Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person

Marion Oswald

To cite this article: Marion Oswald (2017) Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person, Information & Communications Technology Law, 26:1, 6-31, DOI: 10.1080/13600834.2017.1269870

To link to this article: https://doi.org/10.1080/13600834.2017.1269870

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 2017
VOL. 26, NO. 1, 6–31
http://dx.doi.org/10.1080/13600834.2017.1269870

Routledge
Taylor & Francis Group

Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person

Marion Oswald

Department of Law, University of Winchester, Winchester, UK

ABSTRACT

In the early twentieth century, it was still possible to be relatively anonymous at a large gathering, to be visible, yet not the subject of detailed scrutiny or surveillance. A century on, the impact of digital technology has reduced our expectations of privacy, whether physical or online. This article discusses the interpretation of 'private' and 'public' in today's technologically enabled world by reference in particular to case-law on the reasonable expectation of privacy. The article goes on to discuss the potential of technological methods for controlling, blocking and obfuscating digital information and devices as means for individuals to regain control over their privacy, ultimately concluding that these technologies, themselves alone, do not provide a long term solution to privacy harms. Finally, the article puts forward an alternative model for consideration pursuant to which certain information about individuals available to the 'masses' digitally or on the Internet, or which can be generated from such information, should no longer be regarded as 'public' in the sense of there being no privacy in respect of it. Thus, the term 'private' when applied to the digital world must be redefined.

KEYWORDS

privacy; technology; digital; private; public; surveillance

Introduction – the large party moves online

At one of the Great Gatsby's spectacular parties, the golf champion Jordan Baker remarked to Nick Carraway that she likes large parties: 'They're so intimate. At small parties there isn't any privacy.'[1]

At first glance, this statement seems nonsensical. How can there be intimacy – a closely personal or private relationship[2] – at a party where 'the cars from New York are parked five deep in the drive'?[3]

So what did Jordan mean by 'privacy'? She cannot mean secrecy, being totally unobserved or hidden. She may not recognise Brandeis and Warren's famous 'right to be let alone' as defining her concept of privacy.[4] *My right to be let alone from what?* she

CONTACT Marion Oswald marion.oswald@winchester.ac.uk

[1]F Scott Fitzgerald, *The Great Gatsby* (1925) ch 3.
[2]*Oxford English Dictionary*.
[3]F Scott Fitzgerald (n 1).
[4]Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193.

might have asked. This concept of privacy, as Solove has argued, fails to provide much guidance.[5]

So does she mean a right to control the communication of information about herself?[6] Jordan was living in an era without instant systematic access to information. Even so Gatsby could not control the stories circulating at the party about him: he had killed a man; he was a German spy during World War I; he was in the American army; he was an 'Oxford' man. Jordan herself had been accused of cheating in a golf tournament, a row that 'nearly reached the newspapers' but then died away.[7] As a well-known sports-woman, Jordan may have found this accusation upsetting but would she have thought of it as private? It is unlikely that she would have believed that she owned the information – that she had a quasi-property right in it[8] – recognising that 'personal information rarely belongs to just one individual; it is often formed in relationships with others'.[9] Indeed, Nick Carraway recalled that the scandal and Jordan's name had remained together in his mind.

Rather than considering privacy as secrecy or as a right to own information, Jordan appears concerned about being free from worry about disturbance or detailed scrutiny from other people. She expects space from others, even when she is with other people.[10] This is a party full of 'casual innuendo and introductions forgotten on the spot, and enthusiastic meetings between women who never knew each other's names'.[11] Thus Jordan *can* be in public, in the sense of being observable, but without being the focus of public attention; she would not have been able to achieve this at a smaller gathering where everyone knew her name. The extent to which information about her is collected and used certainly contributes to whether she feels free from detailed scrutiny, but her concerns seem wider than this: a wish to avoid intrusion in terms of offensive observation and judgement.[12] She might look favourably on the general idea of public privacy or freedom from unjustified surveillance in public places as a way of protecting her individual personality and dignity, but perhaps struggle to pin down when she had a 'reasonable expectation of privacy' in any particular place.

In Strasbourg case law, the reasonable expectation of privacy test is one of the factors relevant to the question of whether Article 8 of the European Convention of Human Rights (right to respect for private life) is engaged. In the UK Supreme Court judgment in *Catt*, Lord Sumption said:

> Given the expanded concept of private life in the jurisprudence of the Convention, the test cannot be limited to cases where a person can be said to have a reasonable expectation about the privacy of his home or personal communications. It must extend to every occasion on which a person has a reasonable expectation that there will be no inference with the broader right of personal autonomy recognised in the case law of the Strasbourg court. This is consistent with the recognition that there may be some matters about which there is a reasonable expectation of privacy, notwithstanding that they occur in public and are patent to all the world.[13]

[5]Daniel J Solove, *Understanding Privacy* (Harvard University Press 2009) 17.
[6]Alan Westin, *Privacy and Freedom* (Atheneum, New York 1967) 7.
[7]F Scott Fitzgerald (n 1).
[8]Paul Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harv L Rev 2055.
[9]Solove (n 5) 27–28.
[10]Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 (3) University of Pennsylvania Law Review, 477, 553.
[11]F Scott Fitzgerald (n 1).
[12]Jane Yakowitz Bambauer, 'The New Intrusion' (2012) 88 Notre Dame L Rev 25.
[13]*R (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9 [10].

Despite the acknowledgement that it can be possible to be private in public, the test remains open to criticism on the grounds that it 'is highly dependent on the interpretation and application of what qualifies as a reasonable expectation of privacy', often a matter of guesswork.[14] In her home country however, Jordan's ability to enforce her privacy at Gatsby's large party may be even more curtailed. In *Katz*, the US Supreme Court said: 'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'[15] This approach would hold that once something is public, its protection (against unreasonable searches and seizures in *Katz*) is lost. Some tort cases have recognised the concept of 'limited privacy', the idea that when an individual reveals information to one or more persons, she retains a reasonable expectation that they will not disseminate it further, although 'American law eschews a categorical answer' as to when a limited disclosure will render information 'public' for tort law purposes.[16] 'Hard-line' cases however have rejected the basic premise of limited privacy.[17] Nowadays, the hard-line approach has extended not only to the question of public and private physical spaces but to the impact of technology, for instance, so-called 'butt calls': calls made inadvertently by a mobile phone left unlocked in a jacket or back pocket. In *Huff* (a decision that considered the reasonable expectation of privacy in the context of wiretap legislation), the US Court of Appeals held that:

> a person who knowingly operates a device that is capable of inadvertently exposing his conversations to third-party listeners and fails to take simple precautions to prevent such exposure does not have a reasonable expectation of privacy with respect to statements that are exposed to an outsider by the inadvertent operation of that device.[18]

This was despite the fact that Mr Huff did not intend to make the call and regarded the contents of the conversation overheard by the phone as private.

This brings us onto the question of whether Jordan would hold the same views today. Ninety years on, would she still believe that large parties are intimate? In 1925, Jordan inhabited only a 'real world' space, her privacy threatened primarily by tangible forms of intrusion – photographs, physical surveillance, wire-tapping, media gossip – and often with technologies only available to the State. In the Internet era, 'the most powerful predators in terms of privacy violations have become we ourselves'.[19] She could be said to be effectively attending a digital 'large party' with an unlimited number of often hidden actors armed with technologies which have the tracking, identification and information retrieval abilities unheard of in the 1920s.

Before the party (at a 'real world' location, a private party on private premises), this century's Jordan might type an update onto her blog – *Diary of a Female Golfer* – which is written under an assumed name; she takes care not to mention real names or sensitive information about relationships or work. She sends a message on her Twitter account, intending this for the followers that she knows. Unbeknown to her, her Twitter account has location tracking enabled. When she arrives at the party, other guests take

[14]Anne SY Cheung, 'Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd' (2009) 2 JML 191, 200.
[15]*Katz v United States* (1967) 389 US 347, 351.
[16]Lior Jacob Strahilevitz, 'A Social Networks Theory of Privacy' (2005) 72 University of Chicago Law Review 919, 939.
[17]ibid 943–46.
[18]*Huff et al v Spaw* 2015 WL 4430466 (6th Cir. 21 July 2015), 12.
[19]Cheung (n 14), 195.

photographs of her, perhaps via a wearable device which makes 'the procedure of taking a photo or filming imperceptible to the third person who becomes the subject of the photo or the film'.[20] They use facial recognition apps to identify her, and post messages on Twitter. A drone hovers overhead, operated by a journalist, live-streaming footage to Periscope. In this decade, an allegation of cheating by a famous sportswoman would certainly have circulated on social media before making the newspapers; Nick Carraway can re-read every online account with a few clicks on his smart phone, even if the allegation later turned out to be untrue. An Internet troll 'outs' her as being the author of *Diary of a Female Golfer*. As for Gatsby, he would have little chance of remaining anonymous to strangers at his own party, his face and every story written about him available via a simple Internet search.

It is almost certain that today's Jordan would find a large party a lot less intimate. Technology has enabled the physical space to be intermingled with the virtual and the Internet risks reducing her personality to an assemblage of disparate facts, inferences, presumptions and opinions, information that as a combined mass, would previously have been available only to close acquaintances attending a small party. As Brunton has commented 'our online lives are no longer just our online lives. They *are* our lives.'[21] The immediate availability of that information, and the ability of strangers (whether physically present or online) to identify her and associate her with it, is likely to become of increased importance to her. So must Jordan accept the changes to her privacy that a near-century has brought?

'Public', 'private', technology and the law

Privacy and data protection laws, related freedom of information and freedom of speech interests, and intrusion torts all have a role to play and ride to a large extent on the concepts of 'public', 'private' and the 'reasonable expectation of privacy'. This section will explore these concepts in the light of selected EU and US case-law, recognising that privacy issues, and the definitions of public and private, are not limited to particular types of claims. Jordan appreciates that it is not feasible to expect absolute invisibility either physically or digitally but looks instead to achieve relative anonymity or privacy in certain contexts. She seeks the same comfort digitally and online as she found at Gatsby's physical large party. Silva and Reed argue that in the 'real' world, the extensive time and effort involved in the process of identification means that anonymity can be thought of as a binary state, whereas in the online world 'even the common citizen has access to a huge amount of information resources', thus weakening the relative strength of anonymity.[22] They use the underlying structure of the Internet and digital technologies – the often hidden connection between user, machine, IP address and Internet Service Provider – to argue for an expectation of relative anonymity in the cyber world, concluding that once a user makes information available to the masses online in a particular situation,

[20] Andreas Kotsios, 'Privacy in an Augmented Reality' (2015) 23(2) Int J Law Info Tech 157, 168.

[21] Finn Brunton interviewed in The Slate: Anna Diamond, 'Does That Look Like Me?' The Slate (September 14, 2015) <http://www.slate.com/articles/technology/future_tense/2015/09/an_interview_with_obfuscation_co_author_finn_brunton_about_online_privacy.single.html> accessed March 2016.

[22] Sara Nogueira Silva and Chris Reed, 'You Can't Always Get What You Want: Relative Anonymity in Cyberspace' (2015) 12 (1) SCRIPTed 37, 38.

an individual cannot expect not to be named in another situation.[23] These arguments are open to debate. First, it is hard to see how such a stark distinction between real space and cyberspace can still hold water. Digital technologies operating in real world settings link to online search, investigation and identification technologies in order to return information to those real world settings (an example being the deployment of facial recognition technologies within shops, not only for crime-prevention but to enable the retailer to identity age, gender and race, with the potential for digital photographs taken in the real world to be compared to those online[24]). The process is so interlinked that it could almost be said that there is no longer any point in trying to distinguish the real and the cyber. If so, it would follow from Silva and Reed's position that individuals should expect little anonymity in the real as well as the cyber world. In addition, this distinction between real and cyber tends to lead to the view that anything online can no longer be (or be expected to be) anonymous or private (because the Internet's infrastructure facilitates tracking and identification), whereas in the real world, physical boundaries allow us to seek out private or secret spaces in which we have a reasonable expectation of privacy.

Jordan finds this situation unacceptable. She regards the advice not to put anything on the Internet that you would not want to see on the front page of a newspaper as absurd. She thinks of her tweets as the equivalent of having a chat with her friends at home,[25] and her blog as a 'communication channel to friends and family'.[26] As a digital native, she is less concerned about protecting her data from government intrusion, marketers or spammers, and more concerned about keeping control over her personal space and protecting social boundaries.[27] She might understand Jones's view that the online world is 'a social space in its own right', one where she might divulge more than she generally does in the off-line world.[28] So she would feel a sense of shock and intrusion if unintended audiences accessed her online persona.[29] She wants to attend Gatsby's next large party free from the fear that strangers can digitally identify her, profile her and circulate her image. Surely the law will support her? She is disappointed to learn that the situation is far from clear.

[23] ibid 44.

[24] Asher-Schapiro, 'Facial Recognition Technology Is Big Business – And It's Coming for You' Vice News (13 August 2015) <https://news.vice.com/article/facial-recognition-technology-is-big-business-and-its-coming-for-you> accessed March 2016.

[25] A Dash, 'What Is Public? It's So Simple, Right?' The Message (24 July 2014) 'What if the public speech on Facebook and Twitter is more akin to a conversation happening between two people at a restaurant? Or two people speaking quietly at home, albeit near a window that happens to be open to the street? And if more than a billion people are active on various social networking applications each week, are we saying that there are now a billion public figures?'; Also see Vincent Miller, The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life (SAGE, 2015) 97 which discusses the breakdown of the divide between writing and conversation online and the 'collapse' of public and private audiences:

> Unfortunately, outside readers and legal regimes often do not acknowledge the distinction between private and public talk, as it is usually assumed by both that once something is posted on the web and is potentially available to the general public, it becomes a public statement and thereby open to public and legal scrutiny.

[26] Christopher Wienberg and Andrew S Gordon, 'Insights on Privacy and Ethics from the Web's Most Prolific Storytellers' (2015) Proceedings of ACM Web Science 2015, 28 June–1 July 2015, Oxford, UK [4.2].

[27] D Bradbury, 'The Kids Are Alright' (2015) 10(1) Engineering & Technology 30, 32.

[28] Brian Christopher Jones, 'The Online/Offline Cognitive Divide: Implications for Law' (2016) 13(1) SCRIPTed 84, 89.

[29] Patricia Sanchez Abril, 'Recasting Privacy Torts in a Spaceless World' (2007) 21(1) Harvard Journal of Law & Technology 2, 16.

The public/private dichotomy

The public/private dichotomy offers little assistance in delineating Jordan's privacy rights. Nissenbaum argues that:

> its limitations have come to light as digital information technologies radically alter the terms under which others – individuals and private organizations as well as government – have access to us and to information about us in what are traditionally understood as private and public domains.[30]

The decision in the US case of *Huff* (mentioned above) is an extreme example of such limitations. A person who operates a device which 'might grant access to others'[31] does not exhibit a reasonable expectation of privacy, even though the overheard conversation was conducted in a hotel room and intended to be private: an example of the functionalities of the technologies (perhaps unknown to the user) dictating the resultant privacy protection. In the wider context of Fourth Amendment jurisprudence and Government surveillance, Heymann's concern is for the impact that technology now available to ordinary citizens has on the definition of 'public' (and therefore on what is a 'search' in the US):

> It is not that the law has changed. Officials have long been entitled to observe what is in plain view from a public location. What has changed dramatically is what can now be seen from areas open to the public … Now observations from great distances can detect much by using highly sophisticated lenses and other sensors. Moreover, modern surveillance sees what the inattention of a human viewer might have caused to be overlooked and modern surveillance remembers and archives what might otherwise have been forgotten.[32]

Heymann argues that not only should Government use of such technologies be more closely regulated, but that legislation 'could forbid anyone – private individuals as well as governments – from engaging in certain forms of surveillance of their neighbors … This would prevent the area of privacy from continuing to narrow as it appears that it might do.'[33]

Reasonable expectation of privacy

In reviewing Strasbourg Article 8 case law (and putting aside for a moment the unlikelihood of the Convention ever applying in the US), Jordan finds herself uncertain as to the extent of her rights. She feels that she should have a reasonable expectation of privacy at the party and she is encouraged by the decision in *Egeland* that taking a photograph of an individual without consent may engage Article 8.[34] She remains unsure however as to the factors that should be taken into account at the second stage, balancing her Article 8 rights against the right of freedom of expression in Article 10: the Court's reasoning has been described as 'unsatisfactory and unclear'.[35] The apparent tension between the Strasbourg court's decision in *Von Hannover v Germany*[36] and its subsequent

[30]Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 117.
[31]*Huff* (n 18), 11.
[32]Philip B Heymann, 'An Essay on Domestic Surveillance' (2015) 3(2) Lawfare Research Paper Series, 10.
[33]ibid 20.
[34]*Egeland and Hanseid v Norway* (App No 34438/04) ECHR 16 July 2009.
[35]Kirsty Hughes, 'Photographs in Public Places and Privacy' (2009) 1(2) JML, 159, 171.
[36]*Von Hannover v Germany* (App No 59320/00) ECHR 24 September 2004.

decision in *Von Hannover v Germany (No. 2)*[37] leaves open the distinction between a 'public' and 'private' individual and arguably relaxes the requirement that an image must contribute to a 'debate of general interest'.[38] The majority decision in the UK case of *Campbell*[39] is concerning, in particular as regards the treatment of photographs taken in a public place and the extent to which inconsequential information will be regarded as private. In *Campbell*, Lady Hale noted (obiter) that photographs and the covert way in which they were taken were not of themselves objectionable:

> The activity photographed must be private. If this had been, and had been presented as, a picture of Naomi Campbell going about her business in a public street, there could have been no complaint.[40]

Lady Hale further observed that readers of newspapers will be interested in how Ms Campbell looks 'if and when she pops out to the shops for a bottle of milk'.[41]

Along similar lines, Lord Hoffman said:

> The famous and even the not so famous who go out in public must accept that they may be photographed without their consent, just as they may be observed by others without their consent.[42]

Jordan takes Lord Hoffman's statement to mean that she must tolerate photographs of herself in her daily life and in public places, even though these make no contribution to a 'debate of general interest'. But what of photographs of the 'not so famous' that many would find intrusive or even creepy, such as the covertly taken photographs posted (some with titles such as 'Three little pigs') on the Facebook and Tumblr pages 'Women Who Eat On Tubes'[43]? The website's founder openly admitted that he was 'watching' and 'photographing', styling his own activities as an artistic 'observational study'.[44] Others regarded the project as crossing a boundary into voyeuristic stranger-shaming. The decision in *Weller*,[45] which focused on the English tort of misuse of private information, came close to resolving the questions left by *Campbell* and *Von Hannover* as regards photographs of everyday activities. The case involved the publication by the Mail Online in the UK of un-pixelated photographs of the children of famous musician Paul Weller. The photographs showed the family engaged in everyday activities in a public place – shopping and sitting in a café – in Los Angeles. Dingemans J held, applying the grounds laid out in *Murray*,[46] that there was a reasonable expectation of privacy; the photographs showed the emotions on the children's faces while on a family outing, 'one of the chief attributes of their respective personalities',[47] and the newspaper knew that the photographs had been taken without consent. Even though the photographs were taken in a jurisdiction where publication would have been lawful, the judge concluded that the

[37] *Von Hannover v Germany (no. 2)* (App No 40660/08) ECHR 7 February 2012.
[38] *Von Hannover v Germany* (n 36) [60].
[39] *Campbell v Mirror Group Newspapers* (2004) UKHL 22.
[40] ibid [154].
[41] ibid.
[42] ibid [73].
[43] <http://womenwhoeatontubes.tumblr.com/> accessed March 2016.
[44] 'Women Who Eat On Tubes: The Fightback Begins' Channel 4 News (11 April 2014) <http://www.channel4.com/news/women-who-eat-on-tube-founder-were-all-wildlife> accessed March 2016.
[45] *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB).
[46] *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.
[47] *Weller* (n 45) 170–71.

tort of misuse of private information still applied to the publication of the photographs in the UK. In terms of the balance between the children's Article 8 rights and the newspaper's rights under Article 10, the judge came down in favour of the children, concluding that the publication of the photographs did not contribute to a debate of general interest. The decision was upheld by the Court of Appeal, Lord Tomlinson MR observing that the court does not necessarily require evidence of harm; it can apply common sense and its own experience regarding the undermining of the child, and the risk of bullying.[48]

Would such expectations of privacy be limited to children, Jordan might ask? Hughes concludes that it is possible that the reasoning in *Weller* could apply to photographs of adults in public places; in any event it is not ruled out.[49] An adult, for instance, the non-famous partner of a public figure, could seek to show a reasonable expectation of privacy if he was photographed and identified by name, although this may be dealt with by pixelating his face.[50] And what of public, famous or semi-famous figures such as Jordan? Hughes states that it may also be possible to argue that *Weller* should apply to public figures 'who have sought a degree of privacy', thus bringing the domestic courts in line with Strasbourg.[51]

One could speculate how this might apply to those using non-traditional routes of online publication such as social media and bloggings sites. Could there be an expectation of privacy if a photograph of an everyday activity was taken by an everyman-on-the-street and then posted to a social media site with an identifying comment? Consent is very likely to be absent in those circumstances. It is arguable that pixilation (at the very least) should occur on such Internet sites unless consent can be demonstrated. If so, who would take primary responsibility for ensuring this happens: the individual user who has taken the photograph, the person who has uploaded it to the site, the one who has taken steps to identify the individual or the provider of the online service?

Kotsios argues that under EU data protection law (often regarded as a sub-set of privacy) consent must be given by the third person for the user of a wearable device to take a photo of an individual, upload it and use facial recognition on it.[52] It is well established that an individual can be a 'data controller' under EU data protection law if the domestic purposes exemption does not apply.[53] Kotsios points to the Article 29 Data Protection Working Party opinion on social media which states that a high number of contacts on social media 'could' be an indication that the household exemption does not apply, as would extending access beyond self-selected contacts.[54] The Working Party goes on to note however that even if the domestic exemption does not apply, other exemptions might, such as the exemption for literary expression and in any event a balance must be struck between privacy and freedom of expression. The new EU Regulation continues the domestic exemption approach. It clarifies that a purely personal or household activity falling outside data protection law is one 'without a connection with a professional or commercial activity' and including 'social networking and online activity' undertaken in the

[48] *Weller and Ors v Associated Newspapers Ltd* [2015] EWCA Civ 1176 [41].
[49] Kirsty Hughes, 'Publishing Photographs Without Consent' (2014) 6(2) JML 180, 187–88.
[50] ibid 188.
[51] ibid.
[52] Kotsios (n 20) 179.
[53] Case C-212/13 *Ryneš v Úrad pro ochranu osobních údaju* [2014]; Case C101/01 *Bodil Lindqvist* [2003].
[54] WP 163, 0189/09/EN, Opinion 5/2009 on online social networking, 6.

context of such personal activity.[55] So, putting to one side the practical difficulties of enforcing against individuals, the data protection position is by no means clear cut.

Technological functionality and privacy

Jordan finds further examples of technological functionality impacting on resultant privacy protection. She is discouraged by the 'Night Jack' case in which the author of an anonymous blog was refused an injunction preventing the publication of his identity. The blogger's claim was based upon the publication of allegedly private information in contravention of Article 8 of the European Convention of Human Rights. It failed the first step: whether the claimant had a reasonable expectation of privacy in relation to the information in question. Eady J held that blogging is essentially a public rather than a private activity.[56] He also determined that even though a blogger may take steps to disguise their identity, as Jordan has done, it is a 'significantly further step' to say that if others can determine the blogger's identity, they should be prevented from revealing it.[57] The judge went on to consider in some detail the stage two balancing test should he have been wrong about stage one, concluding that because of the blogger's role as a police officer and the nature of the political comments made in the blog, there was a considerable public interest in his identity being known. It should be emphasised however that the claim failed at step one, whether there was a reasonable expectation of privacy in the relevant information in the first place. Reviewing this case, Hughes concludes that the decision leaves bloggers very vulnerable; it seems to render privacy settings redundant if another is capable of circumventing them.[58]

Another criticism that could be made of the decision is that it fails to acknowledge that the majority of blogs are personal diary types, providing bloggers with a unique opportunity for expressive privacy.[59] McCullagh comments that:

> Bloggers are aware of a risk posed by external parties who might be interested in collecting or collating the information they post; thus they seek to restrict their blog readership and content. Also, the comments reveal that bloggers were likely not to blog about controversial social, moral or philosophical issues which would draw negative responses or criticism from readers or members of wider society. This suggests that bloggers consciously and intentionally negotiate the boundary between public and private.[60]

Other decisions have taken a more nuanced approach to information published 'publicly' on the Internet. *Rocknroll*[61] concerned photographs of the claimant, partially naked, taken at a private party on private premises. The claimant had recently married the actress Kate Winslet, his second wife, and the defendant intended to publish the photographs in the Sun newspaper. The photographs were taken by another guest and posted on his Facebook page, where they became accessible to the general public due to a later change in the privacy settings.

[55]Regulation (EU) 2016/679 Recital (18).
[56]*The Author of a Blog v Times Newspapers* [2009] EWHC 1358 (QB) [11].
[57]ibid [9].
[58]Kirsty Hughes, 'No Reasonable Expectation of Anonymity?' (2010) 2(2) JML 169, 175.
[59]Karen McCullagh, 'Blogging: Self Presentation and Privacy' (2008) 17(1) ICTL 3, 19.
[60]ibid 14.
[61]*Mr Edward Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch).

Briggs J rejected the argument that the photographs had come into the public domain 'so as to be beyond recall'[62] although it has to be said that the judge did lay emphasis on the lack of evidence of widespread public inspection of the photos:

> No internet search of the claimant by his name would have revealed them, nor even a simple search or inspection of the wall-page or home-page of [the] Facebook account. The probability is, on the present evidence, that the photographs would only have been found either as the result of very expert, expensive and diligent research, or as the result of a tip-off by someone who knew about them and their whereabouts.[63]

One wonders though if this case would have had a different outcome if evidence had been put forward to show that facial recognition and profiling technology (of the sort generally available to the normal citizen) could easily retrieve the photographs on other sites to which they had been transferred. Would then the judge have concluded that a line had been crossed such that there was no longer any privacy left to be protected?

In *Morley*, the Upper Tribunal overturned the First-Tier Tribunal and held that the details of youth council members held by a local council were exempt from disclosure under the UK's Freedom of Information Act 2000, even though some of the names had been publicly visible on the group's Facebook page.[64] The Upper Tribunal rejected the argument that, by putting themselves on Facebook, the members had consented to their information being used in another way.[65,66] This might be viewed as an example of Nissenbaum's contextual privacy theory in action.[67] The First-Tier decision certainly failed to give sufficient consideration to the difference between information held by a public authority and that held in a private context, and the overall context in which personal data was disclosed on the Facebook page. Nissenbaum's theory has been criticised as being accurate only where there is a relationship between the information discloser and disclosee, not the case when information is made available to the masses online.[68] This criticism is not entirely invalidated by the *Morley* decision. Although the case concerned in part names disclosed on a Facebook page, the information requested was held by the local authority, with which the individuals had a relationship. The existence of the Facebook page was used by the requestor as an argument that the youth councillors should have no expectation of privacy in the personal details held separately by the local authority, an argument dismissed by the Upper Tribunal. The case did not consider the transfer or use of the personal details disclosed on the Facebook page and what an appropriate flow of such information might have been, a decision that is likely to be little more than educated speculation. It may be feasible however to agree upon categories of information uses and flows that are *not* appropriate.

[62]ibid [20].
[63]ibid [25].
[64]*Surrey Heath Borough Council v Information Commissioner and John Morley* [2014] UKUT 0339 (AAC).
[65]ibid 6–7.
[66]For a critique of the First-Tier decision, see Marion Oswald, 'Facebook group implies consent to disclosure of personal data' (2013) 3(1) International Data Privacy Law 61.
[67]The 'right to privacy is neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information' Nissenbaum (n 30) 127.
[68]Silva and Reed (n 22) 44.

Inappropriate use of publicly available information

Inappropriate use of publicly available information was dealt with in the Northern Irish case of *CG*.[69] CG was convicted in 2007 of a number of sex offences against children, served a sentence of imprisonment and was released on licence in 2012. McCloskey operated a Facebook page called 'Keeping our Kids Safe from Predators 2' on which he posted a photograph of CG and an article from the Irish News at the time of CG's conviction. Comments on the Facebook page posted by others included abusive and violent language about CG and members of his family and comments identifying CG's location and providing identifying details about CG and his children. As Stephens J described it, McCloskey was in effect 'gathering all the available information he could obtain about all the sex offenders in Northern Ireland and publishing that information on his profile/page'.[70]

CG sued both McCloskey and Facebook on the grounds of misuse of private information, breach of Articles 2, 3 and 8 of the ECHR and harassment. Stephens J used the categories of sensitive personal data in the UK's Data Protection Act 1998 (DPA), and in particular sex life and the commission of an offence, to provide 'a useful touchstone as to what information is deemed to be private' for the purposes of the tort of misuse of private information, and in relation to the balancing exercise between CG's Article 8 rights and McCloskey's Article 10 rights.[71] The court concluded that CG had an expectation of privacy in the following information (individually and in combination):

(a) Any photograph of him that could be used to identify where he lived and increase the risk of harassment of him and his family;
(b) His name, if used in conjunction with other information which might identify where he lived;
(c) His present address or description of the area in which he lived;
(d) His previous address/area where he lived if this could be used to identify his present address;
(e) His criminal convictions except as ought to be disclosed in accordance with public protection arrangements in Northern Ireland;
(f) The risks that he posed to the public except as ought to be disclosed in accordance with those public protection arrangements;
(g) Information about his family.[72]

In considering the balance between Article 8 and Article 10, the judge considered whether McCloskey could have availed himself of any defence or exemption under the DPA. It was determined that McCloskey's activities did not fall within any of the schedule 2 and 3 conditions necessary for the processing of sensitive personal data. Even if McCloskey's activities could be classified as journalism, McCloskey could not believe that his activities were in the public interest as required by section 32. The judge concluded that the balance came down firmly in favour of CG; the information published in the judge's view harmed the public interest, created a risk of re-offending and incited violence

[69] *CG v Facebook Ireland Limited and Joseph McCloskey* [2015] NIQB 11.
[70] ibid [70].
[71] ibid [79].
[72] ibid [83].

and hatred.[73] Although the judge made no determination as to whether Facebook was a data controller under the DPA, he ruled that it was also a publisher and had misused private information from the date on which it had been put on notice by the claimant (Facebook's defence under the E-Commerce Directive therefore failed).

Does Jordan also have an expectation of privacy in all the above categories of information, such that she should be able to control its dissemination absent any public interest justification? This conclusion cannot be reached with any certainty. Indeed, the *CG* decision could be criticised for placing too much emphasis on the DPA's definition of sensitive personal data. Information could be sensitive, giving an individual certain rights in respect of it under the DPA, but not private. It is difficult to understand how CG's image (taken as it was from a newspaper article) and the fact of his conviction for serious offences could be said to be private, particularly since such a relatively short period of time had passed since the conviction. If McCloskey's site had limited itself to republishing or linking to publicly available images and newspaper articles without allowing third party comments, would the balance have fallen the other way? Although combining and consolidating (and thus highlighting) disparate sources of publicly available information has a privacy impact (as the *Google Spain*[74] case has famously determined), the harmful consequences to CG would have been reduced and McCloskey's public interest arguments on the basis of journalistic activity may have had a chance of success.

The decision of the Strasbourg court in *Satakunnan*[75] should be noted however. In Finland, the tax details of citizens are publicly available and the applicant companies had published a magazine containing data on 1.2 million persons' taxable income and assets, and developed a SMS search tool using the data. The Strasbourg court refused to overturn the Finnish court's decision that publishing taxation information to such an extent could not be considered as journalism but was the unlawful processing of personal data.[76] The decision leaves open the question of how much publicly available information will need to be published in order to tip the balance into unlawful processing, and certainly seems to ignore the view that the acquisition and exchange of information can be an integral part of freedom of speech and the creation of knowledge.[77] In a strongly worded dissenting opinion, Judge Tsotsoria said that:

> Establishing a quantitative framework for publicly available information and limiting the freedom guaranteed by Article 10 on this ground does not correspond to the notion of a "pressing social need".[78]

Having reviewed this selection of case-law, Jordan feels none-the-wiser as to the circumstances in which she would be deemed to have a reasonable expectation of privacy, whether she can control any inappropriate use of information that she posts on the Internet, or if she can free herself from identification and profiling by digital technology. She doubts that any of the conduct at the party would satisfy the requirements of the

[73]ibid [98].
[74]Case C-131/12 *Google Spain v AEPD and Mario Costeja Gonzalez* [2014].
[75]*Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (App No 931/13) ECHR 21 July 2015.
[76]ibid 17 [68].
[77]Jane Yakowitz Bambauer, 'Is Data Speech?' (2014) 66 Stan L Rev 57, 60.
[78]*Satakunnan* (n 75), 31 [10].

offence or tort of harassment under the Protection from Harassment Act 1997.[79] She decides to take an alternative approach.

Taking privacy into her own hands: controlling, blocking and lying

What can Jordan do if she wants to take matters into her own hands, and become a 'privacy vigilante'?[80] She already uses an ad-blocker and a tracker detector,[81] and an internet browser which automatically deletes cookies on shutdown and lets her express her preference not to be tracked by websites.[82] Friends suggest that she use the Tor network which protects against Internet surveillance by distributing transactions over several places on the Internet, so no single point links to a user's destination; the network is used by journalists, bloggers, activists and whistleblowers among others.[83] She researches this further and discovers that, in terms of technical strategies, computer science researchers have tended to distinguish between tools such as peer-to-peer networks, proxies and anonymising networks such as Tor which aim to hide or disguise information and which require the use of third party infrastructure, and tools and techniques involving obfuscation and/or disinformation and which only require changes at the client-side.[84] The first category of solutions has been criticised for forcing the user to impose unwanted trust onto the third party entities[85] and as Bernal points out, such solutions are 'relatively obscure' and only protect those 'in the know'.[86] In addition, Jordan finds media articles suggesting that Tor and the like could be tainted with an association with criminal activities such as drug dealing and child abuse.[87] For these reasons, she decides to focus her attention on a selection of techniques that could, in theory, be implemented by her individually.

Personal data stores

First, she might attempt to take control of her personal information by using a personal data store (PDS), a form of trust network described by Pentland as 'a combination of a computer network that keeps track of user permissions for each piece of personal data, and a legal contract that specifies both what can and can't be done with the data, and what happens if there is a violation of the permissions'.[88] PDSs are said by their promoters to enable individuals to take back control over their personal data and manage their relationship with suppliers. In particular, PDSs aim to provide information as a tool in

[79] 1997 c.40, ss1(1), 2 and 3.
[80] Marion Oswald, 'Seek, and Ye Shall Not Necessarily Find: The Google Spain Decision, the Surveillant on the Street and Privacy Vigilantism' in K O'Hara et al (eds), *Digital Enlightenment Yearbook* (IOS Press 2014) 99–115.
[81] Such as Ghostery <https://www.ghostery.com/en/why-ghostery/for-individuals/> accessed March 2016.
[82] Such as Mozilla Firefox <https://www.mozilla.org/en-US/firefox/dnt/> accessed March 2016.
[83] <https://www.torproject.org/about/overview.html.en> accessed March 2016.
[84] S T Peddinti and N Saxena, 'Web Search Query Privacy: Evaluating Query Obfuscation and Anonymizing Networks' (2014) 22 J Comput Sec 155, 157.
[85] ibid 156.
[86] Paul Bernal, *Internet Privacy Rights* (Cambridge University Press 2014) 135.
[87] M Ward, 'Tor's Most Visited Hidden Sites Host Child Abuse Images' BBC News (30 December 2014) <http://www.bbc.co.uk/news/technology-30637010> accessed March 2016; 'Peeling the Onion – Tor's Criminal Content Revealed' InfoSecurity Magazine (5 March 2014) <http://www.infosecurity-magazine.com/news/peeling-the-onion-tors-criminal-content-revealed/> accessed March 2016.
[88] Alex Pentland, *Social Physics: How Good Ideas Spread – The Lessons from a New Science* (The Penguin Press, New York 2014) 182.

the hands of the individual (as opposed a tool in the hands of business).[89] But despite the prediction of significant market growth in PDSs,[90] service providers would need to be prepared to change their business models fundamentally if PDSs are to fulfil their potential.

The process of the user attaching terms and conditions to the data at the point of sharing required by PDSs raises numerous questions around contract formation and incorporation of terms, 'battle of forms' and offers and counter-offers, not to mention the challenges of negotiating in any meaningful way with online service providers.[91] How would observed or derived data be handled: by the data subject's terms, by new regulation or both? There would have to be limits on the scope of the user's terms, for instance, attempting to restrict use of information for journalistic purposes in the public interest. The position regarding consumer rights would need to be considered. The UK's Consumer Rights Act does not apply to situations where consumers exchange personal data in return for access to digital content.[92] The EU's draft Directive on digital content would extend protection to these types of exchanges[93] although in responding to these proposals, a number of issues have been raised. For instance, the UK's Competition and Markets Authority has said:

> 'When the form of payment is data rather than money, the 'value' of the data may be difficult to assess given that the value of data is a fluid value depending on various factors (the same data may be more valuable, for example, to one trader than to another and may depend on other data available to the trader). So how is the value of data assessed? A practical example may be the case of an app which is 'purchased' for, say, £1, £5 or through data exchange: if the contract is silent, how does one assess against what standard the digital content should be assessed?'[94]

Furthermore, dialogue around PDSs tends to include the assumption that individuals 'own' their information, a concept not (yet) recognised by English law.[95] A property-based approach to information and privacy has been argued for as reflecting most people's attitude towards their data and creating 'a shared understanding of the trust based nature of the relationship between the *in personam* rightholder and the *in rem* collector of information'.[96] This however is by no means an accepted approach. While Samuelson argues for protection akin to trade secrecy law,[97] Lemley believes that creating an intellectual property right in personal data 'is a very bad idea'[98] ('politically unsaleable', risky to the public domain and easily signed away through contract).

The control promised by PDSs may in any event be somewhat illusory. Lazaro and Métayer point out that control cannot be an absolute protection and that it is somewhat paradoxical that 'the term "control" as interpreted by lawyers seems to be used as a key

[89]Ctrl-Shift, 'Personal Information Management Services: An Analysis of an Emerging Market' June 2014, 11.
[90]ibid 7.
[91]See Dave Murray-Rust, Kieron O'Hara, Marion Oswald, Max Van Kleek and Nigel Shadbolt, 'Privacy by Obfuscation with Personal Data Management Architectures: Possibilities and Constraints' Workshop on Economics and Surveillance, ACM Web Science, June 30, 2015, Oxford, UK section 4.
[92]2015, c.15 s 33.
[93]Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2015/0287 (COD).
[94]The CMA's response to the UK Government's call for views on the draft directives on the online sales of digital content and tangible goods, 15 February 2016, 2.
[95]The Court of Appeal in *Fairstar Heavy Transport v Adkins* [2013] EWCA Civ 886 declined to determine whether there was any proprietary right in information.
[96]Christopher Rees, 'Who Owns Our Data?' (2014) 30(1) Computer L Sec Rev 75, 79. See also Christopher Rees, 'Tomorrow's privacy: personal information as property' (2013) 3(4) IDPL 220, 221.
[97]Pamela Samuelson, 'Privacy as Intellectual Property?' (1999–2000) 52 Stan L Rev 1125.
[98]Mark A Lemley, 'Private Property' (1999–2000) 52 Stan L Rev 1545, 1547.

privacy principle in situations where "control", in the technical sense, is effectively relinquished (or at least shared)'.[99] Subject to the development of a supportive legal and commercial ecosystem (a not insignificant task), a PDS could allow Jordan to regain a degree of control over her personal data and its further dissemination on the Internet, but only if she is placed in a position to monitor compliance and to enforce the contractual agreement. A PDS, combined with the suppression of links to irrelevant or inadequate information pursuant to the *Google Spain* decision, may contribute to increasing her relative obscurity on the Internet. However, a PDS can be effective only where Jordan has a relationship with those wishing to use her personal information. At the party, she has no such relationship. Her concerns relate not just to the use of data but also to the ability of known and unknown individuals to identify, profile, and to intrude upon her. How can she influence their activities when she may have no knowledge of them and no means to give meaningful consent or otherwise? Hildebrandt believes that real user empowerment is dependent upon moving away from sources of information that data controllers are willing to provide, instead giving individuals the ability to engage in 'counter-profiling' in order to increase front-end transparency of profiling, for instance, 'employing inference machines to infer the monetary value of the data and the manipulability of persons that match specific patterns'.[100] Hildebrandt recognises, however there is currently no legal obligation to provide the socio-technical infrastructure required for counter-profiling.[101]

Blocking identifiable data

Secondly, blocking. Jordan would want to see social media and lifelogging technologies take steps to block, pixelate or 'Shrekify'[102] the public display of any recognisable image of her unless she has given permission.[103] At the party itself, Jordan might deploy a Google Glass blocker, which impersonates the Wi-fi network, sends a 'deauthorisation' command and cuts the headset's internet connection,[104] and she could don a 'Privacy Visor', prototype glasses which use light-reflecting material to disrupt facial recognition technology.[105]

In terms of the practices of internet service providers, Jordan might take some encouragement from recent enforcement actions taken by EU data protection regulators in relation to the data collection practices of Google[106,107] and

[99]Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12(1) SCRIPTed 4, 30.
[100]Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015) 223.
[101]ibid.
[102]An algorithm that could automatically replace faces in photos with artificial ones: Tereza Pultarova ''Shrekifying' Faces Could Protect Privacy Online' Engineering & Technology, August/September 2015, 20–21.
[103]See for instance C Gurrin, R Albatal, H Joho and K Ishii 'A Privacy by Design Approach to Lifelogging' in K O'Hara et al (eds), *Digital Enlightenment Yearbook* (IOS Press 2014) 68.
[104]A Greenberg, 'Cut Off Glassholes' Wi-Fi With This Google Glass Detector' Wired (3 June 2014) <http://www.wired.com/2014/06/find-and-ban-glassholes-with-this-artists-google-glass-detector/> accessed March 2016.
[105]C Osborne, 'Privacy Visor Which Blocks Facial Recognition Software Set for Public Release' ZDNet (10 August 2015) <http://www.zdnet.com/article/privacy-visor-which-blocks-facial-recognition-software-set-for-public-release/> accessed March 2016.
[106]Dutch Data Protection Authority, Press Release 9 July 2015 <https://cbpweb.nl/en/news/privacy-campaign-google-following-possible-sanction-dutch-dpa> accessed March 2016.
[107]For an assessment of regulators' reaction to Google's new privacy policy, see Judith Rauhofer, 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?' (2015) 1(1) EDPLR 5.

Facebook[108], and against Facebook's 'real-name' policy.[109] It has been reported that the need for an opt-in has prevented the launch of Facebook's Moments facial recognition app in Europe.[110] Such enforcement activities have laid particular emphasis on the provision by the service provider of ever more detailed information to enable the user to give consent to the processing of their personal data. Ensuring such consent is meaningful rather than 'non-negotiable, non-informed, pressurised and illusory'[111] remains a challenge however, an example being the copying by brands of photos posted on social media, justified on the grounds of 'implied consent' given by the user by tagging a company in their posts and the site's often opaque terms of use.[112] Indeed, this focus on consent risks ignoring the larger issue of the legality of data combination practices, instead shifting responsibility onto the user for controlling the way in which their personal data is processed.[113]

Importantly, the user may not be the individual who is being photographed or identified. Selvadurai and Hörnle comment that:

> Big data and face recognition technologies [FRT] raise the question of whether consent is a meaningful justification for the processing of facial recognition data. The user is by definition unsure what he or she is consenting to. Consent to publication and republication of a photo on another profile, for example, is one thing, but aggregating information across the Internet and re-identifying individuals through face recognition technology from a single tagged photo goes much further and beyond the imagination of the average user. Powerful FRT means that users cannot foresee how and by whom their personal identifying information will be used, hence the limits of consent to justify such processing. … Hence users are in need of protected, private spaces where FRT cannot be used.[114]

Such a protected space seems some way off. In the US, privacy groups have withdrawn from talks on a voluntary code of conduct for companies that use facial recognition technologies on the basis that 'industry stakeholders were unable to agree on any concrete scenario where companies should employ facial recognition only with a consumer's permission'.[115] Kotsios proposes a solution that would appoint social media sites as the guardians of privacy by making them responsible for contacting third persons for permission to display an identifiable photo. This solution takes as its hypothesis however the suggestion that people will consent to facial recognition by the sites, resulting in further identifiable information being collected by commercial

[108]Dutch Data Protection Authority, Press Release 6 May 2015 <https://cbpweb.nl/en/news/facebook-provides-information-after-formal-demand-dutch-dpa> accessed March 2016.
[109]J Fioretti, 'German Regulator Orders Facebook to Allow Pseudonyms' (28 July 2015) <http://www.reuters.com/article/2015/07/28/us-facebook-germany-pseudonyms-idUSKCN0Q21U620150728> accessed March 2016.
[110]D Seetharaman 'Facial-Recognition Concerns Keep Facebook 'Moments' from Europe' *Wall Street Journal* (18 June 2015) <http://blogs.wsj.com/digits/2015/06/18/facial-recognition-concerns-keep-facebook-moments-from-europe/> accessed March 2016; A description of Moments can be found at <https://newsroom.fb.com/news/2015/06/introducing-moments/> accessed March 2016.
[111]Lillian Edwards, 'Privacy, Law, Code and Social Networking Sites' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar 2013) 332.
[112]S Ember and R Abrams 'On Instagram and Other Social Media, Redefining 'User Engagement' (The New York Times, 20 September 2015) <http://www.nytimes.com/2015/09/21/business/media/retailers-use-of-their-fans-photos-draws-scrutiny.html> accessed March 2016.
[113]Rauhofer (n 107) 14.
[114]Niloufer Selvadurai and Julia Hörnle, 'Just a Face in the Crowd' (2015) OUPBlog <http://blog.oup.com/2015/06/face-recognition-technologies-identity-international-law/> accessed March 2016.
[115]Privacy Advocates Statement on NTIA Face Recognition Process, 16 June 2015 https://www.eff.org/document/privacy-advocates-statement-ntia-face-recognition-process accessed March 2016.

bodies.[116] As Kotsios acknowledges, there are significant interoperability questions and the issue of the person who cannot be contacted via social media because they do not have an account.[117] The Working Party has previously advised that:

> Even if the SNS had the means to contact the non-user and inform this non-user about the existence of personal data relating to him/her, a possible e-mail invitation to join the SNS in order to access these personal data would violate the prohibition laid down in Article 13.4 of the ePrivacy Directive on the sending of unsolicited electronic messages for direct marketing purposes.[118]

In addition, tracking of non-users has been the subject of recent enforcement action by EU data protection authorities.[119]

Should Jordan take matters into her own hands therefore and deploy the Google Glass blocker, she may well fall foul of computer misuse legislation if she did not have the consent of the network owner. In the UK, there would be a risk of a section 3 offence under the Computer Misuse Act 1990 – an unauthorised act with intent to impair the operation of any computer. Instead she might take up a suggestion made by Haddadi et al – the 'continuous broadcast of a Do-Not-Track beacon from smart devices carried by individuals who prefer not to be subjected to image recognition by wearable cameras', although the success of this would depend on regulatory enforcement and whether device providers received and conformed to such requests.[120] Jordan has no wish however to be forced to broadcast her presence at the party to avoid image recognition. As for wearing the Privacy Visor, as well as drawing undue attention to herself, she thinks she looks ridiculous!

Obfuscation technologies

Finally, obfuscation, by which technology is used to produce false or misleading data in an attempt, as Murray-Rust et al put it, to 'cloud' the lens of the observer.[121] This is the technological equivalent of what most of us will have already done online: missing off the first line of our address when we enter our details into an online form; subtly changing our birthday; deliberately giving an incorrect email address in exchange for a money-off voucher. A PDS could, for instance, be used to add 'chaff' (adding multiple data points amongst the real ones), hide real search queries among many 'ghost' ones[122] or simulate real behaviour such as going on holiday. Obfuscation could obstruct stylometric analysis (used to attribute authorship to anonymous texts) by, for instance, changing the text so that there is no distinctive style.[123] On the face of it, obfuscation may seem to be an attractive alternative approach, providing individuals with a degree of control over how much 'real' information is released

[116]Kotsios (n 20) 184.
[117]Kotsios (n 20) 185.
[118]Opinion 5/2009 (n 54) 8.
[119]Natasha Lomas, 'Facebook Ordered to Stop Tracking Non-users in France' TechCrunch (9 February 2016) <http://techcrunch.com/2016/02/09/facebook-ordered-to-stop-tracking-non-users-in-france/> accessed March 2016.
[120]H Haddadi, A Alomainy, I Brown, 'Quantified Self and the Privacy Challenge in Wearables' Society for Computers & Law (5 August 2014) <http://www.scl.org/site.aspx?i=ed38111> accessed March 2016.
[121]D Murray-Rust, M Van Kleek, L Dragan, N Shadbolt, 'Social Palimpsests – Clouding the Lens of the Personal Panopticon' in K O'Hara et al (eds) *Digital Enlightenment Yearbook* (IOS Press 2014) 76.
[122]See the description of 'TrackMeNot' in Finn Brunton and Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (The MIT Press 2015) 13–14.
[123]ibid 31–33.

and some confidence that often unknown profiling activities will be hampered. Brunton and Nissembaum note that obfuscation 'offers the possibility of cover from the scrutiny of third parties and data miners for those without other alternatives'.[124] They admit that obfuscation is not a strong privacy system like encryption; instead it can enable an individual to assert a sense of autonomy, or can provide tools for protest or obscurity.[125]

Obfuscation raises ethical issues.[126] Do the ends justify the arguably 'dishonest' means? Does noise-generation inappropriately waste resources and 'pollute' important data flows? Are obfuscators free-riding on others' data? Brunton and Nissenbaum conclude that 'obfuscation offers a means of striving for balance defensible when it functions to resist domination of the weaker by the stronger'.[127] That may well be so but there could still be consequences for an individual. Murray-Rust et al distinguish between official data, where obfuscation may be a criminal offence, and other data that can be obfuscated 'without legal consequence'[128] a rather stark distinction. First, on the civil side, those who use social media sites and other online services are required to agree to terms and conditions, which almost without fail will govern the collection of customer data, and will often include identity disclosure requirements or 'real name' policies. Obfuscation technologies threaten the data collection business model on which many online businesses rely. Terms and conditions can be updated to prohibit obfuscation methods, and technology designed to enforce the terms and to identify bots: 'Those in the surveillance business respond to neutralization efforts with their own innovations which are then responded to in a re-occurring patterns … innovations may offer only temporary solutions.'[129] Secondly, might Jordan be committing fraud or a computer misuse offence by using obfuscation technologies?[130] A theoretical and some might say far-fetched risk at this point in time maybe, but one that many less technologically savvy individuals may be reluctant to take.

Jordan concludes that obfuscation methods may provide her with 'cover' online and a means to prevent individual exposure. Overall however, although all these privacy vigilante methods have their place, she questions whether they place too much responsibility on the individual for privacy protection. Of themselves, they seem to be more of a sticking plaster against the privacy problems created by the existing system. She wishes to find a way that the 'mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone'[131] can become a principle universally recognised online.

[124]Finn Brunton and Helen Nissenbaum, 'Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation' (2011) 16(5) First Monday <http://firstmonday.org/article/view/3493/2955> accessed March 2016.
[125]Brunton and Nissenbaum (n 122) 58.
[126]Brunton and Nissenbaum (n 122) 63–70.
[127]Brunton and Nissenbaum (n 122) 70.
[128]Murray-Rust et al (n 121) 90.
[129]Gary T Marx, 'A Tack in the Shoe and Taking Off the Shoe: Neutralization and Counter-Neutralization' (2009) 6(3) Dynamics, Surveillance and Society 294–306, 299.
[130]In England and Wales, fraud offences have been criticised as being so broad as to effectively criminalise lying (D Ormerod, 'The Fraud Act 2006 – Criminalising Lying' [2007] Crim LR 193); Where terms and conditions prohibit the use of obfuscation technologies in order to access data held by the service, arguably attempting to do so would be unauthorised (even if the user did not in fact read the terms), thus satisfying the conditions for commission of the s1 offence under the UK's Computer Misuse Act 1990.
[131]Solove (n 10) 553 quoting from *Saunders v American Broadcasting Companies* 978 P.2d 67, 69–70 (Cal. 1999) '"The concept of 'seclusion' is relative. The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."'.

Jordan's fightback – or how to make the large party more intimate in the twenty-first century

It has been argued that cyberspace is special and therefore we need a different approach to law-making for it,[132] although perhaps it is the consequences of the cyber, rather than any particular 'space', that requires a different approach. Technology and social media increasingly makes information public that would have been private in the past and it is specious to equate this to a homeowner failing to draw the curtains over a window.[133] (In any event, we do not expect someone to press their noses against our un-curtained window or to look around the back garden because we have left the gate open!) Digital and online technologies can give access to information about an individual that she assumed was hidden, anonymised or hard to find, more akin to a physical search of home or person (an activity that when done by the State has traditionally been subject to strict criteria or a warrant). Social media sites are commonly regarded as just another form of public space, although unlike a real-world public space where there is generally no systematic monitoring, social media is characterised by explicit observation of content and interactions.[134] The expansion of social networking over the last decade has seen privacy-by-default system settings turn into disclosure-by-default; thus 'the boundaries between the public and private spheres become blurred'.[135]

European case-law has been edging towards a more nuanced appreciation of the private nature of certain information generally viewable online, although the concept of 'reasonable expectation of privacy' causes considerable contextual uncertainty, and the courts have been prepared to allow technological advances to impact upon the boundaries of public and private, sometimes to the detriment of the individual. PDSs, obfuscation technologies and blocking methods, although available to the informed user, have as yet, no settled legal or commercial infrastructure to support their widespread use.

This section reviews four approaches that have been put forward by scholars to target legitimate privacy harms. First, Bernal argues for a rights-based approach to the protection of autonomy online as, he says, data protection has become a piece of technical legislation 'more about the regulation of data flow than the protection of individuals' privacy'.[136] One such right would be the right to compartmentalise any number of separate identities[137], an approach related to Tene's disaggregated identities.[138] Giving the unmasking of Night-Jack as an example, Bernal also argues for a right to maintain anonymity online, with such a right involving the protection of links between online and offline identities.[139] Bernal believes that 'the balancing of rights in coming to any decision [to reveal links] should be weighted heavily in favour of not revealing the links'.[140] The rights put forward by Bernal are not, he admits, legally enforceable but something more akin to natural

[132]Chris Reed, *Making Laws for Cyberspace* (Oxford University Press 2012) 26.
[133]See *Huff* (n 18) [10].
[134]Stefan Straus and Michael Nentwich, 'Social Network Sites, Privacy and the Blurring Boundary Between Public and Private spaces' (2013) Science and Public Policy 726.
[135]ibid.
[136]Bernal (n 86) 223.
[137]Bernal (n 86) 249.
[138]Omer Tene, 'Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services' (2013) 8(2) JICLT 118–32.
[139]Bernal (n 86) 256–57.
[140]Bernal (n 86) 257.

rights[141] and additional steps would be needed to interpret and enforce these rights, and to define exceptions and the treatment of competing interests.

Secondly, Richards and Hartzog believe that privacy law's legacy of harm and control is pessimistic and worn out, arguing that trust can add force to privacy concepts by taking inspiration from the law of fiduciaries.[142] They would recognise the role of trust in *all* information relationships, although with higher duties of care and loyalty being imposed where there is greater trust or potential for exposure.[143] Hartzog has previously argued for the level of practical obscurity given to information online to be used by the courts to determine if information is eligible for privacy protection.[144] The later article goes further and suggests that privacy law should embrace the concept of discretion, the expectation that information will stay within certain networks even if it does not stay completely confidential.[145] This would recognise the blurred lines between public and private:

> Regulators, legislators and judges should create some kind of obligation on entrustees to obfuscate disclosures such that the general public or specifically unauthorized parties are unlikely to find or understand entrusted information, even when the information is not strictly confidential,

with the enhancement of tort law offering a potential route to implementation.[146]

Bambauer also uses tort law to consider information-age privacy harms, specifically proposing adaptations to the US tort of intrusion upon seclusion.[147] She criticises privacy laws and theories that attempt to constrain the dissemination and re-use of personal information as failing to account for 'the significant social costs of propertizing facts'.[148] Instead, Bambauer proposes that the intrusion tort 'should provide recourse, not for the creation of personal data, which is a necessary byproduct of well-functioning technologies, but for the *observation* of that data'.[149] She distinguishes between capture and observation, i.e. between automated data processing (not caught by her restated tort) and observation related to a particular data subject.[150] Bambauer lays particular stress on the importance of free flow of information and her restated tort[151] is based around *unexposed* information:

> Information that is voluntarily shared with an individual or the public can be observed without offense by that individual, in the case of the former, and by any individual in the case of the latter. The offensiveness element winds up turning on whether the observed could have and should have expected their information to be exposed to the observer.[152]

---

[141] Bernal (n 86) ix.
[142] Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (3 September 2015) 34–35. Available at SSRN: <http://ssrn.com/abstract=2655719> accessed March 2016.
[143] ibid 36.
[144] Woodrow Hartzog and Frederic Stutzman, 'The Case for Online Obscurity' (2013) 101 Calif L Rev 1. The article argues that information is obscure online if it lacks one or more key factors that are essential to discovery or comprehension: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity.
[145] Richards and Hartzog (n 142) 39.
[146] Richards and Hartzog (n 142) 40.
[147] Bambauer (n 12) 230. The tort of intrusion imposes liability on anyone who intentionally intrudes on the seclusion of another if the intrusion would be highly offensive to a reasonable person.
[148] Bambauer (n 12) 209.
[149] Bambauer (n 12) 209–10.
[150] Bambauer (n 12) 249.
[151] *One who intentionally observes another is subject to liability to the other if the observation would be highly offensive to a reasonable person* Bambauer (n 12) 245.
[152] Bambauer (n 12) 245.

The proposal therefore appears to continue the hard-line approach as regards information exposed in 'public', with no acknowledgement of the blurring of the boundaries between public and private. Such exposed information would not qualify for protection under the restated tort, even though observation, in particular through technical means, may well be unexpected to the observed and lead to investigation of the individual and so to intrusion.

Finally, Austin criticises reliance on tort liability and its focus on wrongs, instead proposing that privacy should be thought of in terms of powers.[153] Taking ideas from the law of search and seizure, Austin proposes that the relationship of power that the surveilling party holds over the other should be recognised and regulated accordingly (the 'power-over' analysis).[154] Linked to this is Austin's 'power-to' analysis, that the law should facilitate individuals' ability to do things that they otherwise would not be able to, rather than protecting them from harms.[155] Austin suggests that such a restatement would lead to positive privacy obligations being imposed on information intermediaries to secure the conditions for individual self-presentation[156] and to broad access rights for individuals to data profiling techniques.[157]

A new private: misuse of the digital person

Building on the four proposals outlined above, this article suggests an alternative model that could tackle some of the modern day Jordan's privacy concerns. The model recognises that information or activities do not have to be secret or unexposed for privacy issues to occur, while avoiding a structure that involves the deletion or hiding of information already available in the public domain. Instead, it considers what might be the most personal or 'private' of information or activities, even if these are exposed online or digitally, and how an individual might be protected from inappropriate intrusion based on the exploitation of this information to de-anonymise, make links or generate presumptions. Protection would not rely upon technological functionality or concepts of obscurity online (often dependent on the individual's knowledge of such technological functionality) although efforts to obscure information could be a helpful factor in determining difficult issues on the boundary. The model would move away from the concept of data controller, preferring that responsibilities should apply to all. Tort law would appear to provide a promising avenue for implementation although Austin's criticisms of a tort approach are acknowledged, and consideration given to how a new model could move away from the concept of harm. In terms of intermediaries, publication or communication would be a mere factual requirement for the tort, reflecting Oster's reconceptualisation of intermediary liability for defamation.[158] Defences relating to 'innocence' would be limited to intermediaries which had not participated in, facilitated, activated or controlled the misuse.

Could the tort of misuse of private information be adapted to reflect above? Misuse of private information was confirmed to be a tort in England and Wales by Tugendhat J in

[153]Lisa M Austin, 'Enough about Me: Why Privacy Is About Power, Not Consent (or Harm)' in Austin Sarat (ed) *A World Without Privacy* (Cambridge University Press, 2015) 177.
[154]ibid 160–61.
[155]ibid 160.
[156]ibid 180.
[157]ibid 182.
[158]Jan Oster, 'Communication, defamation and liability of intermediaries' (2015) 35(2) Legal Studies 348, 349.

Vidal-Hall.[159] The judge also stated that damages for distress are recoverable in a claim for this tort[160] and as seen in the *CG* case, a tortious claim can be brought against individuals and organisations alike. A new understanding of 'private' would be required however (replacing the reasonable expectation of privacy test) and the above model might be better summarised as misuse of the digital person. It would include the following elements:

(a) Certain information about individuals (see (b)) exposed digitally or available to the 'masses' on the Internet, or which can be generated from such information, should no longer be regarded as 'public' in the sense of there being no privacy in respect of it;
(b) The above principle would apply to digital information/information online that represents the fundamentals of a person (such as name, location, family, health, beliefs and image, see the suggestions in Figure 1). The extent to which information about a person's job, public persona and criminal/civil offences fall within the fundamentals of a person would have to be agreed (see Areas marked * on Figure 1). This would provide an opportunity to develop clearer statutory principles as to when, for instance, offences recede into the past and become part of a person's private life[161] (and so part of the fundamentals of a person). This model could exist in parallel with the 'right to be forgotten' in *Google Spain*; the principles surrounding the fundamentals of a person may serve to inform the circumstances in which links to material should be deleted;
(c) The fundamentals of a digital person would be regarded as 'private'; 'private' as applied in this model would not depend upon information being hidden or unseen but on whether it fell within one of categories representing the fundamentals of a person. If it did, only certain actions would be permitted in respect of it, thus reflecting Austin's concerns over the power that the surveilling party holds over the other and so regulating at the point of action;
(d) Discernible digital information that falls within the fundamentals of a person (for instance, a blog in which a person expresses their views and talks about their life) can be viewed, read, searched, stored, linked to and reported upon, but not further used (unless an exception applied) to generate new information or intelligence about an individual that falls within the fundamentals of a person (profiling the person based on blog contents in this example);
(e) It would not be permitted (unless an exception applied) to generate new information or intelligence about an individual that falls within the fundamentals of a person, i.e. information that was not already apparent from the disclosed information. Consequentially this would mean, for instance, that it would not be permitted to use facial recognition to identify an individual from an anonymous image, identify an anonymous author of a blog, track location from Tweets or from location data generated by a smart phone to try to determine residence, or deduce health conditions from a fitness app for the purposes of a life insurance quote;
(f) Application of the above principles would not depend upon falling within the definition of 'data controller' under the DPA; the rules would apply to all;

[159] *Judith Vidal-Hall & ors v Google Inc* [2014] EWHC 13 (QB) [70].
[160] ibid [74].
[161] *R(L) v Commissioner of Police of the Metropolis (Secretary of State for the Home Department intervening)* [2009] UKSC 3 [27].

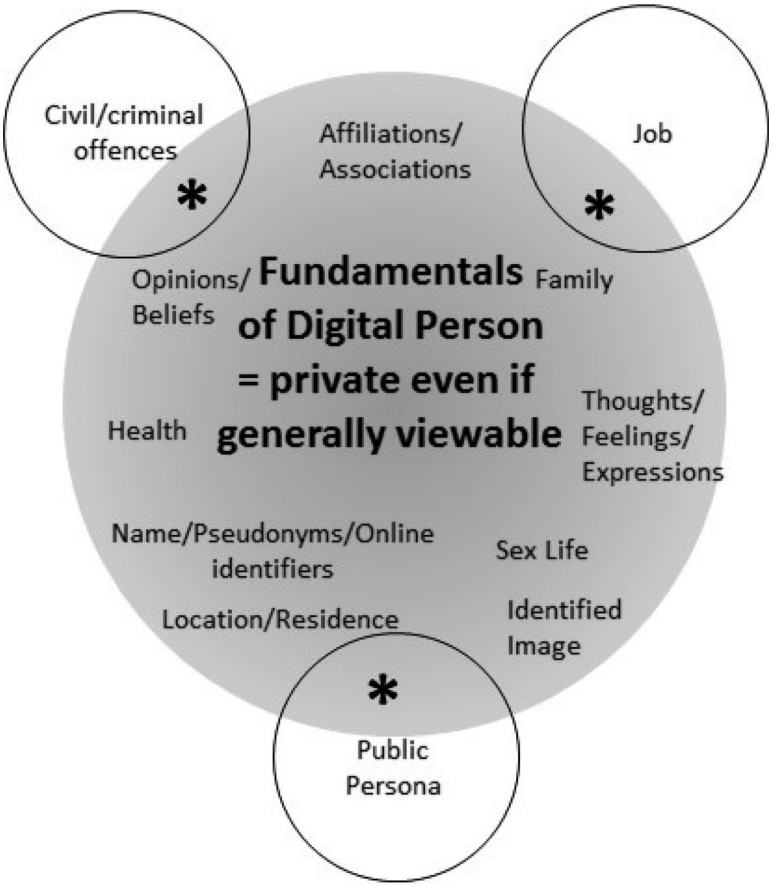

Figure 1. Fundamentals of a digital person.

(g) Public interest exceptions (for journalistic activities and media freedoms in particular[162]) must apply. If an exception were to be based on consent, this would require careful crafting in order to avoid the unavoidable and increasingly meaningless 'click-to-agree' approach to privacy compliance that tends to exist today, and consideration given to what additional powers individuals would require in order to rebalance the relationship with surveillers.

The advantages of the above model (and a number of issues) might be said to include the following:

(i) It is technology-neutral. The principles in (d) and (e) above consider the elements of a person's identity deserving of privacy protection rather than regulating particular technology that might interfere with privacy;

[162]See András Koltay, 'The Concept of Media Freedom Today: New Media, New Editors and the Traditional Approach of the Law' (2015) 7(1) J Med L, 36 exploring the extent to which new media players might claim protection under the right to media freedom.

(ii) It can tackle many of the privacy problems that Solove identifies in his Taxonomy of Privacy[163] – surveillance, interrogation, aggregation, identification, disclosure, distortion, intrusion, decisional interference – without the need to define an exhaustive list of these problems or activities. Instead the approach focuses on the aspects of an individual which are the most fundamentally personal;

(iii) Public interest and other exceptions can be determined based on cultural and societal norms. This model requires the public interest to be assessed by the person or organisation responsible for the activity (appealable to the court or regulator). This is not to underestimate the challenges of determining appropriate public interest exceptions and the jurisdictional conflicts that would arise. It is beyond the scope of this article to explore this in any detail. Suffice to say that the question of whether what some might regard as trivia, gossip or entertainment should be regarded as in the public interest would have to be determined decisively[164];

(iv) The model does not attempt to hide or delete information that is already available in public, thus having regard to freedom of speech considerations. It would not regulate the taking of digital photographs per se or the posting of these online unless the individual was identified from the image. However unpalatable the site may seem, 'Women who eat on tubes' would not of itself be prevented but the identification of the anonymous women in the photographs would be regulated under the new model.

Information and images that relate to an individual's job or public persona would not be regulated unless the matter fell within Areas * on Figure 1. Thus the information exposed in the *Huff* case would most likely fall outside the model, not because of the nature of the technology but because of the work-related nature of the information. Determining the boundaries of these Areas has the potential to cause considerable uncertainty and debate however. Identified photographs of Jordan lunching with her children would seem to fall squarely within fundamentals of a person. On the other hand, Jordan's attendance at Gatsby's large party, no doubt a glittering 'A-list' affair, would most likely fall outside Area *, a determination to displease Jordan but probably the right one;

(v) The model would require online service providers and intermediaries to take a hard look at their business practices and to implement changes to reflect the new requirements, for instance, to prevent tagging of previously anonymous digital photographs. The model does not however address all undesirable data gathering practices (such as the one recently announced by Spotify: a change to its privacy policy to allow the service to access contacts held on a user's smart phone[165]);

(vi) Although there is a partial overlap with the definition of sensitive personal data under EU data protection law, the model is not consent-based (and avoids the implication that 'public' equals consent) nor does it rely on the application of the data controller definition.

[163]Solove (n 5) 103–70.

[164]See Rebecca Moosavian, 'Deconstructing "Public Interest" in the Article 8 vs Article 10 Balancing Exercise' (2014) 6(2) JML 234.

[165]Zoe Kleinman, 'Spotify Says Sorry after Privacy Policy Anger' BBC News (21 August 2015) <http://www.bbc.co.uk/news/technology-34016658> accessed March 2016.

In terms of translating the above approach into law, Reed argues that the law-maker must achieve respect for any law operating in cyberspace, and to do so must ensure that the cyberspace actor recognises the law's obligations as having some sensible meaning (understandable, possible to obey, with a clear connection between the obligations and the law's normative aim).[166] It should be recognised that the law in cyberspace rarely achieves control of a user's activities; instead the primary aim should be to influence and persuade.[167] Influence and persuasion would be the main aim of the above proposal, bearing in mind the difficulty of enforcement against individual cyberspace actors. Action could be more realistically taken against intermediaries, and in this way, provide a strong incentive for intermediaries to change online structures and so indirectly influence the behaviour of individuals. It is to be hoped however that a law-maker would be pushing against an open door in terms of the proposal's normative aim. The case-law and research reviewed in this article indicate that there is an increasing awareness of the privacy impact of new technologies, and of the need to revisit the definitions of public and private as they apply to the Internet. Indeed, a private member's Bill sponsored by Liz Saville Roberts MP has at the date of writing had its first reading in the UK House of Commons aimed at consolidating offences relating to digital crime.[168] The Bill also aims to introduce new offences relating to surveillance and monitoring, for instance, using a digital device to repeatedly locate, listen or watch a person without legitimate purpose[169] or to take multiple images of an individual unless it is in the public interest to do so and where the intent was not legitimate.[170] These proposals have some similarities with the model set out in this article, although this model attempts to be technology-neutral and to focus not on the action – listening, locating or watching – but on what fundamentally personal elements are created through such activities and how these can be protected. It reflects Miller's call for consideration

> to be given towards digital … components of self as matter of being or part of the self, not as 'representational of' or 'information about' persons. Such a shift in thinking is necessary to give personal data 'ethical weight' and thus maintain any prospect of privacy.[171]

Compliance with such new model may be self-fulfilling if the law represented a set of principles that individual cyberspace actors believed in, or could be persuaded to believe in. We ourselves might be initially resistant, having become used to environment in which we can post digital photos of anyone, Tweet comments about others and 'Google' someone at will. We might regard this proposed model as representing 'a sort of elitist condescension of, or distaste for, the "masses"'.[172] We might therefore need convincing that most of our day-to-day online activities would not be prevented. Even more strident resistance is likely to come from those businesses operating in the behavioural advertising field, those funded by such advertising, and those using Big Data analysis of individual

[166]Reed (n 132) 221.
[167]Reed (n 132) 222.
[168]Criminal Offences (Misuse of Digital Technologies and Services)(Consolidation) Bill 2015–16 <http://services.parliament.uk/bills/2015-16/criminaloffencesmisuseofdigitaltechnologiesandservicesconsolidation.html> accessed March 2016.
[169]ibid clause 8.
[170]ibid clause 10.
[171]Vincent Miller, *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life* (SAGE 2015).
[172]Moosavian (n 164) 254.

profiles to inform decision-making. The model would allow exceptions to the principles to reflect acceptable commercial practices however, with the drafting of such exceptions providing an opportunity for an open and large-scale review of information practices online.

Conclusion

To return to Jordan's dilemma – whether large parties can still be intimate – this article concludes that they can be, or at least they could be. Social media, Internet search tools, facial recognition and profiling technologies are the digital equivalent of an ever-present long lens. These digital intrusions are now part of our world, whether real or digital. Jordan cannot ever hope to be as free from detailed scrutiny in the twenty-first century as she was at Gatsby's large party in 1925. Our information-rich society has many positives in terms of transparency, knowledge-dissemination and freedom of speech, yet the exponential growth in digital and Internet technologies has had a rather invidious effect on perceptions of public and private. It is time to question the common assumption that being online and operating with digital technologies are the equivalent of being seen physically in public. Being observed on the street is generally down to chance; being connected digitally attracts a much higher degree of systematic observability, potentially impacting on the relatively anonymous nature of walking down the street in the real world. The model proposed in this article recognises this. It does not attempt to prevent the observation taking place. Instead it proposes that society should define the things about a person that we care about the most – the fundamentals of a person – and protect that from undesirable digital intrusion. In this way, the model could offer a potentially multi-jurisdictional way of influencing attitudes and ultimately changing behaviours.

Disclosure statement

No potential conflict of interest was reported by the author.