1997)

McKennitt v Ash, QB 73 [2008].

Parmiter v Coupland [1840] 6 M&W 105.

Sim v. Stretch [1936] 2 All ER 1237, HL.

Smith v. Advfn PLC, All E.R.(D) 335 (Q.B.D.).

Estonia
Delfi AS v. Estonia, no. 64569/09, §§ 7, 94, EUR. CT. H.R. (October 10, 2013).

France
Dailymotion / Nord-Ouest production et autres, Cour d'appel de Paris 4ème chambre, section A (6 May 2009).

Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (May 22, 2000 and November 22, 2000) No RG:00/0538 [LICRA v. Yahoo!]

L'Union Des Etudiants Juifs De France (UEJF) & La Ligue Contre Le Racisme et L'Antisemitisme [LICRA I] Inc. & Yahoo! France, T.G.I. Paris, May 22, 2000.

Oliver Martinez & Robert Martinez v MGN Limited (25 October 2011) Tribunal de grande instance de Paris, France.

Max Mosley v Google Inc. and Google France, TGI Paris, Court of First Instance, RG# 11/07970 (6 Nov. 2013).

Jean Yves L. dit Lafesse / Myspace, TGI Paris Ordonnance de référé (22 June 2007).

Germany

FDPIC v. Google Inc., BGE 138 II 346 (31 May 2012).

OLG Koblenz Urteil vom 20. Mai 2014 – 3 U 1288/13.

EDate Advertising GmbH v X (25 October 2011) Bundesgerichtshof, Germany.

Italy

Padova Maria Luisa v Google Inc. (10847/2011) Tribunale Ordinario de Milano (Mar. 31, 2011).

Netherlands

Arthur van M., C/13/569654 / KG ZA 14-960 (19 Sept. 2014) (Amsterdam).

Switzerland

Google Inc. und Google Switzerland, BGE 138 II 346 E. 6. [*FDPIC v. Google Inc.*, BGE 138 II 346 (31 May 2012)]

International Jurisprudence

Bier BV v Mines de Potasse d'Alsace, Case 21/76, CJEU [1976]; ECR 1735 (1976).

Chauvy and others v. France (2005) 41 EHRR 29 (ECtHR).

Digital Rights Ireland Ltd. v Ireland & Karntner Landesregierng & others (Joined Cases C-293/12 and C-594/12) CJEU (April 8, 2014) seeking preliminary ruling on ePrivacy Directive (OJ 2006 L 105, p. 54).

eDate Advertising v X and *Olivier Martinez & Robert Martinez v MGN Limited*, [2011] C-509/09 & C-161/10 CJEU, [2012] QB 654.

Google Spain v Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, CJEU (13 May 2014).

Handyside v. United Kingdom, 1 EHRR (Ser. A) 737 (1979).

Lingens v. Austria 8 EHRR 407 (ECtHR) (1986).

Pfeifer v. Austria (2007) 48 EHRR 175 (ECtHR).

Polanco Torres and Movilla Polanco v. Spain, [ECtHR] 34147/06, [2010] 1341.

Scarlet Extended SA v. SABAM (Societe belge des auteurs, compositeurs et editeurs, C-70/10 CJEU (24 Nov. 2011).

Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA, C-68/93 CJEU [1995]; ECR I-415 9 (26 July 1996).

Other Jurisdictions

Guillot v Istek Corp. [2001] F.C.J. No. 1165

Grant v. Torstar Corp. 2009 SCC 61, [2009] 3 SCR 640.

Murphy v. LaMarsh (1970), 73 W.W.R. 114 (BCCA).

Vaquero Energy Ltd. v. Weir, 2004 ABQB 68, 352 A.R. 191.

e Legislative History

California Senate Bill 761 (14 March 2011), <http://info.sen.ca.gov/pub/11-12/bill/sen/sb_0751.

Consumer Privacy Protection Act Of 2011, (14 Mar. 2014), http://www.gpo.gov/fdsys/pkg/BILLS-112hr1528ih.pdf.

Do Not Track Online Act Of 2011 (14 March 2014), http://commerce.senate.gov/public/?a=Files.Serve&File_id=85b45cce-63b3-4241-99f1-Obc57c5c1cff.

Do Not Track Kids Act Of 2011, (14 March 2014), http://online.wsj.com/public/resources/documents/billdreaft050.

A New Commercial Privacy Bill Of Rights, (14 March 2014), http://www.kerry.senate.gov/imo/media/doc/Commercial%20.

Proposal For A Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation) 2012/0011 (COD) (1 January 2013).

Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Federal Trade Commission, (December 2010), http://www.ftc.gov/opa/2010/12/privacyreport/shtm.

f Administrative And Executive Materials

Issuance Of Safe Harbor Principles And Transmission To European Commission, 65 Fed. Reg. 45, 666 (24 July 2000).

In re FTC and Myspace, Federal Trade Commission, file 1023058.

In re FTC and Snapchat Inc., Federal Trade Commission, file 140508.

Jurisdiction And The Recognition And Enforcement Of Judgments In Civil And Commercial Matters, Brussels I Regulation, 2001/44/EC, (22 December 2000).

Regulation 2007/864/EC *On The Law Applicable To Non-Contractual Obligations*, Article 1(2)(g), (11 July 2007) [Rome II]

Regulation 2006/2004/EC on Cooperation Between National Authorities Responsible For The Enforcement Of Consumer Protection Laws [2009] OJ L337.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 1/99 concerning the level of Data Protection in the United States and the Ongoing Discussion between the European Commission and the United States Government, DG MARKT DOC 5098, WP 15 (26 Jan 1999).

g Books, Book Chapters & Monographs

ALAN BADDELEY, MICHAEL W. EYSENCK, & MICHAEL C. ANDERSON, MEMORY (2009).

FREDERICK BARTLETT, REMEMBERING: A STUDY IN EXPERIMENTAL SOCIAL PSYCHOLOGY (1932).

JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS (2006).

YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFERS MARKETS AND FREEDOM (2006).

Dana Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics*, in YOUTH, IDENTITY AND DIGITAL MEDIA, MACARTHUR FOUNDATION SERIES ON DIGITAL LEARNING – YOUTH, IDENTITY, AND DIGITAL MEDIA (2007).

ADRIAN BRIGGS, THE CONFLICT OF LAWS (3rd) (2013).

MANUEL CASTELLS, THE INFORMATION AGE: ECONOMY, SOCIETY AND CULTURE: THE POWER OF IDENTITY, vol. 2 (1997).

MANUEL CASTELLS, THE INTERNET GALAXY (2001).

THE CHAMBERS DICTIONARY (12th) 2011

JIE CHEN, POPULAR POLITICAL SUPPORT IN URBAN CHINA (2004).

THOMAS COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT (1879) as cited by Louis Brandeis and Samuel Warren, *The Right to Private Property*, 4 HARV. L. REV. 193.

Lillian Edwards, *Privacy, Law, Code and Social Networking Sites*, in RESEARCH HANDBOOK ON GOVERNANCE OF THE INTERNET (Ian Brown, ed., 2013).

RACHEL EHRENFELD, FUNDING EVIL (2003).

AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

MARTHA FINNEMORE, NATIONAL INTERESTS IN INTERNATIONAL SOCIETY (1996).

DAVID FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND (1967).

David Flaherty *Controlling Surveillance: Can Privacy Protection be made Effective*? in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (P.E. Agre & M. Rotenberg, eds, 1998).

RICHARD WIGHTMAN FOX, TRIALS OF INTIMACY: LOVE AND LOSS IN THE BEECHER-TILTON SCANDAL (1999).

LAWRENCE FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY (2007).

LAWRENCE FRIEDMAN, THE HORIZONTAL SOCIETY (1999).

ERVING GOFFMAN, INTERACTION RITUAL: ESSAYS ON FACE-TO-FACE BEHAVIOR (1982).

ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

ERVING GOFFMAN, STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY (1990).

Eric Goldman, *The Regulation of Reputational Information*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET, 293 (Berin Szoka & Adam Marcus eds, 2010).

MAURICE HALBWACH, ON COLLECTIVE MEMORY, (L.A. Coser ed. and trans. 1992).

JOEL HAWES, ADDRESS TO THE YOUNG MEN OF HARTFORD AND NEW HAVEN, Lecture 4, *Formation And Importance Of Character* 91 as reproduced by Princeton University Library (1828).

Martijn Hesselink, *The Ideal of Codification and the Dynamics of Europeanisation: The Dutch Experience*, in THE HARMONIZATION OF EUROPEAN CONTRACT LAW IMPLICATIONS FOR EUROPEAN PRIVATE LAWS, BUSINESS AND LEGAL PRACTICE (Stefan Vogenauer & Stephen Weatherill eds, 2006).

SAMUEL H. HOFSTADTER, THE DEVELOPMENT OF THE RIGHT OF PRIVACY IN NEW YORK (1954).

T.E. HILL & A. ZWEIG, GROUNDWORK FOR THE METAPHYSICS OF MORALS, (A. Zweig trans. 2011).

MICHAEL IAPOCE, A FUNNY THING HAPPENED ON THE WAY TO THE BOARDROOM: USING HUMOR IN BUSINESS SPEAKING, 129 (1988).

HENRY JENKINS, CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE (2006).

IMMANUEL KANT, THE GROUNDWORK OF THE METAPHYSIC OF MORALS, (Grundlegung Zur Metaphysik Der Sitten, 1785) as reproduced and edited by Thomas E. Hill, *et al.*, trans. by Arnulf Sweig (2002).

W. PAGE KEETON et al., PROSSER AND KEETON ON THE LAW OF TORTS (5th) (1984).

LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.O (2000).

GARY MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (1988).

Gary Marx, *The Iron Fist and the Velvet Glove: Totalitarian potential within democratic structures*, in THE SOCIAL FABRIC: DIMENSIONS AND ISSUES, 135-161 (J.F. Short, ed 1986).

VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

VIKTOR MAYER-SCHÖNBERGER AND KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

BONNIE S. MCDOUGALL AND ANDERS HANSSON, EDS. CHINESE CONCEPTS OF PRIVACY (2002).

MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN (1994).

LAWRENCE MCNAMARA, REPUTATION AND DEFAMATION (2007).

GEORGE HERBERT MEAD, MIND, SELF AND SOCIETY (1934)

HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRATION OF SOCIAL LIFE (2009).

THOMAS PAINE, THE POLITICAL WRITINGS OF THOMAS PAINE, vol. 1 (available online from General Books LLC, 1870).

JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).

EDWARD PARSONS DAY, DAY'S COLLACON: AN ENCYCLOPEDIA OF PROSE QUOTATIONS, (1884) as reproduced by Digital Commons, http://digitalcommons.butler.edu/cgi/viewcontent.cgi?article=2009&context=wordways

RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF EMERGENCY (2006).

WILLIAM PROSSER, SECOND RESTATEMENT OF THE LAW OF TORTS (4th 1971).

Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, in CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE, 3 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

ROY ROSENZWEIG, CLIO WIRED: THE FUTURE OF THE PAST IN THE DIGITAL AGE, 8 (2011).

JOHNNY RYAN, A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE (2010).

AUSTIN SARAT, et al., IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY (2012).

ANDREJ SAVIN, EU INTERNET LAW (2013).

WILLIAM SHAKESPEARE, OTHELLO: THE MOOR OF VENICE (as reprinted in The Oxford Shakespeare, Stanley Wells ed., 2008).

ROBERT ELLIS SMITH, BEN FRANKLIN'S WEBSITE: PRIVACY AND CURIOSITY FROM COLONIAL AMERICA TO THE INTERNET (2000).

DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR AND PRIVACY ON THE INTERNET (2007).

DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

Malcolm Thorburn, *Identification, Surveillance, and Profiling: On the Use and Abuse of Citizen Data'*, in PREEMPTING CRIMINAL HARMS (Dennis, Sullivan ed., 2012).

VIRGIL, AENEID, Book VI at para 703, (as trans. by H.R. Fairclough 1916), http://www.theoi.com/Text/VirgilAeneid6.html.

Xhengxu Wang, *Political Trust in China: Forms and Causes*, in LEGITIMACY: AMBIGUITIES OF POLITICAL SUCCESS OR FAILURE IN EAST AND SOUTHEAST ASIA, 113-139 (L. White ed., 2005).

ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY (1972).

Oscar Wilde, *The Decay Of Lying*, in INTENTIONS (Oscar Wilde ed., 1889)

Franz Werro *The Right to Inform Versus the Right to be Forgotten: A Transatlantic Clash*, in HAFTUNGSRECHT IM DRITTEN MILLENNIUM (LIABILITY IN THE THIRD MILLENNIUM) (A. C. Ciacci, et al., eds. 2009).

TENNESSEE WILLIAMS, THE MILK TRAIN DOESN'T STOP HERE ANYMORE (1963).

JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET - AND HOW TO STOP IT (2008).

JONATHAN L. ZITTRAIN, JURISDICTION (2005).

h Academic Journals

Anders Albrechtslund, *Online Social Networking as Participatory Surveillance*, FIRST MONDAY (3 MAR. 2008) http://firstmonday.org/ojs/index.php/fm/article/view/2142/1949

Meg Ambrose, *It's About Time: Privacy, Information Lifecycles, and the Right to Be Forgotten.* 16 STAN. TECH. L. REV.396–422 (2012).

Meg Leta Ambrose and Jef Ausloos, *The Right to be Forgotten Across the Pond*, 3 J. INF. POL. 1 (2013).

Meg Leta Ambrose, *et al.*, *Seeking Digital Redemption: the Future of Forgiveness in the Internet Age*, 24 SANTA CLARA COMPUTER & HIGH TECH. L. J. 99 (2010).

Meg Angelo, *You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship*, 17 INT'L REV. INF ETHICS. 23 (2012).

Ellyn M. Angelotti, *Twibel Law: What Defamation and its Remedies Look Like in the Age of Twitter*, 13 J. HIGH. TECH. L. 430 (2013),

https://www.suffolk.edu/documents/jhtl_publications/ANGELOTTI-MACROFINALFINAL.pdf

David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. CIV. RTS-CIV. LIB. L. REV. 261, 262 (2010).

David S. Ardia, *Freedom of Speech, Defamation, and Injunctions*, 55 WILLIAM & MARY L. REV. 4 (2013).

Alissa Ardito, *Social Media, Administrative Agencies, And The First Amendment*, 65 ADMIN. L. REV. 301, 378 (2013).

Jeff Ausloos, *The Right to be Forgotten - Worth Remembering?* 28 CLSR, 143-152 (2011).

Hadar Aviram and Annick Persinger, *Perceiving and Reporting Domestic Violence Incidents in Unconventional Settings: A Vignette Survey Study*, 23 HAST. W. L. J. 159 (2012).

Patricia Avidan, *Protecting the Media's First Amendment Rights in Florida: Making False Light Plaintiffs Play by Defamation Rules*, 35 STET. L. REV. 227 (2005).

Shazia Aziz *et al.*, *The Impact of Texting/SMS Language on Academic Writing of Students – What do we need to panic about?* 55 ELIXIR LING. & TRANS. J. 12884 (2013),

Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 NYU L. REV. 1 (2004).

Jamison Barr & Emmy Lugus, *Digital Threats on Campus: Examining the Duty of Colleges to Protect Their Social Networking Students*, 33 WEST. N. ENG. L. REV. 757 (2011).

Susan Benesch, *Troll Wrastling for Beginners: Data-Driven Methods to Decrease Hatred Online*, BERK. CTR. INT. & SOC. (Mar. 25, 2014) http://cyber.law.harvard.edu/events/luncheon/2014/03/benesch.

Yochai Benkler, *Freedom in the Commons: Towards a Political Economy of Information*, 52 DUKE L. J. 1245-1276, http://www.law.duke.edu/shell/cite/pl?52+Duke+L.+J.+1245.

William Bennett, *Rome II and Defamation*, BR. INST. INTL & COMP. L. (BIICL) (27 Sept. 2010), *http://www.biicl.org/files/5177_bennett_27-09-10_biicl.pdf.* (2010).

Steven C. Bennett, *The 'Right to be Forgotten': Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L., 161 (2012).

Paul A. Bernal, *A Right to Delete?'* 2 EUR. J. L. & TECH., 2, (2011), http://ejlt.org/article//view/75/144.

Jean-Fancois Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 INF. SOC. 33–45 (2002).

Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N. C. L. REV. 2, (2012) http://ssrn.com.abstract=2024661.

William O. Bertlesman, *Injunctions Against Speech and Writing: A Re-Evaluation*, 59 KY L.J. 319, 323 (1971

S.J. Best, B.S. Krueger, & J. Ladewig, *The Polls – Trends: Privacy in the Information Age*, 70 PUB. OPIN. Q., 375 (Fall 2006).

Randall P. Bezanson, *Libel Law and the Realities of Litigation: Setting the Record Straight*, 71 IOWA L. REV., 226, 227 (1985).

Joseph Blocher, *Reputation as Property in Virtual Economics*, 118 YALE L.J. POCKET PART 120 (2009);

dana boyd, *The Future of Privacy: Privacy Norms can Inform Regulation*, 32nd INT. CONF. D. P. & PRIV. COMMISS. (29 Oct. 2010).

dana boyd, *Debate: Networked Privacy*, 10 SURV. & SOC. 348 (2013).

Dana boyd & Nichole B. Ellison, *Social network sites: Definition, history, and scholarship.* 13 J. COMP.-MED. COMM., (2007) http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Randall Bezanson, *Libel Law and the Realities of Litigation: Setting the Record Straight*, 71 IOWA L. REV., 226, 227 (1985).

Louis Brandeis and Samuel Warren, *The Right to Private Property*, 4 HARV. L. REV. 193.

Paul S. Braterman, *How Science Figured Out the Age of Earth*, SCI. AM. (20 Oct. 2013), http://www.scientificamerican.com/article/how-science-figured-out-the-age-of-the-earth/http://www.scientificamerican.com/article/how-science-figured-out-the-age-of-the-earth/.

Ben E. Bratman, *Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 10 (2002).

Susan Brenner, *Cyber Metrics: Old Wine, New Bottles?* 9 VIRG. J. LAW & TECH., 1 (2004).

John G. Browning, *Why Can't We Be Friends? Judges' Use of Social Media*, 68 U. MIAMI L. REV. 447 (2014).

Gena & John G. Browning, *Social Networking Dos and Don'ts for Lawyers and Judges*, 73 TEX. B. J., 192 (2010).

Graham Carmode & Balachander Krishnamurthy, *Key differences between Web 1.0 and Web 2.0*, 13 FIRST MONDAY (2 June 2008), http://journals.uic.edu/ojs/index.php/fm/article/view/2125/1972#p2.

Pere Simon Castellano, *The Right to be Forgotten under European law: a Constitutional Debate*' 6 LEX ELECTRONICA, 1 (2012).

Michael Alison Chandler, A President's Illness Kept Under Wraps', WASH POST (3 Feb. 2007) http://www.washingtonpost.com/wp-dyn/content/article/2007/02/02/AR2007020201698.html.

Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 2 (2013).

Chris Conley, *The Right to Delete*, Association for the Advancement of Artificial Intelligence (AAAI) Spring Symposium Series, 8 (2010).

Susan Corbett, *The retention of personal information online: A call for international regulation of privacy law*, 29 COMP. L. & SEC. REV. 246 (2013).

Jill Cottrell, *What does 'Defamatory' Mean? Reflections on* Berkoff v. Berchill, TORT L. REV. 149 (1998).

Neville Cox, *Delfi AS v Estonia: The Liability of Secondary Internet Publishers for Violation of Reputational Rights under the European Convention on Human Rights*, 77 MOD. L. REV. 619-629 (July 2014).

Tamas Dezlo Czigler, *Choice of Law in the Internet Age: US and European Rules*, 53 ACTA JURIDICA HUNGARICA - HUNGARIAN J. L. STUD. 193 (2012).

Ron Deibert, *The Growing Dark Side of Cyberspace (…and what to do about it)*, 1 PENN ST. J. L. & INT'L. AFF. 260 (2012).

Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L. REV. 7.

Christina Demetriou & Adam Silke, *A Criminological Internet 'Sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap*', 45 BRIT. J. CRIM., 213, http://ssrn.com/abstract=1160788.

S.A. Dobbin *et al. Applying Daubert: How Well Do Judges Understand Science And Scientific Method?* 85 JUDICATURE, 244–47 (March/April 2002).

Martin Dodge, & Robert Kitchin, *Code, objects and home spaces*, 41 ENVIRONMENT AND PLANNING, 1344 (2009).

Ron A. Dolin, *Search Query Privacy: The Problem of Anonymization*, 2 HASTINGS SCI. & TECH. J. 137 (2013).

John J. Dougherty, *Obsidian financial Group, LLC v. Cox and Reformulating Shield Laws to Protect Digital Journalism in an Evolving Media World*, 13 N.C.J.L. & TECH. ON. 287, http://www.ncjolt.org/sites/default/files/6RD_Dougherty_287_322.pdf.

George W. Downs & Michael A. Jones, *Reputation, Compliance, and International Law*, 32 J. L. STUDIES, S95 (2002), http://www.nyu.edu/gsas/dept/politics/faculty/downs/reputation.pdf.

William Dutton, *Programming to Forget: Review of* DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE BY VICTOR MAYER-SCHONBERGER, 327 SCIENCE (19 Mar. 2010), 1456.

Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U. CHI. LEGAL F. 207 (1996).

Paul Easton, *Splitting the Difference: Layshock and J.S. Chart a Separate Path on Student Speech Rights*, 53 B.C.L. REV. E. SUPP. 17 (2012), http://lawdigitalcommons.bc.edu/bclr/vol53/iss6/3.

EDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited, 5 RB MEDIA & ENT. L., http://www.5rb.com/case/edate-advertising-gmbh-v-x-and-olivier-martinez-and-robert-martinez-v-mgn-limited/.

Ellison, P., Govern J., Petri, H. & M. Figler, *Anonymity and Aggressive Driving Behavior: A Field Study*, 10 J. SOC. BEH. & PERS. 265.

Karen Eltis, *Does Avoiding Judicial Isolation Outweigh the Risks Related to 'Professional Death by Facebook?*, 3 LAWS (2014) 636, 639, www.mdpi.com/journal/laws/.

Karen Eltis, *Breaking through the 'Tower of Babel': A 'Right to be Forgotten' and How Trans-Systemic Thinking can help Reconceptualize Privacy Harm in the Age of Analytics*, 22 FORD. INTEL. PROP. MED. & ENT. L. J., 69.

Kathy English, *The longtail of news: To unpublish or not to unpublish*, Report, Toronto Star Online Journalism Credibility Project, (Oct. 2009) http://www.apme.com/?Unpublishing.

Kenneth Farrell, *Global Privacy in Flux: Illuminating Privacy across Cultures in China and the US*, 2 INTL J. COMM., 993 (2008).

Stefan Ferber, *How the Internet of Things Changes Everything*, HARV. BUS, REV. (7 May 2013), https://hbr.org/2013/05/how-the-internet-of-things-cha/.

G.A. Fine, *Reputational Entrepreneurs and the Memory of Incompetence: Melting Supporters, Partisan Warriors, and Images of President Harding*," 101 AMER. J. SOC. 1159-1193 (1996).

Nichoel Forrett, *Cookie Monster: Balancing Internet Privacy with Commerce, Technology and Terrorism*, 20 TOURO L. REV. (2004), http://digitalcommons.tourolaw.edu/lawreview/vol20/iss2/11.

Steven J. Frenda, *et al.*, *Sleep Deprivation and False Memories*, PSYCH. SCI. (2014).

Charles Fried, *Privacy*, 77 YALE L. J. 475. (1968).

William H. Freivogel, *Does the Communications Decency Act Foster Indecency?*, 16 COMM. L. & POL. 17 (Winter 2011)

Luciano Floridi, *The Ontological Interpretation of Informational Privacy*, 7 ETH. & INF. TECH., 185-200.

S.I. Gatowski, *et al.*, *Asking The Gatekeepers: A National Survey Of Judges On Judging Expert Evidence In A Post-Daubert World*, 25 J. L. & HUMAN BEHAVIOR 433–58 (2001).

Carlisle George & Jackie Scerri. *Web 2.0 and User-Generated Content: legal challenges in the new frontier*, J. INF. L. & TECH. (JILT) http://go.warwicck.ac.uk/jilt/2007_2/George_scerri.

Seema Ghatnekar, *Injury By Algorithm: A Look Into Google's Liability For Defamatory Autocompleted Search Suggestions*, 33 LOY. L.A. ENT. L. REV. 171 (2013), http://digitalcommons.lmu.edu/elr/vol33/iss2/3.

Tarleton Gillespie, *The Politics of Platforms*, NEW MEDIA & SOC. SEARCH (2010), http://ecommons.librarty.cornell.edu/handle/1813/12774,

Mary Ann Glendon, *The Rule of Law in the Universal Declaration of Human Rights*, 2 NW. J. INT'L HUM. RTS. 1 (2004). http://scholarlycommons.law.northwestern.edu/njihr/vol2/iss1/5.

Estella Gold, *Does Equity Still Lack Jurisdiction to Enjoin a Libel or Slander*? 48 BROOK. L. REV. 231, 262 (1982).

Eric Goldman, *Online User Account Termination and 47 U.S.C. §230(c)(2)*, UC 2 IRV. L. REV. (2012).

Cathy Gonzalez, *The role of blended learning in the world of technology* (2004) http://www.unt.edu/benchmarks/archives/2004/september04/eis.htm>.

Google ordered to change autocomplete function in Japan, BBC NEWS (26 Mar. 2012), http://www.bbc.com/news/technology-17510651.

S. Gosling, *et al. Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information*, 14 CYBERPSY., BEH., & SOC. NETW. 483 (2011).

Nanette Gottlieb, *Playing with Language in E-Japan: Old Wine in New Bottles"*, 12 JAP. STUDIES, 393-407 (2010)).

Mark Grabowski, *Are Technical Difficulties At The Supreme Court Causing A 'Disregard Of Duty?'* 3 J. L. TECH. & INTERNET, 1 (2011).

Marc H. Greenberg, *A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market*, 18 BERK. TECH. L.J. 1191 (2003), http://scholarship.law.berkeley.edu/btlj/vol18/iss4/6.

Graham Greenleaf *"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?* 29 COMPUTER L. & SEC. REV. (2013), http://ssrn.com/abstract=2262296.

Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAN. L. REV. 453 (1990).

Paul Haahr & Steve Baker, *Making search better in Catalonia, Estonia, and everywhere else*, cited by Ron A. Dolin, Search Query Privacy: *The Problem of Anonymization*, 2 HASTINGS SCI. AND TECH. L.J. 137, note 14.

Trevor C. Hartley, *'Libel Tourism' and the Conflict of Laws*, 59 INT'L & COMP. L. Q. 25, 26 (2010).

Geoffrey C. Hazard Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CAL. REV. 1061, 1078 (1978)

John Hendel, *Why Journalists Shouldn't Fear Europe's 'Right to be Forgotten'"*, ATLANTIC (25 Jan. 2012), http://www.theatlantic.com/technology.archive/2012/01/why-journalists-shouldn't-fear-europe's-right-to-be-forgotten.html.

Laura E. Heymann, *The Law of Reputation and the Interest of the Audience*, 52 B.C.L.REV. (2011).

Martin Hilbert & Priscila Lopez, *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE, 60.

Patricia Hunt, *Tortious Tweets: A Practical Guide to Applying Traditional Defamation Law to Twibel Claims*, 73 LA L. REV., 578, http://twitter.com/about.

David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN L. REV. 1367, 1367 (1996).

Yuval Karniel, *Defamation on the Internet: A New Approach to Libel in Cyberspace*, 2 J. INT'L MED. & ENT. L. 215 (2009).

Gaurav Keerthi, *Digital Politics: Old wine, new bottle? (*30 October 2013), http://gauravkeerthi.com/blog/2013/10/digital-politics-old-wine-new-bottle/.

Teo Keipi et al. *Who prefers anonymous self-expression online? A survey-based study of Finns aged 15–30 years*, 18 Inf., Comm. & Soc. (2015)

Sylvia Kierkegaard, *et al.*, *The review of the Council of Europe Data Protection Convention 108*, 23 COMP. L. & SEC. REV. 223 (2011).

Andrew T. Kenyon, *What Conversation? Free Speech and Defamation Law*, 73 MODERN. L. REV., 697 (2010).

Harry D. Krause, *The Right to Privacy in Germany – Pointers for American Legislation?* DUKE L. J., 481 (1965).

Jan-Jaap Kuipers, *Joined Cases C-509/09 & 161/10*, 49 COMMON MARKET L. REV., 1211 (2012).

Jan-Jaap Kuipers, *Towards a European approach in the Cross-Border Infringement of Personality Rights*, 12 GERM. L. J. 1681, 1697 (2011).

Christopher Kuner, *The European Commissions' Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, BLOOMBERG BNA PROV. & SEC. L. REP. (6 Feb. 2012) 1-15.

Christopher J. Kunke, *Rome II and Defamation: Will the Tail Wag the Dog?* 19 EMORY INT'L. L. REV. 1733 (2005).

Kaley Leetaru, *New media vs. Old media: A portrait of the Drudge Report* 2002-2008, 14 FIRST MONDAY (6 July 2009), http://journals.uic.edu/ojs/index.php/fm/article/view/2500/2235.

Jill Lepore, *The Prism: Privacy in an age of publicity*, NEW YORKER (24 June, 2013) 32, 36, CIV. RTS-CIV. LIB. L. REV. 261 (2010).

Jill Lepore, *The Cobweb: Can the Internet be Archived?* NEW YORKER 26 Jan. 2015), 34.

Vladimir Lernet *et al.*, *'Internet Delusions': The Impact of Technological Developments on the Content of Psychiatric Symptoms*, 43 ISR J. PSYCHIATRY RELAT. SCI., 47 (2006).

Lawrence Lessig, *The Law of the Horse: What Cyberlaw might Teach*, HARV. L. REV. (1999)

Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace* 49 DUKE L.J. 855, 862-63 (2000).

Lyrissa Barnett Lidsky, *Defamation, Reputation, and the Myth of Community*, 71 WASH. L. REV. 1, 37 (1996).

Laura E. Little, *Internet Defamation, Freedom of Expression, and the Lessons of Private International Law in the United States*, 14 EUR. YEARBOOK PRIV. INTL L., 2 (2012).

Jaqueline Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video"*, 96 IOWA L. REV. 919 (2010).

Elizabeth F. Loftus, *Reconstruction of automobile destruction – Example of interaction between language and memory*, 13 J. VERBAL LEARNING & VERBAL BEH. 585 (1974)

Elizabeth F. Loftus & Jacqueline E. Pickrell, *The formation of false memories*. 25 PSYCH. ANNALS, 720-725 (1995).

S. Elizabeth Malloy, *Anonymous Bloggers and Defamation: Balancing Interests on the Internet*, 84 WASH. U. L. REV. 1187 (2006).

Steve Mann *et al.*, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURV. & SOC. 1, 331-355 (2003),

Inga Markovits, *Selective Memory: How the Law Affects what we forget and remember about the past: the Case of East Germany*, 35 LAW & SOC. REV. 513.

Viktor Mayer-Schonberger & Malte Ziewitz, *Jefferson Rebuffed: The United States And The Future Of Internet Governance*, 8 STAN. TECH. L. REV. (2013).

Michael McFall, *American and English Libel Law - Which Approach is Best?* EUR. J. L. & TECH. (2012).

Dhiraj Murthy, *Twitter and elections: are tweets predictive, reactive, or a form of buzz?* 18 Inf. Comm. & Soc. 816 (2015).

Kurt H. Nadelmann, *The Benelux Uniform Law on Private International Law*, 18 AM. J. COMP. L. 406, 420 (1970).

Marlene Arnold Nicholson, *McLibel: A Case Study in English Defamation Law*, 18 WIS. INT. L. J., 1 (2000).

Alastair Mullis & Andrew Scott, *Tilting at Windmills: the Defamation Act 2013*, 77 MOD. L. REV. 87 (2014).

Csongor Istvan Nagy, *Jurisdiction, Applicable Law and Personality Rights in EU Law – Missed and New Opportunities*, 8 J. PRIV. INT'L. L., 251, 253 (2012), also cited as Csongor Istvan Nagy, *The Word is a Dangerous Weapon: Jurisdiction, Applicable Law, and Personality Rights in EU Law – Missed and New Opportunities*, 8 J. PRIV. INT. L. 251 (2012).

Beth Simone Noveck, *Trademark Law and the Social Construction of Trust: Creating the Legal Framework for Online Identity*, 83 WASH.U.L.Q. 1773 (2005);

Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERK. TECH. L.J. 1115 (2005).

Elissa A. Okoniewski, *Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet*, 18 AM. U. INT'L L. REV. 295 (2002).

Michael E. O'Neill, *Old Crime in New Bottles: Sanctioning Cybercrime*, 37 GEO. MASON L. REV. 237 (2000).

Rodney W. Ott, *Fact and Opinion in Defamation: Recognizing the Formative Power of Context*, 58 FORD. L. REV. (1990) 761.

Mary-Rose Papandrea, *Moving Beyond Cameras in the Courtroom: Technology, the Media, and the Supreme Court*, 2012 BYU L. Rev. 1901 (2012). http://digitalcommons.law.byu.edu/lawreview/vol2012/iss6/7.

David Pogue, *Why Google Glass is Creepy*, 308 SCI. AM. (14 May 2014).

Richard A. Posner, *The Right of Privacy*, 12 GEORGIA L. REV. 393, 393 (1977).

Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691, 692 (1986).

Roscoe Pound, *Interests Of Personality* (parts 1, 2) 28 HARV. L. REV. 343 (1915).

David Pritchard, *Rethinking Criminal Defamation*, 14 COMM. L. & POL'Y 303 (2009)

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383-423 (1960).

Martin H. Redish, *Of New Wine and Old Bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution*, 38 JURIMETRICS J. 575-610 (1998).

Alan Reed, *The Anglo-American Revolution in Tort Choice of Law Principles: Paradigm Shift or Pandora's Box?* 18 ARIZ. J. INT'L & COMP. L. 867, 878 (2001).

Chris Reed, *How to Make Bad Law: Lessons from Cyberspace*, 73 MODERN L. REV. 903-932 (2010), http://ssrn.com.abstract=1538527.

Mathias Reimann, *Codifying Torts Conflicts: the 1999 German Legislation in Comparative Perspective*, 60 LA. L. REV. 1297, 1307 (2000).

Curtis Reitz, *Enforcement of the General Agreement on Tariffs and Trade*, 17 U. PA. J. INT'L. ECON. L., 555 (1996).

Carla L. Reyes *The U.S. Discovery –EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy*, 19 DUKE J. COMP. & INT'L L. 359 (2009).

Fitzpatrick Glenn Harlan Reynolds, *Libel in the Blogosphere: Some Preliminary Thoughts*, 84 WASH. U. L. REV. 1157 (2006).

J. Lee Ricardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?* 6 B. C. INTL. & COMP. L. REV., 243, 245.

Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. R. 1887 (2010).

Neil. M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L. J., 123 (2007).

Matthew Rimmer, *Gossip we can trust: defamation law and non-fiction*, 9 MEDIA A. & L. REV., 37 (Mar. 2004)

Jeffrey Rosen, *The Purposes of Privacy: A Response*" 89 GEO. L. J. 2117 – 2137 (2001).

Hannes Rosler, *Dignitarian Posthumous Personality Rights - An Analysis of U.S. and German Constitutional and Tort Law*, 26 BERKELEY. J. INT'L L. 153 (2008) http://scholarship.law.berkeley.edu/bjil/vol26/iss1/4.

Mary Rumsey, *Runaway Train: Problems of Permanence, Accessibility, and Stability in the Use of Web Resources in law Review Citations*, 94 LAW LIBR. J. 27, 35 (2002).

Johnny Ryan, *How the atom bomb helped give birth to the Internet*, ARS TECHNICA (21 Feb, 2011), http://arstechnica.com/tech-policy/2011/02/how-the-atom-bomb-gave-birth-to-the-internet/3/.

Elizabeth Samson, *The Burden to Prove Libel: A Comparative Analysis of Traditional English and U.S. Defamation Laws and the Dawn of England's Modern Day*, 20 CARDOZO J. INT. & COMP. L. (JICL) (2012), http://ssrn.com/abstract=2170040.

Austin Sarat, *et al.* (eds), IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY, *Introduction*, (2012).

Andrej Savin, *How Europe formulates internet policy*, 3 INT. POL. REV. (26 Feb. 2014), http://policyreview.info/articles/analysis/how-europe-formulates-internet-policy.

Julian Sanchez, *Book Review*: *The Future of Reputation: Gossip, Rumor, and Privacy Online by D. Solove*, ARS TECHNICA (Oct. 6, 2008), http://arstechnica.com/tech-policy/2008/10/future-of-reputation/.

Giovanni Sartor, *Privacy, Reputation, and Trust: Some Implications for Data Protection*, EUR. U. INST. Working Paper No. 2006/04 (2006), http://ssrn.com/abstract=891123.

Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV L. REV. 1966 (2013).

Paul M. Schwartz and Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?* 98 CAL. L. REV. 1925, 1947 (2010).

Paul M. Schwartz & Daniel L. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 85 NYU L. REV. 1814 (2011).

Paul M. Schwartz & Daniel H. Solove. *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. (2014).

Julie Shaw and Stephen Porter, *Constructing Rich False Memories of Committing Crime*, PSYCH. SCI. (14 Jan. 2014).

Stephen A. Siegel, *Injunctions for Defamation, Juries, and the Clarifying Lens of 1868*, 56 BUFF. L. REV. 655 (2008).

Stijn Smet, *Freedom of Expression and the Right to Reputation: Human Rights in Conflict*, 26 AM. U. INT'L. REV., 183 (2010).

Michael L. Smith, *Search Engine Liability for Autocomplete Defamation: Combating the Power of Suggestion*, 2013 J. L. TECH. & POLICY, 314, 314-315 (2013).

Kirsten Rabe Smolensky, *Rights of the Dead*, 37 HOFSTRA L. REV. 763 (2009)

Rodney A. Smolla, *Let the Author Beware: The Rejuvenation of the American Law of Libel*, 132 U. PA. L. REV. 1 (1983).

Rodney A. Smolla, *The First Amendment, Journalists, and Sources: A Curious Study in Reverse Federalism'*, 29 CARDOZO L. REV. 1423 (2008), http://cardozolawreview.com/Joomla1.5/content/29-4/29.4_smolla.pdf.

Chris Snijders, et al. *Big Data': Big gaps of knowledge in the field of Internet*, 7 INTL. J. INT. SCI. 1 (2012), http://www.ijis.net/ijis7_1/ijis7_1_editorial.html.

Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 S. DIEGO L. REV., 745 (2007).

Daniel J. Solove, *A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere*, 84 WASH. U. L. REV. 1195 (2006).

Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477 (2006).

Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, University of San Diego School of Law, Public Law and Legal Theory Research Paper 55, 34 (June 2003).
B. Sparrow *et al.*, *Google Effects on Memory: Cognitive Consequences of Having information at our finger tips*, 333 SCIENCE, 776 (2011).

Justin Storbeck & Gerald L. Clore, *With Sadness Comes Accuracy; With Happiness, False Memory Mood and the False Memory Effect*, 16 PSYCH. SCI., 785-791 (2005).

John Suler, *The Online Disinhibition Effect*, 7 CYBERPSY. & BEH. 324 (2004).

Symeon C. Symeonides, *Rome II and Tort Conflicts: Missed Opportunities*, 56 AM. J. COMP. L. (2008).

Mary K. Taylor & Diane Hudson, *"Linkrot" and the Usefulness of Web Site Bibliographies*, 39 REF. & USER SERVICES Q. 273 (2000).

Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, UTAH L. REV., No 4, 1433, 1435 (2008).

Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 11 YALE J. L. & TECH. 351 (Fall 2013).

Adam Thierer, *The Pursuit of Privacy in a World Where Information Control is Failing*, 36 HARV. J. L. & PUB. POL., 410 (2013).

Adam J. Tutaj, *Intrusion upon Seclusion: Bringing an "Otherwise" Valid Cause of action into the 21st Century*, 82 MARQ. L. REV. 655 (1999).

Michalus Vafopolous, *Being, space, and time on the Web*, 43 METAPHILOSOPHY, 405-425.

Robert K. Walker, *Note: The Right to be Forgotten*" 64 HAST. L. J. 257 (2012).

Van Vechten Veeder, *The History and Theory of Defamation Law*, 3 COL. L. REV. 546 (1903).

Kathleen Elliott Vinson, *The Blurred Boundaries of Social Networking in the Legal Field: Just "Face" it*, 41 U. MEMPHIS L. REV. 355 (2010).

James Q. Whitman, *The Two Western Cultures Of Privacy: Dignity Versus Liberty*, 113 YALE L. J., 1151 (2004).

Napoleon Xanthulis, *The Right to Oblivion in the Information Age: A Human Rights Based Approach*, 10 US CHINA REV. 84 – 98 (nd).

Amiram Yehudai, *Informational Blackmail: Survived by Technicality*, 92 MARQ. L. REV. 779, 821 (2009).

Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697 (2010).

Jonathan Zittrain, *The Generative Internet*, 119 HAR. L. REV., 1974, (2006).

Jonathan Zittrain, *The Fourth Quadrant*, 78 FORD. L. REV. 2767 (2010).

I Bills, Warrants, Proposed Legislation, Drafts

In re *A Warrant To Search A Certain E-Mail Account Controlled And Maintained By Microsoft Corporation*, Case 13-MAG-2814; M9-150USDC NY (filed 06/06/14).

Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, ETS Convention 108.

Do Not Track Online Act, H.R. 654, 112th Congress, §2011–2013 (5 May 2011).

Do Not Track Kids Act H.R. 1895, 112th Leg. 1st Spec. Sess. (2011).

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

J Conference Papers, Working Papers, Policy Papers, Reports, Memoranda, Press Releases

Access To Data Protection Remedies In EU Member States, Report, European Union Agency For Fundamental Rights, Publications Office Of The European Union: Luxembourg (2013), http://Fra.Europa.Eu/Sites/Default/Files/Fra-2014-access-data-protection-remedies_en.pdf.

Access to Information, Google Transparency Report, http://www.google.com/transparencyreport/.

J. P. Albrecht, *Report On The Proposal For A Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data* (General Data Protection Regulation) COM (2012)0011-C7-0025/2012-2012/0011(COD), A7-0402/2013, 21.11.2013,

Norberto Nuno Gomes de Andrade, *Oblivion: the Right to be Different from Oneself, Reproposing the 'Right to Be Forgotten'*, in VII International Conference On Internet, Law & Politics, Net Neutrality And Other Challenges For The Future Of The Internet, IDP. Revista de Internet, 13 Derecho Y Politica, 122-137.

Jan Philipp Albrecht, Draft Report On General Data Protection Regulation, Cod 2012/0011 (12 Dec. 2012).

Annual Report 2000, Volume III, Chapter III A.2. OEA/Ser.L/V/II.111 Doc. 20, Inter-American Commission On Human Rights, (rev. 16 April 2001).

Annual Report 1998, Volume III, Chapter IV A. OEA/Ser.L/V/II.102 Doc.6, Inter-American Commission On Human Rights (rev. 16 April 1999).

Annual Report Of The IACHR, 1998 Volume III, Chapter IV A. –OEA/Ser.L/V/II.102 Doc.6 (rev. 16 April 1999); and Annual Report Of The IACHR, 2000 Volume III, Chapter III A.2. –OEA/Ser.L/V/II.111 Doc.20 (rev. 16 April 2001).

Annual Tracking 2013 Report, Office Of The Information Commissioner, United Kingdom (June 2013), http://www.ico.org.uk/about.

Anti-Spam Activities Report, European Union Agency For Network And Information Security (ENISA), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/anti-spam-measures.

Liam Bannon, *Forgetting as a Feature, not a Bug: the Duality of Memory and Implication for Ubiquitous Computing*" 2 CODESIGN, 3-15 (2006).

Basic Principles And Guidelines On The Right To A Remedy And Reparation For Victims Of Gross Violations Of International Human Rights Law And Serious Violations Of International Humanitarian Law, GA 60/147 (16 Dec. 2005).

A Beginner's Guide to BitTorrent – Videos & Guides, BITTORRENT http://wwwbittorent.com/help/guides/beginners-guide.

William Bennett, *Rome II and Defamation*, British Institute of International and Comparative Law (BIICL), http://www.biicl.org/files/5177_bennett_27-09-10_biicl.pdf (2010).

Herbert Burkert, *Privacy – Data Protection: A German/European Perspective*, Research Paper, Max Planck Institute For Research, (nd), https://Www.Coll.Mpg.De/Sites/Www.Coll.mpg.de/files/text/burkert.pdf.

Eva Buechel & Jonah Berger, *Facebook Therapy? Why Do People Share Self-Relevant Content Online?* (2012) SSRN, http://ssrn.com/abstract=2013148.

William J. Clinton & Al Gore, A Framework For Global Electronic Commerce, (1 July 1997) http://www.technology.gov/digeconomy/framwrk.htm.

Collateral Damage: America's Failure to Forgive or Forget in the War on Crime - A Roadmap to Restore Rights and Status After Arrest and Conviction', Report, National Association Of Criminal Defence Lawyers (2014) https://www.nacdl.org/reports/.

Commission Proposes A Comprehensive Reform Of Data Protection Rules To Increase Users' Control Of Their Data And To Cut Costs For Businesses, Communication, European Commission (25 Jan. 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

A Communication To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions", Communication, European Commission, COM 609, 8 (2010).

A Comparative Study of Costs in Defamation Proceedings Across Europe, Report, Centre For Socio-Legal Studies, University of Oxford, 173 (2008), http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/.

A Comparative Study On The Situation In The 27 Member States As Regards The Law Applicable To Non-Contractual Obligations Arising Out Of Violations Of Privacy And Rights Relating To Personality, Final Report JLS/2007/C4/028, European Commission (2007) http://ec.europa.eu/justice/civil/files/study_privacy_en.pdf.

A Comparative Study Of Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments, Final Report JLS/2008/C4/011 – 30-CE-0219363/00-28 European Commission, (Jan. 20, 2010), http://ec.europa.eu/justice/policies/privacy/docs//new_privacy_challenges/final_report_en.pdf.

The Compatibility of "Desacato" Laws with the American Convention on Human Rights, Report, Inter-American Commission On Human Rights (rev. 17 February 1995).

A Comprehensive Approach On Personal Data Protection In The European Union, Communication, European Commission, COM (2010) 609 final.

Cross-border Data Flows and Protection of Privacy, Report, Hague Conference On Private International Law (March 2010), http://www.hcch.net/upload/wop/genaff2010pd13e.pdf.

Mario Viola De Azevedo Cunha *et al.*, *Peer-to-Peer Violations and ISP Liabilities: Data Protection in the User-Generated Web*, Working Paper, European University Institute (2011/11), *http://www.utwente.nl/mb/pa/staff/marin/peer-topeer%20privacy%20violations%20and%20ISP%20Liability.pdf.*

Cybercrime training for judges and prosecutor: a concept, Council Of Europe Project On Cybercrime And The Lisbon Network, (8 Oct. 2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf.

Data Breach Notifications In The EU, Report, European Network And Information Security Agency (ENISA) (2013), www.enisa.europa.**eu**/act/it/library/deliverables/dbn/at.../fullReport.

Data Brokers: A Call For Transparency And Accountability, Study, Federal Trade Commission (May 2014), http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Data Protection Day 2014: Full Speed On EU Data Protection Reform, Communication, European Commission (27 Jan. 2014), http://europa.eu/rapid/press-release_MEMO-14-60_en.htm.

Defamation And Freedom Of Expression: Selected Documents, Council Of Europe, Directorate General of Human Rights (March 2003), http://www.coe.int/t/dghl/standardsetting/media/doc/H-ATCM(2003)001_en.pdf.

Defamation And Insult Laws, Memorandum, United States Helsinki Commission On Security And Cooperation In Europe, http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewDetail&ContentRecord_id=18&Region_id=84&Issue_id=0&ContentType=G&ContentRecordType=G&IsTextOnly/ (December 14, 2001).

Defamation Law: Introduction, Article 19 Working Group, http://www.article19.org/data/files/pdfs/publications/civil-defamation.pdf.

Ron Deibert, *Shadows In The Cloud: Investigating Cyber Espionage 2.0*, Report, Information Warfare Monitor And Shadow Server Foundation (2010), http://deibert.citizenlab.org/publications/.

Chrisanthos Dellarocas, *Designing Reputation Systems for the Social Web*, Paper 2010-18, BOSTON U. S. MGMT (June 13, 2010) http://ssrn.com/abstract=1624697.

Laura DeNardis, *The Emerging Field of Internet Governance*, Yale Information Society Project Working Paper, (Sept. 2010) available at http:www.ssrn/abstract1678343.pdf.

P. Druschel et al., *The Right To Be Forgotten: Between Expectations And Practice*, Report, European Network And Information Security Agency (ENISA) (18 Oct. 2011).

William H. Dutton, et al., *The Internet Trust Bubble: Global Values, Beliefs And Practices*, Report, World Economic Forum (2014), http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf.

A. Eaton, & A.M. Persinger. *Perceiving and Reporting Domestic Violence Incidents in Unconventional Settings: A Vignette Survey*, Report, 4th Annual Conference On Empirical Legal Studies, http://ssrn.com/abstract=142819.

Ending the Chilling Effect: Working to Repeal Criminal Libel and Insult Laws, Organization For Security And Co-Operation In Europe (OSCE) (25 Nov. 2004), http://www.osce.org/fom/13573.

European Commission of Human Rights Preparatory Work on Article 10 of the European Convention on Human Rights, Council of Europe, Strasbourg, 17 Aug. 1956 (DH (56) 15 Oe.Fr., www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaus-Art10-DH/…pdf.
EU-US Joint Press Statement, Press Release, JUSTICE AND HOME AFFAIRS Ministerial Meeting in Washington DC (18 November 2013), http://europa.eu/rapid/press-release_MEMO-13-1010_de.htm.

Facebook claims to become 'biggest stadium in the world' for World Cup, RT (9 June 2014) www.facebook.com/fifaworldcup.

Fact Sheet: EU-US Negotiations on Data Protection, IP/10/1661, EU-US "Umbrella Agreement" for transfers and processing of data in the context of police and judicial cooperation, http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf.

Fact Sheet on the Right to be Forgotten Ruling (C131/12) EC, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Framework For Global Electronic Commerce, Report, United States Government Washington DC, (1 July 1997) http://Clinton4.Nara.Gov/WH/New/Commerce/.

Richard D. Freer, *American and European Approaches to Personal Jurisdiction Based upon Internet Activity*, Research Paper No. 07-15 R, Emory University School Of Law And Legal Theory (2007).

Future Of Big Data, Research Report, Pew Internet Research (20 July 2012), http://www.pewinternet.org/2012/07/20/the-future-of-big-data-2/.

Future of the Internet, INTERNET SOCIETY, https://www.internetsociety.org/internet/how-its-evolving/future-scenarios.

U.S. Internet Users Less Concerned About Gov't Snooping, GALLUP Report http://www.gallup.com/poll/165569/internet-users-less-concerned-gov-snooping.aspx

Urs Gasser & John Palfrey, *Fostering Innovation and Trade in the Global Information Society: the different facets and roles of interoperability*, World Trade Institute Working Paper 2011/39 (June 2012) 8.

Urs Gasser & John Palfrey, *Interoperability in Information and Information Systems in the Furtherance of Trade*, World Trade Institute Working Paper 2012/26 (June 2012) 3.

Bruce Girard, Sean O Siochru, *Communicating in the Information Society*, Paper, Information Technologies And Social Development Project, United Nations Research Institute for Social Development (Nov. 2003), http://www.unrisd.org/80256B3C005BCCF9/(httpAuxPages)/B6020CCE9EBC00FCC1256E550059CB34?OpenDocument.

Beth Givens & Sen. Steve Peace, *A Review of State and Federal Privacy Laws"*, Testimony, California Legislature Joint Task Force On Personal Information And Privacy, Privacy Rights Clearinghouse (1997-2014), https://www.privacyrights.org/ar/jttaskap.htm.

Angela Goodrum, *How to Maneuver in the World of Negative Online Reviews, the Important Ethical Considerations for Attorneys, and Changes Needed to Protect the Legal Profession*, EXPRESSO (2015) http://works.bepress.com/angela_goodrum/5.

D. Gomes & M.J. Silvia. *Modeling Information Persistence On The Web*, Proceedings, VI International Conference On Web Engineering (ICWE06) (2006).

Google Spain SL & Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) & Mario Castejo Gonzales, Opinion, Advocate General Jääskinen To The European Court Of Justice, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62012CC0131:EN:HTML.

Hans Graux, et al. *The Right to be Forgotten in the Internet Era*, Working Paper 11/2012, Interdisciplinary Centre For Law And Ict (ICRI) (2012).

Scott Griffen, *Key Findings: Defences in Defamation Cases*, in Barbara Trionfi, *et al.* eds, Out Of Balance: Defamation Law In The EU, Report For The International Press Institute (10 Mar. 2015), http://www.freemedia.at/ecpm/defamation-law-report.html.

Kuan Hon et al., *The Problem Of 'Personal Data' In Cloud Computing – What Information Is Regulated?* Paper, Centre For Commercial Law Studies, Queen Mary University of London (2011).

Michael Hallsworth *et al.*, *Policy Making In The Real World: Evidence And Analysis*, Report of the Institute For Government (Apr. 2011).

Chris Hoofnagle, et al., *Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection of Data About their Online Activities*, Paper, Berkeley Consumer Privacy Survey (8 Oct., 2012), http://ssrn.com/abstract=2152135.

How The NSA's Domestic Spying Program Works', Report, Electronic Frontier Foundation, https://www.eff.org/nsa-spying/how-it-works.

Human Rights Committee (ICCPR) Concluding Observations On The Fourth Periodic Report Of The United States Of America, CCPR/C/USA/CO/4 (23 Apr. 2014).

IACHR, Report On The Compatibility Of "Desacato" Laws With The American Convention On Human Rights, OEA/Ser. L/V/II.88, doc. 9 rev., 17 February 1995, 197-212.

Interconnection and Interoperability, Background Brief, International Telecommunications Union (ITU), (3-14 Dec. 2012), http://www.itu.int/en/wcit-12/Documents/WCIT-background-brief4.pdf.

International Mechanisms For Promoting Freedom Of Expression, Joint Declaration, United Nations Special Rapporteur On Freedom Of Opinion And Expression, The OSCE Representative On Freedom Of The Media And The OAS Special Rapporteur On

Freedom Of Expression' (2002), http://www.oas.org/en/iachr/expression/showarticle.asp?artID=87&lID=1.

Internet Of Things: Privacy And Security In A Connected World, Report, FTC (Jan. 2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Internet Policy Task Force, Commercial Data Privacy And Innovation In The Internet Economy: A Dynamic Policy Framework, Policy Report, Us Department Of Commerce (2010).

Internet Technology Explained: Hosting, Caching, And Mirroring, Background Paper, Inter-American Commission On Human Rights, (Nov. 1999) http://www.eurim.org.uk/activities/netgov/9911paperinternettech.pdf.

M. Ito et al., Living And Learning With New Media: Summary Of Findings From The Digital Youth Project, (2008) Report on Digital Media and Learning, The John D And Catherine T. Macarthur Foundation, Chicago, http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

The Judiciary And The Media, European Networks of Councils for the Judiciary http://www.encj.eu/index.php?option=com_content&view=category&layout=blog&id=21&Itemid=241&lang=en.

Keith Kirkpatrick, *Technology Confounds the Judges*, 57 Communications Of The Acm, 27 (May 2014), http://cacm.acm.org/magazines/2014/5/174343-technology-confounds-the-courts/fulltext.

Paulan Korenhof, *Forgetting In Bits And Pieces: An Exploration Of The 'Right To Be Forgotten' As Implementation Of 'Forgetting' In Online Memory Processes'*, Working Paper No. 4, Tilburg Institute For Law, Technology, And Society (2013), http://www.ssrn.com/abstract=2326475.

Douwe Korff & Ian Brown, *Final Report Of The Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments*, Report, Eu Commission, Justice, Freedom And Security (20 Jan. 2010) http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

Neelie Kroes, *Why we need a sound Do-Not-Track standard for privacy online*, EUROPA.EU, (11 Mar. 2014), http://ec.europa.eu/archives/commission_2010-2014/kroes/en/blog/donottrack.html;

James A. Lewis, *Internet Governance: Inevitable Transitions*, Paper, Centre For International Governance Innovation (CIGI) (Oct. 2013) http://www.cigionline.org/sites/default/files/no4.pdf.

The Leveson Inquiry Into The Culture Practices And Ethics Of The Press, UK Government National Archives, http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/wp-content/uploads/2011/11/Witness-Statement-of-Max-Mosley.pdf.

Patrick Macklem, *Rybna 9, Praha 1: Restitution and Memory in International Human Rights Law*, University of Toronto, Public Law Research Paper No. 04-12; and NYU Law Centre for Human Rights & Global Justice No. 11 (2004) http://ssrn.com/abstract=617022.

Mary Madden et al., *Teens, Social Media, And Privacy'* Report, Pew Research Parent/Teen Privacy (21 May 2013) http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

Aleecia McDonald & Jon Peha, *Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature*, Paper, Tracking Position Working Group, http://ssrn.com/abstract=1993133 (2011).

Hugh Miller, *The Presentation of Self in Electronic Life: Goffman on the Internet*, Conference Paper, Embodied Knowledge And Virtual Space Conference, University of London (June 1995).

MIZUKO ITO *et al.*, *Living And Learning With New Media: Summary Of Findings From The Digital Youth Project*, John D and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, 9-10 (2008), http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

Gordon E. Moore, *Cramming more components onto integrated circuits*, ELECTRONICS MAGAZINE, 4 (1965).

65 Million Need Not Apply: The Case for Reforming Criminal Background Checks For Employment, The National Employment Law Project, 2 (Ma. 2011), http://www.nelp.org/page/-/65_Million_Need_Not_Apply.pdf.

Online Privacy, Report, European Commission (13 June 2014), http://ec.europa.eu/digital-agenda/en/online-privacy.

Opinion 1/2010 On The Concepts Of 'Controller' And 'Processor", Article 29, Data protection Working Party, Document 169, adopted 16 February 2010, 25 http://ec.europa.eu/justice/data-protection/index_en.htm.

David G. Post, *Personal Jurisdiction on the Internet: An Outline for the Perplexed*, Paper, Temple U. L. Sch. Cyberspace Law Institute (1998).

Privacy Impact Assessment-002 Automated Biometric Identification System (IDENT) Publication, US Department Of Homeland Security (DHS/NPPD) (7 Dec. 2012) http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident.

Progress On EU Data Protection Reform Now Irreversible Following European Parliament Vote, Memorandum 14/186, European Commission (12 Mar. 2014) http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

Proposal For A Council Recommendation Concerning The Protection Of Minors And Human Dignity In Audiovisual And Information Services", Opinion of the Economic and Social Committee, European Commission OJC 214 (10 July 1998).

Propositions of Modernization, The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, ETS 108 Preamble.

P*rotecting Consumer Privacy In An Era Of Rapid Change*, Report, Federal Trade Commission (December 2010), http://www.ftc.gov/opa/2010/12/privacyreport/shtm.

Public Knowledge About Science And Technology, in PUBLIC ATTITUDES AND UNDERSTANDING, Chapter 7, Us National Science Foundation, (2004) http://www.nsf.gov/statistics/seind04/c7/c7s2.htm#note29.

Recommendations for the Technical Implementation of the Art of the E-Privacy Directive, European Union Agency For Network And Information Security (ENISA) (2011), https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn.

Viviane Reding, *The Upcoming Data Protection Reform For The European Union*, 1 INT'L DATA PRIV. L., 3.

Vivian Reding, *Data Protection Day 2014: Full Speed On EU Data Protection Reform*, Memorandum, European Commission (7 Jan. 2014), http://europa.eu/rapid/press-release_MEMO-14-60_en.htm.

Frank Le Rue, *Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression*, Un Council On Human Rights, 17th Sess. agenda item 3, 28-59, UN Doc./A/HRC/17/27 (2011) 28-59.

Safe Harbor Privacy Principles, U.S. DEP'T OF COMMERCE (21 July 2000), www.export.gov/safeharbor/SH_Privacy.asp.

Scheff v. Bock, Digital Media Law Project, http://www.dmlp.org/threats/scheff-v-bock.

Peter Sepulveda-Sandoval, *Digital Shelters*, Poster Presentation, CAST01: Living in Mixed Realities Conference, 21-22 Sept. 2001, Bonn Germany.

Shailendra Palvia, *et al.*, *Advertising Globally on the Internet: New Paradigm or Old Wine in New Bottle*, Paper 112, AMCIS 1999 Proceedings, (1999), http://aisel.aisnet.org/amcis1999/112).

6 New Facts About Facebook, Pew Research (3 Feb 2014), http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/.

Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False, Press release, Federal Trade Commission (8 May 2014), http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

Sarah Spiekermann, *About the Idea of Man in Systems Design: an enlightened version of the Internet of Things?* SSRN (2014), http://ssrn.com/abstract=2046497.

Supplementary Explanatory Memorandum To The Revised OECD Privacy Guidelines, OEDC (2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

Survey Questions: Facebook, Survey, Pew Research http://www.pewresearch.org/files/2014/01/Survey-Questions_Facebook.pdf.

Texas Defamation Law, Digital Media Law Project, http://www.dmlp.org/legal-guide/texas-defamation-law.

Virginia Defamation Law, Digital Media Law Project, *http://www.dmlp.org/legal-guide/virginia-defamation-law.*

Eugene Volokh & Donald L Falk, *First Amendment Protection For Search Engine Search Results*, White Paper, Google Inc. (20 Apr. 2012) http://www.volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf.

Stephen J. Ward, *Digital Media Ethics*, Paper, University Of Wisconsin Center For Journalism Ethics, http://ethics.journalism.wisc.edu/resources/digital-media-ethics/#difficult.

We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online, Press Release, White House Office Of The Press Secretary (23 Feb. 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

David Weinberger, *Tagging and Why it Matters*, Research Publication No. 2005-07, Berkman Center For Internet & Society, http://ssrn/com/abstract=870594.

Wire Service Defence, Digital Media Law Project, http://www.dmlp.org/legal-guide/wire-service-defense.

David Wright, et al., *Are the OECD guidelines at 30 showing their age?* 54 COMM. ACM, 119 (February 2011).

WSIS +10 Statement on the Implementation of WSIS Outcomes, ITU 12 (2014), http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf.

Yahoo's Default = a Personalized Experience, Yahoo Privacy Team Policy Paper (30 April 2014), http://yahoopolicy.tumblr.com/post/84363620568/yahoos-default-a-personalized-experience.

Jonathan Zittrain, *Be Careful What You Ask for: Reconciling a Global Internet and Local Law*, Paper, Harvard Law School (2003), http://ssrn.com/abstract=395300.

K News Magazine, Videos

Leila Abboud, *France calls for EU to regulate Web giants to counter dominance*, REUTERS (19 Sept. 2013) http://www.reuters.com/article/2013/09/19/us-france-eu-webgiants-idUSBRE98I14E20130919.

Elise Ackerman. *Google and Facebook Ignore "Do Not Track" Requests, Claim they confuse Consumers*, FORBES (2 Feb. 2013), http://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/.

Agence French Presse-in-Paris, "French writer details Strauss-Kahn Affair," CHINA DAILY (23 Feb. 2013), http://www.chinadaily.com.cn/cndy/2013-02/23/content_16250243.htm.

Jason St. Amand, *Was Ellen's Liza Minnelli Joke Transphobic*? EDGE SAN FRAN. (3 Mar. 2014), http://www.edgesanfrancisco.com/entertainment/celebrities/news//156105/was_ellen's_liza_minnelli_joke_transphobic?

Meg Leta Ambrose. "A Digital Dark Age and the Right to be Forgotten." 17 J. INTERNET L. (2013) 1, http://explore.georgetown.edu/publications/index.cfm?Action=View&DocumentID=72116.

Julia Angwin & Jennifer Valentino-Devries, *Google Tracked iPhones, Bypassing Apple Browser Privacy Settings*, WSJ (17 Feb. 2012), http://online.wsj.com/articles/.

Charles Arthur, *2015 will be the year wearable tech gets under the skin*, GUARDIAN (9 Dec. 2014), http://www.theguardian.com/technology/2014/dec/09/wearable-tech-health-smartwatches-apple.

Kimberly Atkins, *Technical difficulties at the Supreme Court*, DC DICTA (19 Apr. 2010), http://lawyersusaonline.com/dcdicta/2010/04/19/technical-difficulties-at-the-supreme-court-2/.

Genevieve Balmaker, *Erasing the Record, One Story at a Time*, QUILL (July/August 2013), http://digitaleditions.walsworthprintgroup.com/display_article.php?id=1475867&_width=/.

James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What you Say)*, WIRED (15 Mar. 2013), http://www.wired.com/2012/03/ff_nsadatacenter/all/.

Bank of Scotland Fax Blunder leads to Fine, BBC NEWS (5 Aug. 2013), http://www.bbc.co.uk/news/business-23572574.

Brian Barrett, *Twitter Finally Banned Revenge Porn. Now How to Enforce it?* WIRED (12 Mar. 2015), http://www.wired.com/2015/03/twitter-bans-revenge-porn/.

David Bauder, *Ellen DeGeneres' selfie a landmark social media moment*, ASS. PRESS & CTV NEWS (4 Mar. 2014), http://www.ctvnews.ca/entertainment/ellen-degeneres-oscar-selfie-a-landmark-social-media-moment-1.1712937.

A Brief History of the Internet & Related Networks, INTERNET SOCIETY, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet-related-networks.

California lawmakers pass bill to protect kids from paparazzi, ABCNEWS (7 Sept. 2013), http://abclocal.go.com/kabc/story?id=9240150

Celestine Bohlen, *Drawing the Line on Privacy*, NYTIMES, Europe Edition (15 Mar. 2013), http://www.nytimes.com/2013/03/16/world/europe/16iht-letter16.html?ref=dominiquestrausskahn&_r=0>.

Matthew Braga, *Google Glass raises significant privacy issues*, FIN. POST (19 June 2013), FP11.

Joseph Brean, *'You are already a suspect': Surveillance becoming 'routine' as it evolves into a social media pastime*, NAT. POST (3 June 2013), http://news.nationalpost.com/2013/06/03/surveillance-becoming-intensive-and-routine-as-it-evolves-into-a-social-media-pastime/.

Kevin J. O'Brien, *Fact Finder to European Court Backs Google in a Spanish Privacy Battle*, NYTIMES (25 June 2013) http://www.nytimes.com/2013/06/26/business/global/european-court-opinion-favors-google-in-privacy-battle.html.

Grant Buckler, *Breaking a story with the speed of social media*, GLOBE AND MAIL (1 Dec. 2011) http://www.theglobeandmail.com/report-on-business/small-business/sb-digital/biz-categories-technology/breaking-a-story-with-the-speed-of-social-media/article4179877/.

Vannevar Bush, *As We May Think*, ATLANTIC (1 July 1945) http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/.

David Carr, *When Truth Survives Free Speech*, NYTIMES, B1 (Dec. 11, 2011).

James G. Carr, *A Judge's Guide to Protecting Your Reputation*, 36, TRUTH OR CONSEQUENCES, American Bar Association, 26 (2014) http://www.jstor.org/discover/10.2307/29760783?uid=3739448&uid=2129&uid=2&uid=70&uid=3737720&uid=4&sid=21104468347941.

Tom De Castella, & Kayle Rath, *Prism and privacy: What could they know about me?* BBC NEWS MAGAZINE (12 June 2013), http://www.bbc.com/news/magazine-22853432.

Pere Simon Castellano, *The Right to be Forgotten under European law: a Constitutional Debate*, 6 LEX ELECTRONICA, 1 (2012).

Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (5 Nov. 2006), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

Christopher Chabris, *The Current with Anna Marie Tremonte*, CBC RADIO (11 Feb. 2015), http://www.cbc.ca/thecurrent/podcasts/.

Brian X. Chen, *I-Phone or I-Spy: Feds, Lawyers tackle mobile piracy*, WIRED (12 Apr. 2011), wired.com/gadgetlab/2011/04/iphone-ispy.

Danielle Keats Citron, *Free Speech Does Not Protect Cyberharassment*, NYTIMES (19 Aug. 2014), http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls/free-speech-does-not-protect-cyberharassment.

Kate Connelly, *Right to erasure protects people's freedom to forget the past, says expert*, GUARDIAN (4 Apr. 2013), http://www.guardian.co.uk/technology/2013/apr/04/right-erasure-protects-freedom-forget-past.

Courtney libel suit shows landmark 1964 case relevant in digital age, CBC NEWS (8 Mar. 2014), http://www.cbc.ca/news/technology/courtney-love-libel-suit-shows-landmark-1964-case-relevant-in-digital-age-1.2565330.

Lewis Dartnell, *The digital black hole: will it delete your memories?* GUARDIAN (16 Feb. 2015) http://www.theguardian.com/technology/2015/feb/16/digital-black-hole-delete-memories-information-lost-google-vint-cerf).

Bill Davidow, *The Internet Is the Greatest Legal Facilitator of Inequality in Human History*, ATLANTIC (28 Jan. 2014), http://www.theatlantic.com/business/archive/2014/01/the-internet-is-the-greatest-legal-facilitator-of-inequality-in-human-history/283422/.

Wendy Davis, *AOL Won't Honor Do-Not-Track Requests*, MEDIAPOST (19 Aug. 2014), http://www.mediapost.com/publications/article/232394/aol-wont-honor-do-not-track-requests.html.

Cotton Delo, *Facebook to Use Web Browsing History for Ad Targetting*, DIGITAL ADVERTISING AGE (12 June 2014), http://adage.com/article/digital/facebook-web-browsing-history-ad-targeting/293656/.

Caitlin Dewey, *Internet consensus: DeGeneres' Lisa Minnelli joke 'mean', 'transphobic'*, WASH. POST (3 Mar. 2014), http://www.washingtonpost.com/blogs/style-blog/wp/2014/03/02/internet-consensus-degeneres-liza-minnelli-joke-mean-transphobic/.

Nancy Dillon, *Courtney Love claims ignorance of Twitter in libel suit*, NY DAILY NEWS (23 Jan. 2014), http://www.nydailynews.com/entertainment/gossip/courtney-love-claims-reckless-oath-article-1.1588397.

Kevin Dolak, *Rehtaeh Parsons Suicide: Justice Minister Revisiting Alleged Rape Case*, ABCNEWS (11 Apr. 2013), http://abcnews.go.com/International/rehtaeh-parsons-suicide-justice-minister-revisiting-alleged-rape/story?id=18924592.

Don't complain about your teachers in France, ARS TECH. (6 Mar. 2008), http://arstechnica.com/civis/viewtopic.php?f=23&t=137941. See also *French website Note2Be.com closed by court order*, 6 EDRI-GRAM (12 Mar. 2008), http://history.edri.org/book/export/html/1431,

Sady Doyle, *Outing online sexual predators is a sensationalist stopgap*, GUARDIAN (17 Oct. 2012), http://www.theguardian.com/commentisfree/2012/oct/17/outing-online-sexual-predators-gawker-anonymous.

Peggy Drexler, *The Importance of being Fluent in the Language of texting*, FORBES (23 June 2014), http://www.forbes.com/sites/peggydrexler/2014/06/23/the-importance-of-being-fluent-in-the-language-of-texting/.

David Drummond, *We need to talk about the right to be forgotten*, GUARDIAN (10 July 2014), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate

William H. Dutton, *The EU's Right to be Forgotten and Why it is Wrong*, Oxford Internet Institute (2010), http://www.oii.ox.ac.uk/people/?id=1.

Editorial: Should US Adopt the Right to be Forgotten Electronic Data Collection Raises Privacy Issues, CONN. L. TRIB. (3 Oct. 2014), http://www.ctlawtribune.com/id=1202672292749/Editorial-Should-US-Adopt-the-Right-to-Be-Forgotten-Electronic-Data-Collection-Raises-Privacy-Issues?slreturn=20141014150309.

Pamela Enger, *Brian Williams explains how he 'misremembered' the Iraq helicopter incident*, BUSINESS INSIDER (19 Feb. 2015), http://www.businessinsider.com/brian-williams-explains-how-he-misremembered-the-iraq-helicopter-incident-2015-2.

European Court backs man against France over anti-Sarkozy insult, BBC ONLINE (14 Mar. 2013), http://www.bbc.co.uk/news/world-europe-21783922.

Joseph Fewsmith, *Assessing social stability on the eve of the 17th Party Congress*, CHINA LEADERSHIP MONITOR, 1 (2007)

Julia Fioretti, *EU mulls conferring binding powers on body of data privacy regulators*, REUTERS (14 Nov. 2014), http://www.reuters.com/article/2014/11/14/us-eu-dataprotection-idUSKCN0IY1LR20141114.

Max Fisher, *Yes, it really was a crime in France to insult the president until this week. Here's why*, WASH. POST (26 July 2013) http://www.washingtonpost.com/blogs/worldviews/wp/2013/07/26/yes-it-really-was-a-crime-in-france-to-insult-the-president-until-this-week-heres-why/.

Four in five regard Internet access as a fundamental right: global poll, BBC NEWS (8 Mar. 2010) http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf.

Sam Frizell, *Courtney Love's Bittersweet Twitter Update*, TIME (8 Apr. 2014) http://time.com/54276/courtney-love-twitter-defamation-lawsuits/.

Sandra Fulton, *One Year Later, Consumers are Still Waiting on a Do Not Track Standard*, ACLU.ORG (24 Apr. 2013), https://www.aclu.org/blog/technology-and-liberty/one-year-later-consumers-are-still-waiting-do-not-track-standard.

Gawker Cracks $200,000, CBC RADIO (28 May 2013) http://www.cbc.ca/q/2013/05/28/gawker-cracks-200000/.

Samuel Gibbs, *Twitter bans revenge porn in user policy sharpening*, GUARDIAN (12 Mar. 2015), http://www.theguardian.com/technology/2015/mar/12/twitter-bans-revenge-porn-in-user-policy-sharpening.

Francois Gilbert, *A Legal Analysis of the updated EU General Data Protection Regulation*, ITLAW.com, http://searchcloudsecurity.techtarget.com/tip/A-legal-analysis-of-the-updated-EU-General-Data-Protection-Regulation.

Mark Glaser, *Top 10 Media Stories of 2010: WikiLeaks, Facebook, iPad Mania*, PBS (30 Dec. 2010) http://www.pbs.org/mediashift/2010/12/top-10-media-stories-of-2010-wikileaks-facebook-ipad-mania364.

Sam Gustin, *Is Broadband Internet Access a Public Utility?* TIME (9 Jan. 2013), http://business.time.com/2013/01/09/is-broadband-internet-access-a-public-utility/.

Josh Halliday, *Max Mosley sues Google in France and Germany over 'orgy' search results*, GUARDIAN (25 Nov. 2011), http://www.theguardian.com/media/2011/nov/25/max-mosley-google-france-germany.

Sam Hananel, *Supreme Court considers extent of free speech over Internet*, PBS (30 NOV. 2014), http://www.pbs.org/newshour/rundown/supreme-court-case-considers-extent-free-speech-internet/.

Mark Hansen, *NJ Woman Can Be Prosecuted Over Fake Facebook Profile, Judge Rules*, ABA J. (4 Nov, 2011) http://www.abajournal.com/news/article/woman_can_be_prosecuted_over_fake_facebook_profile_judge_rules/.

Michael Harris, *Book review: 'The Internet is Not the Answer' by Andrew Keen*, WASH. POST (2 Jan. 2015) http://www.washingtonpost.com/opinions/book-review-the-internet-is-not-the-answer-by-andrew-keen/2015/01/02/8627999a-7973-11e4-9a27-6fdbc612bff8_story.html.

Miguel Helft, & David Barbosa, *Google Shuts China Site in Dispute over Censorship*, NYTIMES (22 Mar. 2010) http://www.nytimes.com/2010/03/23/technology/23google.html?_r=0.

John Hendel, *Why Journalists Shouldn't Fear Europe's 'Right to be Forgotten'* ATLANTIC (25 Jan. 2012), http://www.theatlantic.com/technology.archive/2012/01/why-journalists-shouldn't-fear-europe's-right-to-be-forgotten.html.

Nick Hopkins, *UK Gathering secret intelligence via covert NSA operation*, GUARDIAN (7 June 2013), http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism.

Michael Horowitz, *What does your IP address say about you*? CNET (15 Sept. 2008) http://www.cnet.com/news/what-does-your-ip-address-say-about-you/.

Lawrence Hurley, *In U.S., when high-tech meets high court, high jinks ensue*, REUTERS (9 May 2014), http://www.reuters.com/article/2014/05/09/us-usa-court-tech-idUSBREA480N420140509.

In Search of Second Chances, NYTIMES (1 June 2014) SR-10.

Is there a right to be forgotten on Google? LE MONDE (27 Feb. 2013), http://www.aedh.eu/plugins/fckeditor/pdf.

Nicolas Jackson, *United Nations Declares Internet Access a Basic Human Right*, ATLANTIC (3 June 2011), http://www.theatlantic.com/technology/archive/2011/06/united-nations-declares-internet-access-a-basic-human-right/239911/.

Eliana Johnson, *Is Brian Williams Invincible?* NATIONAL REV. ONLINE (6 Feb. 2015), http://www.nationalreview.com/article/398118/brian-williams-invincible-eliana-johnson.

Michiko Kakutani, *Watched by the Web: Surveillance is Reborn*, NYTIMES Book Review of Viktor Mayer-Schonberger & Kenneth Cukier, BIG DATA, (10 June 2013) http://www.nytimes.com/2013/06/11/books/big-data-by-viktor-mayer-schonberger-and-kenneth-cukier.html?pagewanted=all&_r=0.

Leo Kelion, *Q&A: NSA's Prism Internet surveillance scheme*, BBC NEWS (25 June 2013), http://www.bbc.com/news/technology-23027764.

Key Findings: Civil Defamation, FREE MEDIA http://www.freemedia.at/ecpm/key-findings/civil-defamation-laws.html.

Bill Keller, *Erasing History*, NYTIMES (28 Apr. 2013), http://www.nytimes.com/2013/04/29/opinion/keller-erasing-history.html?_r=0.

Bert-Jap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice*, 8 SCRIPTed, 229-256 (2011), http://dx.doi.org/10.2139/ssrn.1986719.

David Kravets, *Supreme Court Rejects Student Social Media Case* WIRED (1 Jan. 2012), http://www.wired.com/2012/01/scotus-student-social-media/.

Jill Lepore, *The Prism: Privacy in an age of publicity*, NEW YORKER (24 June 2013) 36.

Lawrence Lessig, *Against Transparency*, NEW REPUBLIC (20 Oct. 2009), http://www.newrepublic.com/article/books-and-arts/against-transparency.

Lawrence Lessig, CODE V2 (2006), http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Leveson Inquiry: Max Mosley describes outrage at story, BBC NEWS (24 Nov. 2011), http://www.bbc.com/news/uk-15874015.

J.C.R. Licklider, *Man-Computer Symbiosis*, IRE Transactions On Human Factors In Electronics (March 1960), http://groups.csail.mit.edu/medg/people/psz/Licklider.html.

The Long March to Privacy", ECONOMIST (12 Jan. 2006) http://www.economist.com/node/5389362.

Edmund H. Mahony, *U.S. Supreme court Declines review of off-campus, online student speech case*, HARTFORD COURANT, (Oct. 31 2011)

Mike Masnick, *Google Works Out Deal Concerning 'Jew' Suggestions In France*, TECHDIRT (5 July 2012), https://www.techdirt.com/articles/20120705/03231519585/google-works-out-deal-concerning-jew-suggestions-france.shtml.

Mike Masnick, *Judge Who Doesn't Understand Technology Says Wi-Fi is Not Radio Communication,"* TECHDIRT (1 July 2011),

https://www.techdirt.com/blog/wireless/articles/20110701/12225114934/judge-who-doesnt-understand-technology-says-Wi-Fi-is-not-radio-communication.shtml.

Jeff Mason, *Hillary Clinton calls Bosnia snipe story a mistake*, REUTERS (25 Mar. 2008), http://www.reuters.com/article/2008/03/26/us-usa-politics-clinton-idUSN2540811420080326.

Tom McCarthy, *Brian Williams' reports on Katrina called into question by New Orleans residents*, GUARDIAN (6 Feb. 2015), http://www.theguardian.com/world/2015/feb/06/brian-williams-hurricane-katrina-new-orleans-residents.

Vinay Menon, *Give Williams the benefit of the doubt: Menon*, TORONTO STAR (9 Feb. 2015), http://www.thestar.com/entertainment/2015/02/09/give-williams-the-benefit-of-the-doubt-menon.html.

Robinson Meyer, *U.S. Court: Bloggers Are Journalists*, ATLANTIC (21 Jan. 2014) http://www.theatlantic.com/technology/archive/2014/01/us-court-bloggers-are-journalists/283225/.

Zach Minors, *How bickering and greed neutered the 'Do Not Track' privacy initiative*, PC WORLD (22 May 2014) http://www.pcworld.com/article/2158220/do-not-track-oh-what-the-heck-go-ahead.html.

Bradley Mitchell, *What is the difference between bits and bites*, ABOUT.COM (18 June 2014) http://compnetworking.about.com/cs/basicnetworking/f/bitsandbytes.html.

Mosley wins court case over orgy, BBC NEWS (24 July 2008) http://news.bbc.co.uk/2/hi/7523034.stm.

Andrew Murray, *Looking Back at the Law of the Horse: Why Cyberlaw and the Rule of Law are Important*, 10 SCRIPTed 310 (2013), http://script-ed.org/?p=1157.

Daniel Nasaw, *Tale of coming under sniper fire mistaken, Clinton admits*, GUARDIAN (25 Mar. 2008), http://www.theguardian.com/world/2008/mar/25/uselections2008.hillaryclinton

John Naughton, *The Internet of Things: It's a Really Big Deal*, GUARDIAN (14 June 2014) www.theguardian.com/technology/2014/jun/15/networker-internet-of-things-john-naughton-hacking.

Jared Newman, *Dubai detectives will use Goggle Glass facial recognition tech to ID criminals*, PCWORLD (3 Oct. 2014), http://www.pcworld.com/article/2691615/dubai-detectives-will-use-google-glass-facial-recognition-tech-to-id-criminals.html.

No clear cut outcome for Supreme Court's Internet free speech case, CBS NEWS (1 DEC. 2014), http://www.cbsnews.com/news/no-clear-cut-outcome-for-supreme-courts-internet-free-speech-case/.

Number of Internet Users Worldwide Approaching 3 Billion, VOICE OF AMERICA NEWS (6 May 2014) http://www.voanews.com/content/number-of-internet-users-worldwide-approaching-3-billion/1908968.html.

Kevin J. O'Brien, *Fact Finder to European Court Backs Google in a Spanish Privacy Battle*, NYTIMES (25 June 2013) http://www.nytimes.com/2013/06/26/business/global/european-court-opinion-favors-google-in-privacy-battle.html.

Kevin O'Brien, *Privacy Advocates and Advertisers at Odds Over Web Tracking*, NYTIMES (4 Oct. 2012), http://www.nytimes.com/2012/10/05/technology/privacy-advocates-and-advertisers-at-odds-over-web-tracking.html?pagewanted=all&_r=0.

Laura Olson, *Paparazzi who harass stars' kids face tougher penalties*, CHICAGO SUN-TIMES (25 Sept. 2013), http://www.suntimes.com/news/nation/22779614-418/paparazzi-who-harass-stars-kids-face-tougher-penalties.html.

Alexei Oreskovic, *First Look at the Google+ social network: The Top Secret Demo*, REUTERS (28 June 20111), http://blogs.reuters.com/mediafile/2011/06/28/first-look-at-the-google-plus-social-network-the-top-secret-demo/.

Laura Parker, *Jury awards $11.3M over defamatory Internet posts*, USA TODAY (11 Oct. 2006), http://www.usatoday.com/news/nation/2006-10-10-internet-defamation-case_x.htm.

Nicole Perlroth, *Fake Twitter Followers Become Multimillion-Dollar Business*, NYTIMES (3 Apr. 2013) http://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/?_php=true&_type=blogs&_r=0.

Eric Pfanner, *In Europe, Challenges for Google*, NYTIMES (1 Feb. 2010), http://www.nytimes.com/2010/02/02/technology/companies/02google.html.

Brad Plumer, *Tweets move faster than earthquakes*, WASH. POST (25 Aug. 2011) http://www.washingtonpost.com/blogs/wonkblog/post/tweets-move-faster-than-earthquakes/2011/08/25/gIQA4iWHeJ_blog.html.

Private data, public rules, ECONOMIST (28 Jan. 2012), http://www.economist.com/node/21543489;

Reflecting on Learning Theories and Instructing, IDT2ME on *WORDPRESS* (23 Apr. 2011), http://idt2me.wordpress.com/2012/04/23/reflecting-on-learning-theories-and-instructing/#respond.

David Reid, *France ponders right-to-forget law*, BBC (8 Jan. 2010), http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm;

Right of reply as a private law entity, René David (ed.) INTERNATIONAL ENCYCLOPEDIA OF COMPARATIVE LAW, 163, 164 (1986).

The Right to be Forgotten': US Lobbyists Face Off with EU on Data Privacy Proposal, SPIEGEL INTERNATIONAL (17 Oct. 2012), http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html.

James Risen, Eric Lichtblau. *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, NYTIMES (16 Dec. 2005), http://www.pulitzer.org/archives/7037.

Jon Ronson, *Do Twitter users have the right to ruin someone's life?* GUARDIAN (3 Mar. 2015)

Jeffrey Rosen, *The Web Means the End of Forgetting*, NYTIMES (21 July 2010), www.nytimes.com/2010/07/25privacy-t2.html?pagewanted=all&_r=0.

Rebecca Rosen, *Armed with Facebook 'Likes" Alone, Researchers Can tell Your Race Gender and Sexual Orientation'*, ATLANTIC (12 Mar. 2013), http://www.theatlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-and-sexual-orientation/273963/.

Rebecca J. Rosen, *Google Refuses to Remove Police-Brutality Videos*, ATLANTIC (27 Oct. 2011) http://www.theatlantic.com/technology/archive/2011/10/google-refuses-to-remove-police-brutality-videos/247462/.

Susan Rohwer, *Kristin Bell and Dax Shepard's scheme to sideline aggressive paparazzi*, LATIMES (5 Mar. 2014), http://www.latimes.com/opinion/opinion-la/la-ol-kristen-bell-dax-shepard-aggressive-paparazzi-20140305-story.html#page=1.
Eric Savitz, *How Do-Not-Track could kill the Internet Start-up Economy*, FORBES (24 Apr. 2013) http://www.forbes.com/sites/ciocentral/2012/04/24/how-do-not-track-could-kill-the-internet-startup-economy.

Mark Scott, *E.U. Debates Which Nation Will regulate Web Privacy*, NYTIMES (26 May 2014), http://www.nytimes.com/2014/05/27/technology/with-european-data-rules-come-a-need-for-a-cop.html?_r=0.

Somini Sengupta, *No U. S. Action, So States Move on Privacy Law*, NYTIMES (30 Oct. 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?pagewanted=all&_r=0;\.
Connor Simpson, *A Year With Google Glass Will Turn You Into an Obnoxious Monster*, ATLANTIC (30 Dec. 2013), http://www.theatlantic.com/national/archive/2013/12/google-glass-still-weird-will-probably-make-you-hate-your-phone/356579/.

Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets'*, NYTIMES (9 Nov. 2013) http://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html?_r=0.

Suzanne Smalley, *Hillary: Made-Up Memories?* NEWSWEEK (24 Mar. 2008), (reporting that Clinton had told the story "for many years, gradually adding embellishment and changing details. Perhaps she may have actually come to believe it."

Stijn Smet, *The Right to Reputation under the European Convention on Human Rights* STRASBOURGOBSERVERS.COM (1 Nov. 2010), http://strasbourgobservers.com/2010/11/01/the-right-to-reputation-under-the-european-convention-on-human-rights/.

Judith Soal, *Barack Obama and David Cameron pose for selfie with Danish PM*, GUARDIAN (11 Dec. 2013) http://www.theguardian.com/world/2013/dec/10/nelson-mandela-world-leaders-selfie.

Bailey Socha and Barbara Eber-Schmid, *Defining New Media Isn't Easy*, NEW MEDIA.ORG, http://www.newmedia.org/what-is-new-media.html.

Daniel J. Solove, *Justice Scalia's Dossier: Interesting Issues about Privacy and Ethics*, CONCURRING OPINIONS (29 Apr. 2009), http://www.concurringopinions.com/archives/2009/04/justice_scalias_2.html.

Ian Sparks, *'Schoolboy' French journalists annoy White House staff by taking selfies while covering Francois Hollande's U.S. visit*, DAILY MAIL (13 Feb. 2014), http://www.dailymal.co.uk/news/article-2558620/.

Spotlight: Department of Homeland Security, DHS Newsletter (12 Aug. 2012), http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_SLP_12-111_Aug12.pdf.

Tom Spring, *Dawn of a Facebook Democracy? Users Invited to Shape Site's Policies*, PCWORLD (26 Feb. 2009), http://www.pcworld.com/article/160314/facebook.html.

George Stark, *Ellen DeGeneres labelled 'transphobic' after Oscars joke that suggested Liza Minnelli looked like a drag performer falls flat*, DAILY MAIL (4 Mar. 2014), http://www.dailymail.co.uk/tvshowbiz/article-2573116/Ellen-DeGeneres-labelled-transphobic-Oscars-joke-Liza-Minnelli-looked-like-drag-performer-falls-flat-Twitter.html.

Jonathan Stempel. *LinkedIn must face customer lawsuit over e-mail addresses*, GLOBE AND MAIL (13 June 2014), http://www.theglobeandmail.com/report-on-business/linkedin-must-face-customer-lawsuit-over-e-mail-addresses/article19159821/.

C. Stocker, *Puny Punishment for Goliath: Google Case Exposes Weak US Data Privacy Laws*, SPIEGEL INTERNATIONAL (10 Aug. 2012),

http://www.spiegel.de/international/europe/americans-may-have-to-wait-for-europe-for-better-data-protection-a-849372.html.

Jennifer Stoddard, Thirty Years After the OECD Guidelines, Report to OEDC Working Party on Information Security and Privacy (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf.

Adam Tanner, *Finally You'll Get To See The Secret Consumer Dossier They Have On You*, FORBES (25 June 2013) http://www.forbes.com/sites/adamtanner/2013/06/25/finally-youll-get-to-see-the-secret-consumer-dossier-they-have-on-you/.

Adam Tanner, *Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study*, FORBES (25 Apr. 2013) http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/.

Adam Tanner, *Company That Knows What Drugs Everyone Takes is Going Public*, FORBES (6 Jan. 2014) http://www.forbes.com/sites/adamtanner/2014/01/06/company-that-knows-what-drugs-everyone-takes-going-public/.

Teachers in websites closure call, BBC ONLINE (1 Aug. 2007), http://news.bbc.co.uk/2/hi/uk_news/scotland/6925444.stm.

Travis J. Tritten, *In his words: Brian Williams' interview with Stars and Stripes*, STRIPES.COM (9 Feb. 2015), http://www.stripes.com/news/us/in-his-words-brian-williams-interview-with-stars-and-stripes-1.328590#.VNkOaJw3TBo.twitter.

Jennifer Valentino-Devries, *Google to Pay $22.5 Million in FTC Privacy Settlement*, WSJ (9 Aug. 2012) http://online.wsj.com/news/articles/SB10000872396390443404004577579232818727246.

Tanzina Vega, *Code Known as Flash Cookies Raises Privacy Concerns*, NYTIMES (20 Sept. 2010), http://www.nytimes.com/2010/09/21/technology/21cookie.html?_r=3&.

Michael Venables, *The EU's 'Right to be Forgotten': What Data Protections are We Missing in the US?*' FORBES (8 Mar. 2013) http://www.forbes.com/sites/michaelvenables/2013/03/08/the-ecs-right-to-be-forgotten-proposal-in-the-u-s/.

Stephen M. Walt, *The Myth of American Exceptionalism*, FOREIGN POL. (Oct. 11, 2011), http://www.foreignpolicy.com/articles/2011/10/11/the_myth_of_american_exceptionalism?page=full.

Matt Warman, *Online anonymity: impossible after four phone calls*, TELEGRAPH (25 Mar. 2013), http://www.telegraph.co.uk/technology/news/9952841/Online-anonymity-impossible-after-four-phone-calls.html.

Sara M. Watson, *Data Doppelgangers and the Uncanny Valley of Personalization*, ATLANTIC (16 June 2014) http://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780/.

'What are cookies?' KNOWLEDGE BASE, Indiana University https://kb.iu.edu/d/agwm.

Susan White, *EF Cultural Travel v. Explorica: The Protection of Confidential Commercial Information in the American and Canadian Contexts*, CAN. J. L. & TECH. (JULY 2004), http://www.carters.ca/pub/article/ip/sew0704.pdf.

Christopher Williams, *Bank of Scotland fined for 'unforgivable' fax blunder*, TELEGRAPH (5 Aug. 2013) http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10223435/Bank-of-Scotland-fined-for-unforgivable-fax-blunder.html.

Mark Wilson, *Even Goggle's Own Developers Won't Be Seen Wearing Google Glass*, FAST COMPANY (16 May 2013), http://www.fastcodesign.com/1672609/even-google-s-own-developers-wont-be-seen-wearing-google-glass.

Tim Worstall, *Microsoft Sticks with Do Not Track Default: and Boy are the Advertisers Angry*, FORBES (10 Mar. 2012), http://www.forbes.com/sites/timworstall/2012/10/03/microsoft-sticks-with-do-not-track-default-and-boy-are-the-advertisers-angry/.

Jenna Wortham, *Facebook responds to anger over proposed Instagram changes*, NYTIMES (18 Dec. 2012), http://www.nytimes.com/2012/12/19/technology/facebook-responds-to-anger-over-proposed-instagram-changes.html?_r=0.

Anthony York, *Halle Berry, Jennifer Garner to urge crackdown on paparazzi*, LATIMES (Aug. 13, 2013), http://www.latimes.com/local/political/la-me-pc-halle-berry-jennifer-garner-paparazzi-crackdown-20130813,0,3748682.story#ax/.

Jonathan Zittrain, *Build Internet Communitarian Memory* (nd) OPEN DEMOCRACY ONLINE, http://www.opendemocracy.net/jonathan-zittrain-tony-curzon-price/build-internet-communitarian-memory.

Jonathan Zittrain, *The Right to be Forgotten Ruling Leaves Nagging Doubts*, Financial Times (13 July 2014).

l Websites, Blogs, Videos

AB370: California's "Do Not Track" Law, Cooley Llp, http://www.cooley.com/ab370-californias-do-not-track-law.

Rajab Ali, *Technological Neutrality*, 14 Lex Elect. (Rev. du Centre de recherché en droid public) (Fall 2009), http://www.lex-electronica.org/docs/articles_236.pdf.

Alasdair Allan & Pete Warden, *Got an iPhone or 3G iPad? Apple is recording your moves'*, Blog (20 Apr. 2011), http://radar.oreilly.com/2011/04/apple-location-tracking.html.

Meg Ambrose, *EU Right to be Forgotten Case: The Honorable Google Handed both Burden and Boon* (19 May 2014), http://playgiarizing.com.

Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (22 June 2009).

Timothy Garton Ash, *Reputation and Defamation*, Free Speech Debate Blog, http://freespeechdebate.idebate.org/principle/principle-9/reputation-and-defamation.

Emily C. Barbour, *The SPEECH Act: The Federal Response to 'Libel Tourism'*, CRS Report For Congress 7-5700 (16 Sept. 2010), *http://www.fas.org/sgp/crs/misc/R41417.pdf.*

John Perry Barlow, *Declaration of the Independence of Cyberspace*, (8 Feb. 1996) as reproduced by the Electronic Frontier Foundation, https://projects.eff.org/~barlow/Declaration-Final.html.

Nickolaus Bauer, *'Insult law' commonplace in many countries*, Mail & Guardian, (15 Nov 2012), http://mg.co.za/article/2012-11-15-insult-law-nothing-to-do-with-free-speech.

Belleville Woman Charged over Facebook Identity Theft, Facecrooks, (27 Oct. 2011) http://facecrooks.com/Internet-Safety-Privacy/Belleville-Woman-Charged-over-Facebook-Identity-Theft.html/.

Susan Benesch, *Troll Wrastling for Beginners: Data-Driven Methods to Decrease Hatred Online*, Video by Berkman Center for Internet & Society (25 Mar. 2014) http://cyber.law.harvard.edu/events/luncheon/2014/03/benesch.

Richard Beaumont, *Do Not Track Gets Thumbs Down from EU*, Cookie Collective (12 June 2014), http://www.cookielaw.org/blog/2014/6/12/do-not-track-gets-thumbs-down-from-eu/.

Christopher Boyd, *January 1st Instagram Profile Deletion Hoax*, MALWAREBYTES (30 Dec. 2014), https://blog.malwarebytes.org/fraud-scam/2014/12/january-1st-instagram-profile-deletion-hoax/.

dana boyd, *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*, 14 CONVERGENCE 13, 13-14 (2008), http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf

Dana boyd, *Quitting Facebook is pointless: challenging them to do better is not*, Apophenia Blog (23 May 2010) http://www.zephoria.org/thoughts/archives/2010/05/23/quitting-facebook-is-pointless-challenging-them-to-do-better-is-not.html/comment-page-1.

G. Burton, *You have NO privacy. Get over it*, COMPUTING.CO.UK (4 Oct. 2010) http://www.computing.co.uk/ctg/feature/2214593/-you-have-no-privacy-get-over-it#ixzz2WDkuGJJH.

Pamela Chelin, *Courtney Love found not liable in Landmark Twitter Defamation Case*, (24 Jan. 2014) http://www.spin.com/articles/courtney-love-twitter-defamation-lawsuit-verdict-guilty/.

Brian X. Chen, *Iphone or iSpy? Feds, Lawyers Tackle Mobile Privacy'*, WIRED (12 April 2011), http://www.wired.com/gadgetlab/2011/04/iphone-ispy.

Civil Defamation: Undermining Free Expression, ARTICLE 19, http://www.article19.org/data/files/pdfs/publications/civil-defamation.pdf.

Bret S. Cohen, *Unsurprisingly, U.S. Court rules that cloud provider must produce data stored abroad*, IT.CAN (13 Aug. 2014), citing Winston Maxwell & Christopher Wolf, A Global Reality: Governmental Access To Data In The Cloud (2012), http://www.lexology.com/library/detail.aspx?g=44f61e94-d679-4bbc-aa18-6d9bfe7be39f&utm_source=Lexology+Daily+Newsfeed/.

Michael V. Copeland, *Texting isn't Writing; it's Fingered Speech'*, WIRED (1 Mar. 2013) http://www.wired.com/2013/03/texting-isnt-writing-its-fingered-speech/.

Court of Justice of the European Union, Europa.Ca, http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm.

Dominic Crossley, *Case Law: Hamburg District Court: Max Mosley v Google Inc., Google go down (again, this time) in Hamburg* INFORRM'S BLOG (5 Feb. 2014), https://inforrm.wordpress.com/2014/02/05/case-law-hamburg-district-court-max-mosley-v-google-inc-google-go-down-again-this-time-in-hamburg-dominic-crossley/.

Dominic Crossley, *Google go down in Paris: how did it come to this?* INFORRM'S BLOG (13 Nov. 2013), https://inforrm.wordpress.com/?s=Mosley+v+Google+France.

B. Davidson, *Bank of Scotland Receives 75K GBP Penalty Notice for Misdirected Faxes*, PRIVACY ADVISOR (IAPP) (27 Aug. 2013) https://www.privacyassociation.org/publications/uk_bank_of_scotland_receives_75k_gbp_penalty_notice_for_misdirected_faxes.

John Dean, *Why Chief Justice Roberts Dared Not Overturn President Obama's Healthcare Plan*, Verdict: Constitutional Law (29 JUNE 2012), http://verdict.justia.com/2012/06/29/why-chief-justice-roberts-dared-not-overturn-president-obamas-healthcare-plan (29 JUNE 2012).

Defamation and Privacy, Taylor Wessing (2013). http://www.taylorwessing.com/uploads/tx_siruplawyermanagement/IP_Defamation_and_privacy.en.pdf

Deindividuation, 8 June 2014) http://changingminds.org/techniques/techniques.htm.

Chrisanthos Dellarocas, *The Digitization of work-of-Mouth: Promise and Challenges of Online Feedback Mechanisms*, 49 MGMT SC. 1407 (Oct. 2003).

Andrew Dickenson, *Privacy and Personality Rights in the Rome II Regime – Not Again?* CONFLICTOFLAWS.NET (19 July 2010) http://conflictoflaws.net/2010/privacy-and-personality-rights-in-the-rome-ii-regime-not-again/.

Daniel Dimov, *Mobile Phone Spying Software: Legality, Symptoms, and Removal*, Infosec Inst. (8 Mar. 2013), http://resources.infosecinstitute.com/mobile-phone-spying-software-legality-symptoms-and-removal/.

Data Protection and Privacy Laws, Privacy International, https://www.privacyinternational.org/issues/data-protection-and-privacy-laws.

Documents: Rob Ford did 'Hezza', Tries to Buy Crack Video with a Car, GAWKER (12 Apr. 2013) http://gawker.com/documents-rob-ford-did-hezza-tried-to-buy-crack-vid-1476729771.

'Domain Name', WEBOPEDIA, http://www.webopedia.com/TERM/D/domain_name.html.

Laura Drell, *4 Ways Behavioral Targeting is Changing the Web*, MASHABLE (26 Apr. 2011), http://mashable.com/2011/04/26/behavioral-targeting/.

Kelly D. Dubacki, *Renewed Calls for Finalization of EU Data Protection Regulation by 2015*, First Advantage (29 September 2014), http://www.fadv.com/company/blog/entry/articletype/articleview/articleid/144/renewed-calls-for-finalization-of-eu-data-protection-regulation-by-2015.aspx.

Duquesne cancels Rivera over 'selfie', Duquesne Student Media (15 Sept. 2013), http://www.duqsm.com/duquesne-cancels-rivera-over-selfie/.

William H. Dutton, *The EU's Right to be Forgotten and Why it is Wrong*, Oxford Internet Institute Blog at http://www.oii.ox.ac.uk/people/?id=1.

William Dutton, *Programming to Forget*, R*eview of* Delete: The Virtue Of Forgetting In The Digital Age By Viktor Mayer-Schonberger, 327 SCIENCE (19 Mar. 2010) 1456.

Denisa Dzunkova, *Storyful Helps News Organizations Monitor Social Media*, PBS MEDIASHIFT http://www.pbs.org/mediashift/2013/02/storyful-helps-news-organizations-monitor-social-media036/.

Nicholas Eddy, *Improper Exercise of Personal Jurisdiction in Blumenthal v. Drudge* CYBER.LAW.HARVARD (1998), https://cyber.law.harvard.edu/fallsem98/final_papers/Eddy.html.

Alicia Eler, *Why People Have Fake Facebook Profiles*, READWRITE (23 Jan. 2012), http://readwrite.com/2012/01/23/why_people_have_fake_facebook_profiles#awesm=~oGOrS2OC.

Loek Essers, *Google Video Trial To Continue To Italian Supreme Court*, PCWORLD (Apr. 17, 2013), http://www.pcworld.com/article/2035387/google-video-trial-to-continue-to-italian-supreme-court.html.
European Data Protection Supervisor, *Data protection legislation Q&A* http://secure.edps.europa.eu/EDPSWEB/edps/EDPS/.../QA/QA2.

EU Advocate General considers if Google is subject to European privacy laws, Linklaters (18 July 2013), http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-News-18-July-2013/Pages/EU-Advocate-General-considers-Google-subject-European-privacy-laws.aspx#sthash.zHRLWRwk.dpuf.

EU defamation laws fall dramatically short of international standards, IPI report indicates, International Press Institute (July 17, 2014), http://www.freemedia.at/newssview/article/eu-defamation-laws-fall-dramatically-short-of-international-standards-ipi-report-indicates.html.

EU Institutions and Other Bodies, Europa.Eu, http://europa.eu/about-eu/institutions-bodies/index_en.htm.

The EU Single Market: E-Commerce Directive, European Commission (20 Mar. 2014), http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm.

Jordan Fabian, *Chairman to Justices: "Have Either of Y'all Ever Considered Tweeting or Twitting?"* Hillicon Valley: The Hill's Tech. Blog (May 21, 2010), http://thehill.com/blogs/hillicon-valley/technology/99209-/ (quoting Justice Scalia's testimony at a House judiciary subcommittee hearing).

Facebook claims to become 'biggest stadium in the world' for World Cup', RTCOM (9 June 2014), http://rt.com/business/164704-facebook-world-cup-stadium/.

Facebook, *Statement of Rights and Responsibilities*, (15 Nov. 2013) https://www.facebook.com/legal/terms.

Federal Supreme Court: Google Liable for Defamatory Autocomplete Search Terms, DISPUTE RESOLUTION IN GERMANY BLOG (14 May 2013), http://www.disputeresolutiongermany.com/2013/05/federal-supreme-court-google-liable-for-defamatory-autocomplete-search-results/

Greg Finn, *RIP Technorati Blog Search & Rankings: The Once Popular Blog Tools Have been Sunset*, Blog (26 June 2014) searchengineland.com/rip-technorati-blog-search-rankings-popular-blog.

Kelly Fiveash, *Mosley thrash'n'tickle vid case against Google opens in Hamburg: Ex F1 chief's clip campaign flogging a -erm-dead horse?* REGISTER (28 Sept. 2012), http://www.theregister.co.uk/2012/09/28/max_mosley_sues_google_over_hosting_orgy_vid/.

Flash Eurobarometer 359: *Attitudes on Data Protection and Electronic Identity in the European Union*, EUROPA.EU (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, Blog, (9 Mar. 2011) http://peterfleischer.blogspot.ca/2011/03/foggy-thinking-about-right-to-oblivion.html.

Forums, WEX LEGAL DICTIONARY, Legal Information Institute, Cornell University Law School, https://www.law.cornell.edu/wex/forums.

Future Internet Scenarios, Internet Society, http://www.internetsociety.org/internet/how-its-evolving/future-scenarios

Michael Geist, *Cyberlaw shows its true colours*, Blog (6 September 2001), http://www.michaelgeist.ca/resc/html_bkup/sept62001.html

Getting it right, but in a "false light", REPORTERS COMM. FR. PRESS, http://www.rcfp.org/browse-media-law-resources/digital-journalists-legal-guide/getting-it-right-false-light-0.

Glass and Facial Recognition, GOOGLE PLUS (31 May 2013), https://plus.google.com/+GoogleGlass/posts/fAe5vo4ZEcE.

Google refuses US request to take down video, ALAKHBAR (16 Sept 2012), http://english.al-akhbar.com/node/12230.

Gotham City (Gameplay Discussion), SONY.COM (13 Dec. 2013) https://forums.station.sony.com/dcuo/index.php?threads/taking-insults-too-far.182043/?\.

Adam Greenberg, *Telecommunications provider Swisscom investigations stolen data*, SC MAGAZINE (18 Sept. 2013) http://www.scmagazine.com/telecommunications-provider-swisscom-investigates-stolen-data/article/312177/.

Scott Griffin *et al.*, *Out Of Balance: Defamation Law In The European Union And Its Effect On Press Freedom*, International Press Institute, http://www.freemedia.at/fileadmin/uploads/pics/Out_of_Balance_OnDefamation_IPIJuly2014.pdf

Mike Harris, *The EU's commitment to free expression: libel and privacy*, INDEX ON CENSORSHIP (Jan. 2, 2014), http://www.indexoncensorship.org/2014/01/eus-commitments-free-expression-libel-privacy/

Peter Harris, *The three things that employers look for the most in your social media profiles*, WORKPOLIS (22 Feb. 2014) http://www.workopolis.com/content/advice/article/the-three-things-that-employers-want-to-find-out-about-you-online/.

What is Hash Function? TECHNOPEDIA http://www.techopedia.com/definition/19744/hash-function.

Anna Helhoski, *Crack Cocaine Raid Nets Two*, GREENWICH DAILY VOICE, (25 Aug. 2010) http://greenwich.dailyvoice.com/news/crack-cocaine-raid-nets-two.

Steve Henn, *Facebook's Online Speech Rules Keep Users on a Tight Leash*, NPR (3 Apr. 2013), http://www.npr.org/blogs/alltechconsidered/2013/04/03/176147408/facebooks-online-speech-rules-keep-users-on-a-tight-leash.

John Herrman, *What are Flash Cookies and How Can You Stop Them*? POP. MECH. (23 September 2010) http://www.popularmechanics.com/technology/how-to/computer-security/what-are-flash-cookies-and-how-can-you-stop-them.

Highlight – Meet New People, Find and Connect with Friends Nearby, ITUNES PREVIEW (9 July 2014), https://itunes.apple.com/us/app/highlight/id441534409?ls=1&mt=8.

Margaret Honey, *Old Wine in New Bottles: Ethics and the Internet*, Center for Children and Technology (1 August 1999), OWNB_webethics99.pdf.

How to Reveal a Fake Facebook Account, WIKIHOW, http://www.wikihow.com/Reveal-a-Fake-Facebook-Account.

Internet Pioneers, http://www.ibiblio.org/pioneers/licklider.html

Internet Regulation: Not neutral about net neutrality, ECONOMIST (15 Nov. 2014), http://www.economist.com/news/business/21632511-barack-obama-jumps-debate-about-how-regulate-broadband-not-neutral-about-net (indicating US President Obama supports the public utility idea).

Jobvite's 6th Annual Social Recruiting Survey, JOBVITE (13 June 2014) http://web.jobvite.com/Q313_SocialRecruitingSurvey_LandingPage.html.

Francisco J. Rivera Juaristi, *U.S. Exceptionalism and the Strengthening Process of the Inter-American Human Rights System*, HUMAN RIGHTS BRIEF (2012), http://www.wcl.american.edu/hrbrief/20/2juaristi.pdf.

Judge Rules on Temporary Injunction, SWISSCOM (14 Feb. 2014) http://www.swisscom.ch/en/about/medien/press-releases/2014/02/20140213_MM_superprovisorische_Verfuegung.html.

Judgment of the Federal Supreme Court on Google Street View: Decisions on the processing of personal data, Confederation Suisse, http://www.edoeb.admin.ch/datenschutz/00683/00690/00694/01109/index.html/.

Olga Kharif, *The Cookies You Can't Crumble*, BLOOMBERG BUSINESS WEEK (21 Aug. 2014), http://www.businessweek.com/articles/2014-08-21/facebook-google-go-beyond-cookies-to-reap-data-for-advertisers.

Marshall Kirkpatrick, *Facebook Management Has Lost its Grip on Reality*, READWRITE.COM, (26 Feb. 2009), http://readwrite.com/2009/02/26/facebook_managment_has_lost_it.

John Krumm *et al.*, *User Generated Content*, Pervasive Computing (Oct. – Dec. 2008), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4653465.

The Legislative Process, United States House Of Representatives, http://www.house.gov/content/learn/legislative_process/.

Timothy B. Lee, *The Supreme Court's technical cluelessness makes them better justices*, VOX (15 October 2014), http://www.vox.com/2014/4/23/5644154/the-supreme-courts-technical-cluelessness-makes-them-better-justices

Michael Liedtke, *Google grabs personal info off of Wi-Fi networks*, YAHOO FINANCE, (May 28, 2010), http://web.archive.org/web/20100518095457/finance.yahoo.com/news/Google-grabs-personal-info-apf-2162289993.html?x=0.

Tim Lowles, *Max Mosley wins his case against Google in France*, in Defamation and Reputation Management Press Release, Collyer Bristow (6 Nov. 2013) http://www.collyerbristow.com/Default.aspx?sID=90&cID=1214&ctID=43&lID=0.

Vyshali Manivannan, *When 'Trolling' Becomes an Umbrella Term*, NYTIMES (19 Aug. 2014), http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls/when-trolling-becomes-an-umbrella-term.

Farhad Manjoo, *Yes, Ill Matty You*, SLATE (July 2010), http://www.slate.com/articles/technology/technology/2010/07/yes_ill_matty_you.2.html

CC Mark, *On outing in the sci blogging community*, SCIENTOPIA (21 Jan. 2014) http://scientopia.org/blogs/goodmath/2014/01/21/on-outing-in-the-sciblogging-community/.

Florian Martin-Bariteau, *The Mosley/Google Case: Why Privacy Can Not be Argued*, DROITDU.NET (17 Nov. 2013), http://droitdu.net/2013/11/the-mosley-case-paris-why-privacy-can-not-be-argued-for-notice-and-stay-down/.

Alice E. Marwick, Diego Murgia-Diaz, & John G. Palfrey, *Youth, Privacy and Reputation (Literature Review)* Berkman Center Research Publication, 10-29. (2010).

Mike Masnick, Streisand Suing Over Environmentalist's Aerial Shots Of Her Home, TECHDIRT (1 June 2003), https://www.techdirt.com/articles/20030601/1910207.shtml.

Al McConnell, *Speaking Ill: an analysis of posthumous defamation*, https://alistairmcconnell.wordpress.com/essays/speaking-ill-an-analysis-of-posthumous-defamation/

Simon J. McMenemy, *Further Delay to the EU Data Protection Regulation*, Ogletree Deakins blog (4 Mar. 2015) http://blog.ogletreedeakins.com/further-delay-to-the-eu-data-protection-regulation/#sthash.u9gs6RSF.dpuf.

George Herbert Mead (1863-1931), INTERNET ENCYCLOPEDIA OF PHILOSOPHY, www.iep.utm.edu/mead/#5h3a.

David Meyer, *Google loses autocomplete defamation case in Italy*, ZDNET (Apr. 5, 2011), http://www.zdnet.com/google-loses-autocomplete-defamation-case-in-italy-3040092392/.

Justin Mitchell, *Making Photo Tagging Easier'*, FACEBOOK (30 June 2011) https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130.

Daniel Miessler, *The Difference Between Encoding, Encryption and Hashing*, Blog, http://danielmiessler.com/study/encoding_encryption_hashing/.

Ellen Nakashima, *Judge orders Microsoft to turn over data held overseas*, WASH. POST (31 July 2014), available at http://www.washingtonpost.com/world/national-security/judge-orders-microsoft-to-turn-over-data-held-overseas/2014/07/31/b07c4952-18d4-11e4-9e3b-7f2f110c6265_story.html.

Quinn Norton, *iColumn: The Dangers of Deep Packet Inspection*, MAXIMUMPC (2 May 2013), www.maximumpc.com/article/columns/Deep_Packet_Instpectoin_2013.

9th Circuit Reverses in Yahoo v. Juan Carlos Perez, *Facebook tweaks Beacon again, Zuckerberg apologizes*, COMPUTERWORLD, (7 Dec. 2007), http://www.computerworlduk.com/news/security/6592/facebook-tweaks-beacon-again-zuckerberg-apologises/.

OEDC Privacy Guidelines, OECD.ORG (2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OEDC Cross Border Privacy Law Enforcement, OEDC.ORG (2007), http://www.oecd.org/document/25/0,2340,en_2649_37441_37571993_1_1_1_37441,00.html.

Soren Oman, *Implementing Data Protection in Law*, Stockholm Institute For Scandinavian Law, http://www.scandinavianlaw.se/pdf/47-18.pdf.

1.5 million monitored cyber attacks in the United States in 2013, IBM Data Breach Statistics, (April 2014), http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/.

Online Defamation Law, Electronic Frontier Foundation, https://www.eff.org/issues/bloggers/legal/liability/defamation.

Tim O'Reilly, *IoTH: The Internet of Things and Humans*, Oreilly.Com YouTube video, http://radar.oreilly.com/2014/04/ioth-the-internet-of-things-and-humans.html

Ian Paul, *Facebook Photo Tagging: A Privacy Guide*, PCWORLD (9 June 2011) http://www.pcworld.com/article/229870/Facebook_Photo_Tagging_A_Privacy_Guide.html.

Monica Pinto, *The Role of the Inter-American Commission and the Court of Human Rights in the Protection of Human Rights: Achievements and Contemporary Challenges*, Human Rights Brief (2012), http://www.wcl.american.edu/hrbrief/20/2pinto.pdf.

Damon Poeter, *Creepy 'Girls Around Me' App Delivers a Wake-Up Call*, PCWORLD (30 Mar. 2012), http://www.pcmag.com/article2/0,2817,2402457,00.asp.

Population Growth, POPULATION INSTITUTE http://www.populationinstitute.org/?gclid=CjwKEAiAh7WkBRCQj/.

Thomas Porter, *The Perils of Deep Packet Inspection*, SECURITY FOCUS (1 Nov. 2005) http://www.bandwidthco.com/sf_whitepapers/firewalls/The%20Perils%20of%20Deep%20Packet%20Inspection.pdf.

Eric Posner, *We all have the right to be forgotten*, SLATE (14 May 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html

Tim Powers, *Expungement: what does it mean for your record?* Denton County Criminal Defense Lawyer (9 Oct. 2012), http://www.timpowers.com/dentonCriminalDefense/2012/expungement-what-does-it-mean-for-your-record.html.

Private data, public rules, ECONOMIST (28 Jan. 2012), http://www.economist.com/node/21543489.

Emil Protalinski, *Facebook: 5-6% of accounts are fake*, ZDNET (8 Mar. 2012) http://www.zdnet.com/blog/facebook/facebook-5-6-of-accounts-are-fake/10167.

Emil Protalinski, *How to spot a fake Facebook profile (infographic)*, ZDNET (4 Feb. 2012), http://www.zdnet.com/blog/facebook/how-to-spot-a-fake-facebook-profile-infographic/8580.

Public Unredacted Klien Declaration, Electronic Frontier Foundation (28 Mar. 2006), https://www.eff.org/node/55051.

RATE MY PROFESSOR, Terms & Conditions, http://www.ratemyprofessors.com/TermsOfUse_us.jsp>.

Mike Reicher, *State law allows kids to clean their digital past"*, ORANGE COUNTY REGISTER (24 SEPT. 2013), http://www.ocregister.com/articles/online-527862-companies-law.html.

David Reid, *France ponders right-to-forget law*, BBC (8 Jan. 2010), http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm; *Is there a right to be forgotten on Google?* LE MONDE (27 February 2013), http://www.aedh.eu/plugins/fckeditor/pdf.

Padraig Reilly, *European ruling spells trouble for online comment*, INDEX ON CENSORSHIP (10 Oct. 2013), http://www.indexoncensorship.org/2013/10/european-ruling-spells-trouble-online-comment/.

Don Reisninger, *Google: More government takedown requests than ever before*, CNET (25 Apr. 2013) at http://www.cnet.com/news/google-more-government-takedown- requests-than-ever-before/.

Mike Resnick, *Professor Fired for Trashing Colleagues on Professor Ratings Site*, TECHDIRT, 22 Feb. 2006), https://www.techdirt.com/articles/20060222/221239.shtml.

Right of reply as a private law entity, René David (ed.) INT'L ENCYCL. COMP. L. 163 (1986).

'The Right to be Forgotten': US Lobbyists Face Off with EU on Data Privacy Proposal, DER SPIEGEL (17 Oct. 2012), http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html.

Aendrew Rininsland, *Internet censorship listed: how does each country compare?* GUARDIAN (16 Apr. 2012), http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list (indicating which national governments are involved in filtering and the different levels of formal activity).

Heather Rogers, "Is there a right to reputation?" Part 1, INFORRM'S BLOG, (26 Oct. 2010) https://inforrm.wordpress.com/2010/10/26/is-there-a-right-to-reputation-part-1-heather-rogers-qc/.

Jeffrey Rosen, *The Delete Squad: Google, Twitter, and Facebook and the new global battle over the future of free speech* NEW REPUBLIC (29 Apr. 2013), http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules.

Joel Rosenblatt, *Google Won't Face Group E-Mail Privacy Lawsuit: Judge*, BLOOMBERG (19 Mar. 2014) http://www.bloomberg.com/news/2014-03-19/google-won-t-face-group-e-mail-privacy-lawsuit-judge-rules.html.

Ivan Rothman & Philip Zender, *California passes the first "Do-Not-Track" legislation in the US*, ITCAN LEXOLOGY (24 Oct. 2013) http://www.lexology.com/library/detail.aspx?g=a51c3fe0-98b8-4c2d-9035-01e32f2576e2.

Daposh Dutta Roy, *Changing trends in Marketing*, LINKEDIN (2 Sept. 2014), https://www.linkedin.com/today/post/article/20140902140606-616354-changing-trends-in-marketing.

Niri Shan, & Timothy Pinto (eds), *Defamation and privacy law and procedure in England, Germany & France*, Taylor Lessing (Spring 2006), (16 Aug. 2013) http://www.taylorwessing.com/uploads/tx_siruplawyermanagement/IP_Defamation_and_privacy.en.pdf

Marie Shanahan, *Archived Arrest Stories are like Zombies Arising from the Grave*, Marie K. Shanahan Blog (1 Sept. 2013), http://www.mariekshanahan.com/hearst-news-12-and-main-street-connect-defeat-lawsuit-over-archived-arrest-stories/.

Lei Shen & Rebecca Eisner, *New and Proposed US Data Breach Notification laws*, MONDAQ (9 July 2014), http://www.mondaq.com/unitedstates/x/326416/Data+Protection+Privacy/New+and+Proposed+US+Data+Breach+Notification+Laws.

Should the US Adopt the Right to be Forgotten? Video Debate, Berkman Center For Internet & Society At Harvard University (11 Mar. 2015), Http://Intelligencesquaredus.Org/Debates/Past-Debates/Item/1252-The-u-s-should-adopt-the-right-to-be-forgotten-online (featuring Paul Nemitz and Eric Posner arguing for adoption and Jonathan Zittrain and Andrew McLaughlin arguing against.)

Smith, *Facebook Photos: Opt-Out or Tag You're It*, NETWORKWORLD (7 Jan. 2011) http://www.networkworld.com/article/2228269/microsoft-subnet/facebook-photos--opt-out-or-tag-you-re-it.html.

Ian Sparks, *Internet access is a fundamental human right, rules French court*, DAILY MAIL (12 June 2009) http://www.dailymail.co.uk/news/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html.

Joran Spauwen and Jens van den Brink, *Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals*, INFORRM'S BLOG (27 Sept 2014),

State Laws Related to Internet Privacy, National Conference Of State Legislatures (NCSL)(23 Jan. 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

Jonathan Stempel, *Google loses appeal in Street View privacy case*, REUTERS (September 10, 2013), http://www.reuters.com/article/2013/09/10/us-google-streetview-lawsuit-idUSBRE98913D20130910.

Jonathan Stempel, *LinkedIn must face customer lawsuit over e-mail addresses*, GLOBE AND MAIL (13 June 2014) http://www.theglobeandmail.com/report-on-business/linkedin-must-face-customer-lawsuit-over-e-mail-addresses/article19159821/.

Alastair Stevenson, *Right to be Forgotten on the web unworkable, argue data watchdogs*, V3.CO.UK (26 Mar. 2013), http://www.v3.co.uk/v3-uk/news/2257523/right-to-be-forgotten-unworkable-argue-data-watchdogs.

Stop Mattel's 'Hello Barbie' Eavesdropping Doll', Campaign For A Commercial-Free Childhood (CCFC), http://org.salsalabs.com/o/621/p/dia/action3/common/public/?action_KEY=17347.

Danny Sullivan, *How Google Instant's Autocomplete Suggestions Work*, SEARCHENGLINELAND (6 Apr. 2011), http://searchengineland.com/how-google-instant-autocomplete-suggestions-work-62592.

Mark Sullivan, *SXSW Preview: The Year of 'Ambient Social' Apps?* PCWORLD (7 Mar. 2012), http://tech.ca.msn.com/sxsw-preview-the-year-of-ambient-social-apps-1.

Kevin Systrom, *Thank you, and we're listening*, INSTAGRAM blog, http://blog.instagram.com/post/38252135408/thank-you-and-were-listening.

Defamation and Privacy, Taylor Wessing (2013). http://www.taylorwessing.com/uploads/tx_siruplawyermanagement/IP_Defamation_and_privacy.en.pdf

Adam Thierer, *Privacy as an Information Control Regime: the challenges ahead*, TECH. LIB. FRONT (13 Nov. 2010) http://techliberation.com/2010/11/13/privacy-as-an-information-control-regime-the-challenges-ahead/.

Timeline of Computer History, COMPUTERHISTORY, http://www.computerhistory.org/timeline/?category=cmptr.

Hugh Tomlinson, *Privacy and Defamation, Strasbourg blurs the Boundaries*, INFORRM'S BLOG (23 Jan. 2014), https://inforrm.wordpress.com/2014/01/23/privacy-and-defamation-strasbourg-blurs-the-boundaries-hugh-tomlinson-qc/.

Txting is killing language. TED2013, YOUTUBE video (Feb. 2013), http://www.ted.com/talks/john_mcwhorter_txtng_is_killing_language_jk?language=en

United States Privacy Laws, INFORMATION SHIELD, http://www.informationshield.com/usprivacylaws.html.

Vietnam Timeline: 1966, http://www.vietnamgear.com/war1966.aspx

S. Viner, *Social Media Statistics: How College Students are Using Social Networking*, STUDY BREAKS COLLEGE MEDIA (7 Feb. 2014) http://studybreakscollegemedia.com/2014/social-media-statistics-how-college-students-are-using-social-networking/.

Mark Vinall, *EDate Advertising and Martinez*, INFORRM'S BLOG (3 Nov. 2011), http://inforrm.wordpress.com/2011/11/03/case-law-edate-advertising-and-olivier-martinez-mark-vinall/.

Kurt Wagner, *Study finds 77% of College Students use Snapchat Daily*, MASHABLE.COM (24 Feb. 2014) http://mashable.com/2014/02/24/snapchat-study-college-students/.

Rolf H. Weber, *Internet Service Provider Liability: The Swiss Perspective*, JIPITEC 1 (2010) 145.

D. Weinberger, 'Tagging and Why it Matters', Berkman Center Research Publication No. 2005-07, p. 1 as accessed 13 June 2014 at <http://ssrn/com/abstract=870594>.

H.G. Wells, *World Brain: The idea of a Permanent World Encyclopaedia*, Encyclopedie Francaise (Aug. 1937), https://sherlock.ischool.berkeley.edu/wells/world_brain.html

What does IP address stand for? ENG. LANG. TERM., http://www.englishlanguageterminology.org/acronyms-initials-abbreviations/what-does-ip-stand-for.htm.

What is tagging and how does it work?, FACEBOOK (11 June 2014) http://www.facebook.com/help/124970597582337.

What is Timeline review? How do I turn Timeline review on? FACEBOOK http://www.facebook.com/help/168229546579373.

What is the Sarbanes-Oxley Act? Legislative And Governance Fact Sheets (2005), http://www.securit.com/legislative/sarbanesOxley.pdf.

What is Twitter? Twitter Support, https://support.twitter.com/articles/13920-new-user-faqs.

Lance Whitney, *Google grappling with 70,000 'Right to be Forgotten' requests*, CNET (11 July 2014), http://www.cnet.com/news/google-grappling-with-70000-right-to-be-forgotten-requests/.

Wife defends disgraced NFL star Rice after brutal video, YAHOO! SPORTS (9 Sept 2014), http://sports.yahoo.com/news/knockout-victim-wife-defends-rice-firing-214526513--nfl.html.

Christopher Wolf & Bret Cohen, *Pan-America Governmental Access To Data In The Cloud* (17 July 2014), http://www.hoganlovells.com/custom/documents/Pan-American-Governmental-Access-to-Data-in-the-Cloud.pdf.

Lorna Woods, *Google v Spain, landmark CJEU decision in relation to freedom of expression and the right to be forgotten*, INFORRM'S BLOG (13 May 2014), http://inforrm.wordpress.com/2014/05/13/news-google-v-spain-landmark-CJEU-decision-in-relation-to-freedom-of-expression-and-the-right-to-be-forgotten-lorna-woods/.

Colin Woodward, *Estonia, where being wired is a human right*, CHRIST. SCI. MON. (1 July 2003) http://www.csmonitor.com/2003/0701/p07s01-woeu.html.

Working with News Publishers, Google Public Policy Blog, https://groups.google.com/forum/#!forum/public-policy-blog/join.

World's Biggest Data Breaches, Information Is Beautiful pictogram, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

The World Factbook: European Union, Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/geos/ee.html.

Joshua D. Wright, *The Internet of Things: Privacy and Security in a Connected World*, Dissenting Report (27 Jan. 2015), http://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

WSIS +10 Statement on the Implementation of WSIS Outcomes, ITU 12 (2014), http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/36282V2#.pdf.

Ethan Zukerman, *Susan Benesch on dangerous speech and counterspeech*, Blog (2 Mar. 2014) http://www.ethanzuckerman.com/blog/2014/03/25/susan-benesch-on-dangerous-speech-and-counterspeech/.

m Unpublished Manuscripts

Gerlind Berger-Walliser & Franck Valencia, Article, *The Yahoo Case: How to Reconsider State Sovereignty in the Internet Age*, (Dec. 1, 2008), http://ssrn.com/abstract=1927461.

Martin Campbell-Kelly & Daniel Garcia-Swartz, *The History of the Internet: The Missing Narratives*, http://ssrn.com/abstract=867087 (2 Dec. 2005).

Michael A. Einhorn, *Bits, Bots, and Crackups: Life on the Information Superhighway'*, SSRN (11 Oct. 2002) http://ssrn.com/abstract=332700.

Elizabeth Gaffin, *Friending Brandeis: Privacy And Government Surveillance In The Era Of Social Media*, MA Thesis, Naval Post Graduate School (2008).

David Kurt Herold, *An Inter*-nation-*al Internet: China's Contribution to global internet governance?* SSRN, http://ssrn.com/abstract=19227225.

Fredrick Oduol Oduor, *The Evolution of Internet Defamation Law: Will Dow Jones v. Gutnick Survive the International Legal Schisms and Legislative Onslaught?* Paper (2010), http://ssrn.com/abstract=1646168.

Marshall W. Van Alstyne & Erik Brynjolfsson, *Global Village or CyberBalkans: Modeling and Measuring the Integration of Electronic Communities*, MGT. SCI. (forthcoming), http://ssrn.com/abstract=756445

Alan Westin, *Historical Perspectives on Privacy: From the Hebrews and Greeks to the American Republic"*, (unpublished manuscript), as cited in Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. COLL. L. REV., 226.

Kyu Ho Youm, *American "Exceptionalism" in Free Speech Jurisprudence? A Comparison of the U.S. Constitution with the European Convention on Human Rights* (15 July 2006) (unpublished master's thesis in law, Oxford University) as cited in Bruce E.S. Johnson and Kyu Ho Youm, *Commercial Speech and Free Expression: The United States and Europe Compared*, 2 J. INT'L MEDIA & ENT. L. 159, 161 (2013).

APPENDICES

Appendix A — Acronyms

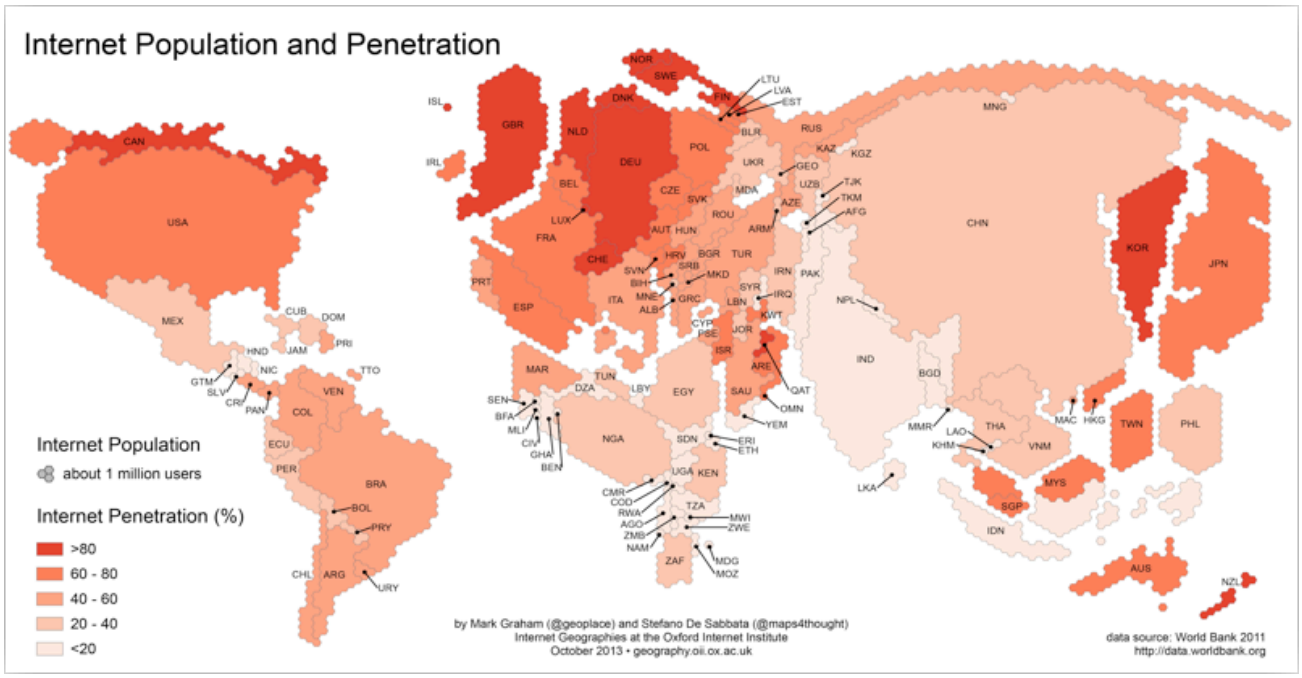
AES	Advanced Encryption Standard
ARPANET	Advanced Research Projects Agency Network
ARPS/DARPA	Defense's Advanced Research Projects Administration
CNIL	National Commission of Informatics and Freedom (Fr)
DIR 2000/31/EC	Directive On Certain Legal Aspects of Information Society Services, In Particular Electronic Commerce, In The Internal Market (E-Commerce Directive)
DIR 2006/24/EC	Directive On The Retention Of Data Generated Or Processed In Connection With The Provision of Publicly Available Electronic Communications Services or of Public Communications Networks (E-Privacy Directive)
DHS	Department of Homeland Security
DoD	Department of Defense (US)
DPA	Data Protection Authorities
DPI	Deep Packet Inspection
ECPA	*Electronic Communications Privacy Act*
EEC	European Economic Community
ECHR	European Convention on Human Rights (formerly 'Charter of Fundamental Human Rights' until Treaty of Lisbon was entered into force 1 December 2009 establishing the EU)
ECtHR	European Court of Human Rights
ENISA	European Network and Information Security Agency
EUDR	Proposed General Data Protection Regulation 2012/0011
FCC	Federal Communications Commission
FRA	Fundamental Rights Agency
FTC	Federal Trade Commission
IACHR	Inter-American Court of Human Rights
ICANN	Internet Corporation for Assigned Names and Numbers
ICJ	International Court of Justice
ICO	Information Commissioner's Office (EU)
ICCPR	International Convention on Civil and Political Rights
ICT	Information and Communications Technology
IDENT	Automated Biometric Identification System
IRA	Internal Revenue Agency
ISP	Internet service providers
ITU	International Telecommunications Union
LICRA	La Ligue Contre Le Racisme et L'Antisemitisme
95 DIRECTIVE	Directive On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (Dir 1995/46EC)
NORDUNET	Nordic Council of Ministers Network
NSA	National Security Agency
NSFNet	National Science Foundation Network

OAS	Organization of American States
OECD	Organization for Economic Cooperation & Development
OSCE	Organization for Security and Co-operation
PII	Personally identifiable information
PRC	People's Republic of China
P2P	Peer-to-peer
SNS	Social Networking Service
TFEU	Treaty on the Functioning of the European Union
UGC	User-generated content
UNHR	Universal Declaration of Human Rights
W3C	World Wide Web Consortium
WSIS	World Summit on the Information Society

Appendix B Maps, Charts, Pictograms

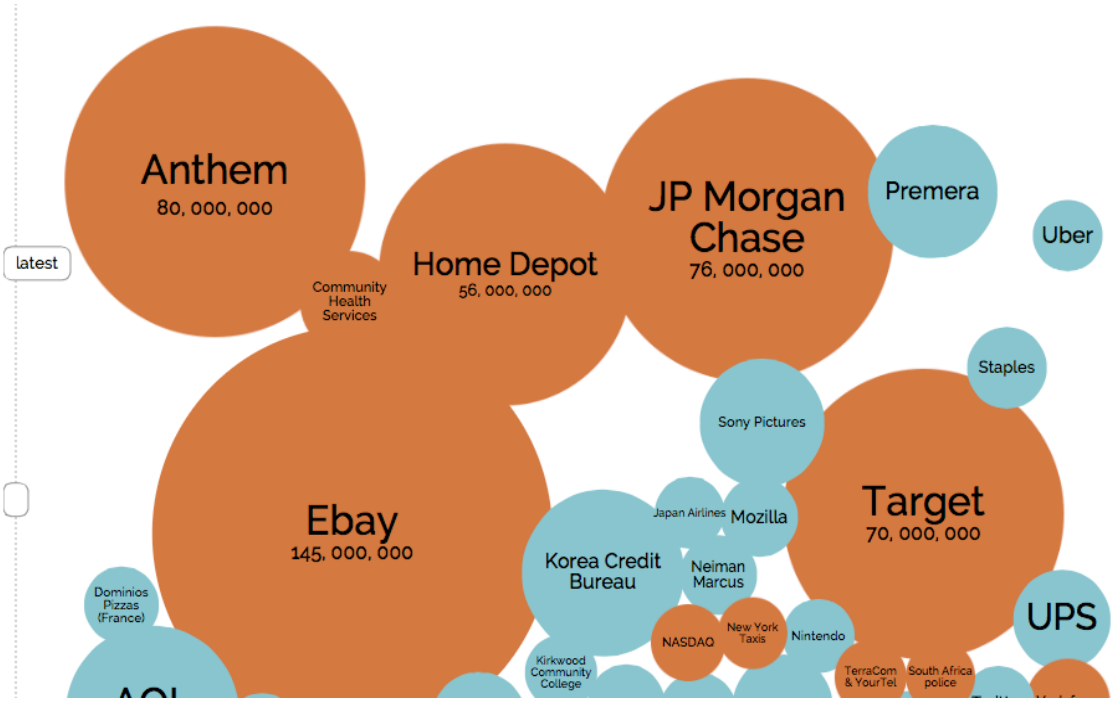
Map 1 Internet Population and Penetration

Source: Mark Graham & Stefano de Sabbato, Oxford Internet Institute using World Bank data. The 2011 data are visualized with a hexagon-shaped cartogram in which the size of each country is drawn based on its population of Internet users.
http://geography.oii.ox.ac.uk/?page=internet-population-and-penetration



Pictogram World's Biggest Data Breaches

Source: *Information is Beautiful* (partial screenshot)
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Map 2 *Out of Balance: Defamation Law in the European Union, a comparative overview for journalists, civil society and policymakers* (January 2015).

Source: International Press Institution
http://www.freemedia.at/fileadmin/user_upload/OOB_Final_Jan2015.pdf.

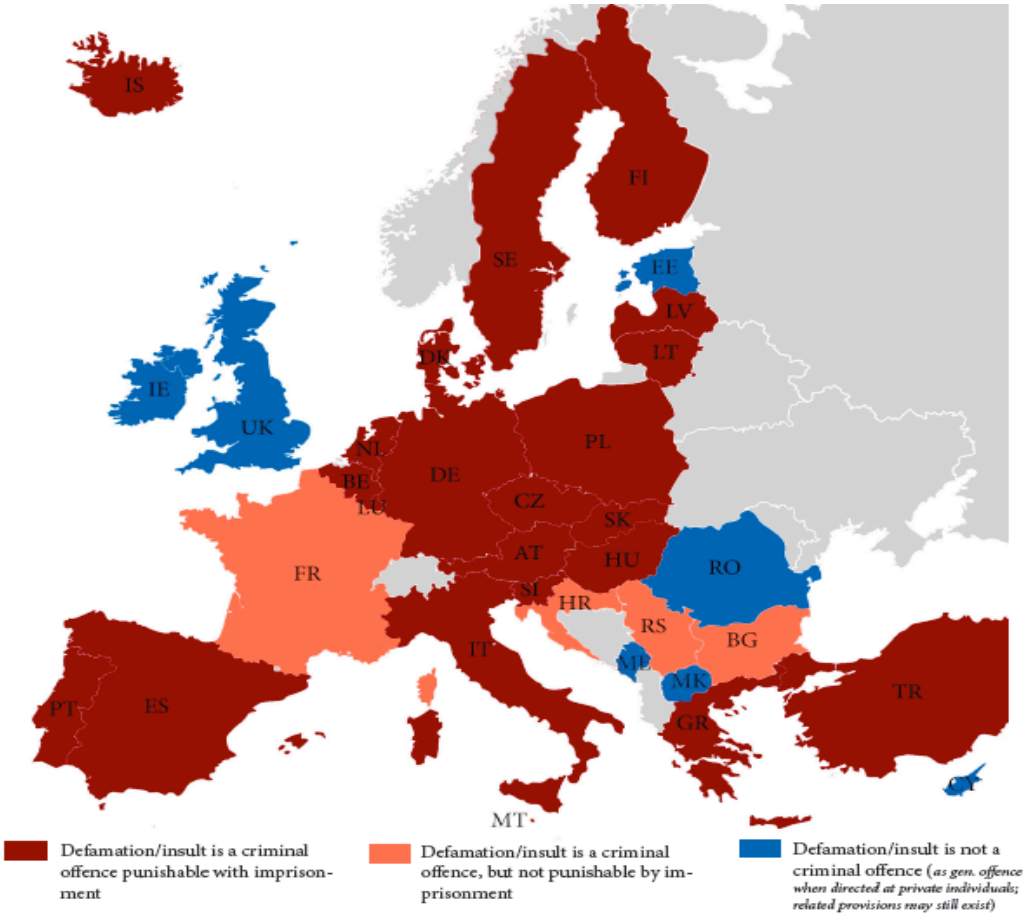


Chart 1 Criminal Offences related to the Protection of Honour, EU Member States and Candidate Countries

Source: *Out of Balance: Defamation Law in the European Union and Its Effect on Press Freedom*, International Press Institute (January 2015) (partial screenshots)
http://www.freemedia.at/fileadmin/user_upload/OOB_Final_Jan2015.pdf.

Chart A: Criminal offences related to the protection of honour, EU member states and candidate countries (Jan. 2015)

Country:	criminal defamation provisions[1]	legal definition	imprisonment as a possible punishment	prison term	other punishment	notes
Austria	insult (*Beleidigung*)	insulting, ridiculing, physically mistreating, or threatening a person with physical mistreatment before at least three other individuals (*CC§115*)	YES	up to 3 months	fine up to 360x daily rate	The daily rate (*Tagessatz*) is a variable rate conditional on a number of factors including the financial situation of the offender. However, the minimum and maximum rates are set at €4 and €5,000, respectively.
AT	defamation (*üble Nachrede*)	accusation of disreputable characteristic or disposition, dishonourable behaviour, or of a behaviour offensive to good morals that may denigrate a person or bring the person into disrepute in the eyes of the public (*CC§111*)	YES	up to 6 months (simple); up to 1 year (public/media)	fine up to 360x daily rate	
AT	false accusation of criminal offence (*Verleumdung*)	putting another person in danger of criminal prosecution by falsely accusing him/her of a criminal offence or of a failure to fulfil an official or professional duty (*CC§297*)	YES	up to 5 years		
Belgium	public insult (*injure/belediging*)	not defined in law; in practice, usually an imprecise allegation that may damage a person's honour (*CC§448*)	YES	8 days to 2 months	fine between €26 and €500	
BE	calumny (*calomnie/laster*)	publicly and maliciously making a precise accusation regarding another person that may damage that person's honour or expose him or her to public contempt without proving the accusation true (*CC§444*)	YES	8 days to 1 year	fine between €26 and €200	

Bulgaria	insult	saying or doing something degrading to the honour and dignity of another in that person's presence (*CC§146*)	NO	N/A	Fine from BGN 1,000 to 3,000; when publicly or via media BGN 3,000 to 10,000	
BG	defamation	making public a disgraceful fact about someone or ascribing to someone a crime (*CC§147*)	NO	N/A	fine from BGN 3,000 to 7,000; when publicly or via media BGN 5,000 to 15,000	
Croatia	insult	insulting another person (*CC§147*)	NO	N/A	fine up to 90x daily rate; fine up to 180x daily rate if committed through media or other public means	The Criminal Code does not specify any exact maximum or minimum limits on the daily rate. Rather, this is fixed by the court, which must consider any aggravating or mitigating circumstances as well as the offender's financial situation.
HR	shaming	presentation or dissemination of facts about a person before a third party that may harm that person's honour or reputation (*CC§148*)	NO	N/A	fine up to 180x daily rate; fine up to 360x daily rate if committed through media or other public means	See above
HR	defamation	knowingly presenting or disseminating untrue facts about a person before a third party that may harm that person's honour or reputation (*CC§149*)	NO	N/A	fine up to 360x daily rate; fine up to 500x daily rate if committed through media or other public means	See above
Cyprus	public vilification	publicly insulting another in such a way that may cause a person to be attacked (*CC§99*)	YES	up to 1 month	Fine up to CYP 75 (€128)	
Czech Republic	defamation (*pomluva*)	communicating false information that can seriously endanger another person's respect among his fellow citizens, in particular damaging his position in employment, and relations with his family, or causing him some other serious harm (*CC§184*)	YES	up to 1 year (general); up to 2 years (media or other public manner)	daily-rate fine, prohibition on practicing profession[2]	General terms: a daily rate is set at between CZK 100 and 50,000, paid between 20 and 730 times
Estonia	none	N/A	N/A	N/A	N/A	N/A
Finland	defamation	spreading false information or a false insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt or disparaging a person in any other manner (*CC§24.9*)	YES	generally no; but up to 2 years if "aggravated", i.e. causing considerable suffering or damage	fine	Criminal fines in Finland are calculated as "day fines", i.e. a set amount multiplied by a number of days between 1 and 120. The amount itself is not subject to any minimum or maximum limits but is rather calculated based on a person's particular financial situation. The Criminal Code states that one-sixtieth of a person's average monthly income is "deemed to be a reasonable amount" for a day fine.
France	insult	any offensive expression, scornful word, or invective that does not contain the accusation of a fact *(L.1881.33)*	NO	N/A	fine up to €12,000	
FR	defamation	any allegation or accusation of a fact that causes an attack on the honour or consideration of a person (*L.1881.32*)	NO	N/A	fine up to €12,000	
FR	(1) non-public defamation (2) non-public insult	(1) non-public defamation toward a person (*CC§R621-1*) (2) unprovoked non-public insult toward a person (*CC§R621-2*)	NO	N/A	(1,2) fine of max. €28 (first degree)	
Germany	insult (*Beleidigung*) *(CC§185)*	not futher defined	YES	up to 1 year (up to 2 years if by means of	fine	German criminal fines are determined on a "daily rate" basis.

Lithuania	libel	spreading of false information about another person that could arouse contempt for this person or humiliate him or undermine trust in him *(CC§154)*	YES	up to 1 year; up to 2 years if allegation of serious crime and committed through media	fine or arrest (temporary detention, up to 90 days)	Fines are calculated in terms of "minimum standard of living" as determined by the court. As both libel and insult are considered to be misdemeanours or minor crimes, the maximum fine in either case will be 100 MSLs
LT	insult	publicly humiliating a person in an abusive manner by an action, word of mouth or in writing *(CC§155)*	YES	arrest only when committed privately; up to 1 year when committed publicly	fine or arrest (temporary detention, up to 90 days)	See above
Luxembourg	public insult (*injure*)	not defined (case law: vague acts or expressions harming reputation) *(CC§448)*	YES	8 days to 2 months	fine of €251 to €5,000	
LU	slander (*calomnie*)	publicly and maliciously making a precise accusation (*l'imputation d'un fait précis*) against another person in order to attack the person's honour or expose him or her to public contempt without proving the accusation *(CC§444)*	YES	8 days to 1 year	fine of €251 to €2,000	
LU	defamation (*diffamation*)	slander, when proof is impossible or legally inadmissible *(CC§444)*	YES	8 days to 1 year	fine of €251 to €2,000	
LU	malicious disclosure (*divulgation méchante*)	slander proven true but committed without any public or private motive but with the sole intention of causing harm *(CC§449)*	YES	8 days to 2 months	fine of €251 to €4,000	
Netherlands	slander (*smaad*)	assault on a person's good name or honour through the imputation of a particular fact with the aim to make the fact public *(CC§261(1))*	YES	up to 6 months	fine up to €8,100 (third degree)	
NL	libel (*smaadschrift*)	defamation that occurs by means of publicly accessible writing or images *(CC§595(2))*	YES	up to 1 year	fine up to €8,100 (third degree)	
NL	intentional libel or slander (*laster*)	defamation or libel committed while knowing the information in question is false *(CC§262(3))*	YES	up to 2 years	fine up to €20,250 (fourth degree), loss of certain civil and political rights	
NL	simple insult (*eenvoudige belediging*)	any intentional not classifiable as slander or libel *(CC§266)*	YES	up to 3 months	fine up to €4,050 (second degree)	
Poland	insult	insulting another person in their presence, or in their absence but with the intention of having the insult reach them *(CC§216)*	YES	generally none; if committed by mass media, up to 1 year	fine, restriction of liberty (community service), or supplementary payment to social cause	See below; [formal insult] even if a defamatory statement is shown to be true, it may still be liable for insult depending on manner presented
PL	defamation	imputing to another person, a group of persons, an institution or organisational unit, conduct or characteristics that may discredit them in the face of public opinion *(CC§212)*	YES	generally none; if committed by mass media, up to 1 year	fine, restriction of liberty (community service), or supplementary payment to social cause	Criminal fines in Poland are set as "daily fines", i.e. the court sets a "daily rate", which is then multiplied by a certain number days (min. 10, max. 540). In setting the daily rate, the court must consider the offender's income and family situation, etc., but the minimum rate is 10 zł (€2.43) and the maximum is 2,000 zł (€485)
Portugal	insult (*injúria*)	alleging a fact or expressing offensive words directly to a person that is/are offensive to	YES	up to 3 months; up to 2 years if committed via the media	fine up to 120 days	For fines, "each day corresponds to an amount between €5 and €500, which the court assigns in virtue of

Montenegro	dissemination of information on personal or family life	presentation or dissemination of information on anyone's personal or family life that may harm his honour or reputation *(CC§197)*	NO	N/A	fine of €3,000 to €10,000; if committed through media or other public means, €5,000 to €14,000; if resulted in grave consequences, min. fine of €8,000	
Serbia	insult	not defined in law *(CC§170)*	NO	N/A	20 to 100 daily fines, or fixed fine of RSD 40,000 to 100,000; if committed via media or other public means, 80 to 240 daily fines or fixed fine of RSD 150,000 to 450,000	
RS	dissemination of information on personal or family life	relaying or disseminating information on a person's personal or family life that may harm his honour or reputation *(CC§172)*	YES	normally up to 6 months; if committed via media or other public means, up to 1 year	fine (unspecified)	
Turkey*	insult (*hakaret*)	undermining the honour, dignity or respectability of another person or attacking a person's honour by attributing to them a concrete act or a fact, or by means of an insult (*CC§125)*	YES	3 months to 2 years; if directed at public official, min. 1 year; if committed in response to a person's religious, political, social, or philosophical beliefs, min. 1 year	judicial fine	Punishments are increased by 1/6 when act is committed publicly

Appendix C Lexicon

Algorithm	a self-contained set of operations to be performed in a particular sequence by a computer. Algorithms exist that perform calculation, data processing, and automated reasoning.
Anonymization:	a process of removing personally identifying information obtained from cookies as well as from the IP address that could identify the user.
Bandwidth	the available capacity for transmitting online information, expressed in bit-rates (bits/second). One byte per second (1 B/s) corresponds to 8 bits/s.
Big Data	data sets so large in volume, speed, or variety that they are difficult to process, analyze, search, share, store, or transfer.
Caching	the automatic storage of data or content that duplicates original values stored elsewhere on a computer. It generally represents a search or search history of a user.
Cookies:	data sent from a website a user has viewed; they are stored in a user's *web browser* while the user is reading or viewing that website. Every time the user loads that website, the browser sends the cookie back to the server to notify the website of the user's previous activity (HTTP cookie, web cookie, Internet cookie, or browser cookie).
Cyborg	a technologically enhanced human featured in children's comics and videogames.
Dark Net	net-speak for the hidden underbelly of the Web, home to both rogues and political activists, and accessed only with the help of specially designed anonymizing software.
Deanonymization:	the insertion of sufficient identifiers (address, birth date) into data so that disclosure of an individual is achieved.
Deep packet inspection:	a form of filtering that examines data packets as they pass an inspection point; it is used to locate activity such as protocol non-compliance, viruses, spam, or other unauthorized intrusions and re-route it to a different destination, such as a spam file, or collected for statistical analysis.
Deindividuation:	a psychological state arising from a lack of attention of others and resulting in the loss of inner restraints.

Domain Name: a name used to establish a unique online identity. Organizations, governments, institutions, etc. can choose a domain name that corresponds to their name, helping Internet users to reach them easily (eg: yorku.ca). There is a hierarchy of names: top-level domain names can be assigned to countries [ca (Canada), ch (china)] or other entities [gov, edu, .ocm, org, net]. ICANN assigns domain names.

DNS server (Domain Name System) a naming system for computers or other resources connected to the Internet that offers a translation (resolution) of human-memorable *domain names* into the corresponding numeric Internet Protocol (IP) addresses needed for the purpose of computer services and devices worldwide. It serves as an Internet directory service.

Disinhibition The de-inhibiting effect of behavior prompted by anonymity; it can present as a more aggressive or punitive level of human activity.

Dropbox a file hosting or cloud storage service operated by Dropbox, Inc. to allow users to create a special folder on their computers that can be accessed by the user from any computer.

Hacktivism indicates anonymous group action to convey a political message through manipulation of a website.

HTML (HyperText Markup Language) the standard language used to create web pages, written in the form of tags enclosed in angle brackets (eg: <html>).

IP address (Internet Protocol address) a set of rules or standards that are used by computers to communicate with each other across a network, such as the Internet. A *DNS server* is used to convert a *URL* (york.ca) to an IP address, which is a number (209.191.93.52) that *routers* use to direct bits of information to its destination.

Internet Service Provider: (ISP) a commercial entity that provides services for accessing, using, or participating in the Internet (commercial, community-owned, not-for-profit, or private). Examples include Bell, Rogers, Shaw, Orange, AOL, or AT&T.

Layers of the Internet: often described as the physical layer (computer device, computer wires that connect devices), the logical layer (layer of code or computer language that enables the physical layer to function); and content layer (all information conveyed by the physical layer).

Mainframes	a high performance computer used for large data compilation and storage, historically considered to involve a centralized as opposed to the later distributed method of computing.
Metatags	provide metadata about an HTML document. It is located within the <head>. It will not be displayed on the page, but will be machine decipherable. Metatags are used to specify page description, keywords, author of the document, when it was last modified, etc. Metadata can be used by browsers (to illustrate how to display content or reload page), search engines (keywords), or other web services.
Operating system:	software that manages the computer's memory, processes, and all of its software and hardware in a computer. For example, the Apple IOS system.
OSI	(Open Systems Interconnection) a computer *protocol* or set of guidelines for implementing networking communications between computers. For example, TCP/IP (Transmission Control Protocol and Internet Protocol), HTTP, and FTP.
Platform	the environment or underlying system that software needs for its operation. The operating system of a computer is an example, such as Windows 2000, Mac OS X or IBM's S/390.
Protocol	a set of guidelines for enabling network communications between computers. The system of protocols which was developed over the initial development of the Internet became known as the TCP/IP Protocol Suite, after the two initial protocols developed: Transmission Control Protocol (TCP) and Internet Protocol (IP).
Pseudonymization:	the process of substituting one ingredient, such as a name, for numbers or other characters that can mask direct identification of the user.
Router	the traffic-directing device that forwards data packets between computer networks. For personal computers, a router can be used to transmit emails, log onto various Internet sites, or stream videos.
Selfie	a self photograph taken with a mobile phone or hand-held digital camera.
Sharding	the automated procedure of breaking up data into fragments for storage in different storage facilities or locations.

Streisand Effect:	the phenomenon, named after American entertainer Barbra Streisand, where the publicity engendered by an invasion of privacy lawsuit far exceeds the original intrusion
Social networking service:	(SNS) web-based services that allow individuals to create a public profile and a list of similar-interest users with whom to share connections, and view and cross the connections within the system.
Tagging	device to identify persons in an online photograph. It occurs in two ways: through a user that is then locked into the memory of networking sites through facial recognition software; and using the insertion of single words on a site that provides a link to that photograph.
Twibel	Libel using the Twitter social media platform.
URL	(Uniform Resource Locator) indicates the location of a file on the web (Yahoo.com). It is expressed in English, designed for people to remember.
Web browser	a software application used to retrieve or present information on the Web. Examples include Safari, Mozilla Firefox, Internet Explorer, and Google Chrome.
Web 2.0	The second generation of the *World Wide Web* that is focused on the ability of people to collaborate and share information online. Also known as the generative Internet.
Web 3.0	The third generation of Internet-based services characterized by intelligent or smart functions that link computers to sensors or the Internet to complete a function without direct human intervention.
Wireless	(Wi-Fi) any type of computer transmission of information that uses wireless (cable-less) data connections, such as radio communications.
World Wide Web	(the Web) an information system of online documents accessed via the Internet using software installed on the user's computer as a web browser.