J Consum Policy (2018) 41:55–75
https://doi.org/10.1007/s10603-017-9364-x

ORIGINAL PAPER

Consumer Protection in Cyber Space and the Ethics of Stewardship

Theresa E. Miedema [1]

Received: 9 January 2016 / Accepted: 12 October 2017 / Published online: 27 October 2017

Abstract This paper explores how consumer protection is evolving in the information-communications technology (ICT) sector. Traditionally, consumer protection law regimes are vertical in design and somewhat paternalistic in attitude. Requirements are imposed by governmental agencies on providers of goods and services with a view to protecting consumers. In many cases, consumers are not actively engaged by regulatory regimes in their own protection and may not be able to contract out of provisions designed for their protection. In the context of internet-based activities, however, a paradigm shift is necessary to protect not only the individual consumer but the wider network of consumers using the internet. This paper explores what consumer protection should look like in our hyper-connected, online world. Its central argument is that a new sort of model is necessary for consumer protection in the ICT sector. In the context of internet-based activities, regulators must engage consumers on a horizontal level as co-stewards of the internet. This involves more than just education about the risks of malware and online scams. The consumer protection framework must draw consumers into its structure as proactive agents working collaboratively with government, internet service providers, and other stakeholders to promote cyber security.

Keywords Law · Information-communications technology · Consumer protection · Cybersecurity · Stewardship

This paper explores how consumer protection is evolving in the information-communications technology (ICT) sector. Consumer activity on the internet, from accessing emails to posting on social media to purchasing goods and services online, has heightened the vulnerability of consumers to scams, hacking, and malware. Consumers' devices and the data and personal information on their devices are at risk in an increasingly always-on, connected world.

At the same time, uninformed consumers pose a risk to the internet; malware can render an unsuspecting and an under-protected consumer's computer a so-called "zombie

✉ Theresa E. Miedema
theresa.miedema@uoit.ca

[1] Trinity College in the University of Toronto, 6 Hoskin Ave, Toronto, ON M5S 1H8, Canada

computer." Consumers may unwittingly become drawn into a botnet attack, where their devices are used by a third party to send spam or to participate in a distributed denial-of-service (DDoS) attack. In October 2016, what appears to be the largest cyber attack in internet history took down Dyn servers using a DDoS attack (Woolf 2016). (Dyn controls most of the domain name system on the internet (Woolf 2016) and offers associated network and traffic services.) The attack disrupted popular social media sites like Twitter and Pinterest, streaming services such as Netflix and Spotify, commercial sites such as PayPal, and news media outlets including the Guardian, the New York Times, and the Wall Street Journal (Thielman and Johnson 2016). This attack was so significant that it triggered an FBI investigation into what had happened.

While the October 2016 attack was the largest DDoS attack, such attacks are relatively common. Past targets have included: GreatFire, which uses mirror sites to sidestep China's internet censorship measures (Brandom 2015); GitHub, one of the world's largest code hosting websites (Brandom 2015); the Telecommunications Regulatory Authority of India ("TRAI website down, Anonymous India claims responsibility" 2015); the Canadian government (Chase 2015); and the Polish air carrier LOT, which was forced to cancel ten LOT flights and delay several others, stranding or delaying approximately 1400 passengers in Warsaw (Szary and Auchard 2015). A week-long attack on the networks of the biggest school district in Idaho, the USA, affected everything on the school district's network, from virtual teaching to standardized testing to payroll (Abel 2015). In short, DDoS attacks have affected a very wide range of websites around the world, from commercial companies to transportation to government to civil society organizations.

In each of the above examples, the computers of ordinary users were drawn into the attacks through the use of malware. Malware and botnets are not merely nuisances and mischief. They pose an increasing threat to the internet as a whole and every computer system that is networked to the internet, from school systems to government to financial institutions to critical infrastructure.

This paper explores what consumer protection should look like in our hyper-connected, online world. Its central argument is that a new sort of model is necessary for consumer protection in the ICT sector. In the context of internet-based activities, regulators must engage consumers on a horizontal level as co-stewards of the internet. This involves more than just education about the risks of malware and online scams. The consumer protection framework must draw consumers into its structure as proactive agents working collaboratively with government, internet service providers, and other stakeholders to promote cyber security.

Traditionally, consumer protection law regimes are vertical in design and somewhat paternalistic in attitude. Requirements are imposed by governmental agencies on providers of goods and services with a view to protecting consumers. In many cases, consumers are not actively engaged by regulatory regimes in their own protection and may not be able to contract out of provisions designed for their protection. In other words, consumers are passive recipients of protection. There are often good reasons for these regulatory frameworks. In the context of internet-based activities, however, a paradigm shift is necessary to protect not only the individual consumer but the wider network of consumers, businesses, and public institutions and infrastructure that use the internet.

This paper begins by providing a brief overview of botnets and DDoS attacks in the next chapter. The chapter "Trends in Consumer Protection Against Online Threats"

reviews current approaches to consumer protection online. "A New Model for Consumer Protection Against Online Threats" argues that consumers should be viewed as co-stewards of the internet and provides both ethical and legal arguments in support of this view, followed by a conclusion.

Botnets and Distributed Denial of Service Attacks

Consumers face a myriad of threats online. Identity and data theft, fraud, and infection by malicious worms and viruses are common and generally known risks. Malware that draws a consumer into a botnet is a more subtle, though no less dangerous, threat. Computers become infected by malware that may have come from any one of a wide range of sources, including an email, a website, and social media sites, for example.

A "bot" (short for robot) is a computer[1] that has been infected by malicious code (malware) that allows the computer to be controlled remotely by a "bot master," that is, the orchestrator of the botnet. This control is exercised without the owner of the device being aware that the device has been compromised. Networks of infected computers are called botnets. Botnets can be used for a range of illicit purposes, from the more benign, though highly inconvenient (e.g., spam) to the intrusive (e.g., identity theft, keylogging, and sniffing traffic) to socially and politically disruptive ends (e.g., distributed denial of service attacks). Of the malicious uses for botnets, distributed denial of service (DDoS) attacks currently pose the greatest concern.

A DDoS attack occurs when the target victim's website or online service is overwhelmed by internet traffic from multiple sources, which renders the website or service unavailable to its legitimate users. The objective is to bring the online service or website offline ("Understanding DDoS" n.d.). The attack is made possible by synchronizing the infected devices within a botnet so that traffic from all the infected computers bombards the website or online service at the same time. The sudden tidal wave of internet traffic from the botnet typically overwhelms the ability of the victim's system to function.[2]

DDoS attacks are not aimed at stealing or destroying confidential information (Goncharov 2012, p.8). Instead, they seek to paralyze a website or service, to bring it offline, and to disrupt its legitimate uses (Goncharov 2012, p.8). DDoS attacks can (and do) cause major social, economic, and political disruption. It is difficult to quantify the economic losses stemming from DDoS attacks.[3] However, Neustar, a major provider of IT/security services, reports that 32% of businesses estimate that they would lose over $100,000 per hour for every hour that their site is down in peak business hours; over 10% of

[1] This paper will refer primarily to computers as the device that becomes infected in a botnet. However, as more and more devices become connected to the internet, botnets will grow to include all such devices. Mobile devices and routers, for example, are already susceptible to malware infection that would render such devices part of a botnet.

[2] For an overview of the different types of DDoS attacks, see Understanding DDOS (n.d.), retrieved May 5, 2015 from www.digitalattackmap.com/understanding-ddos and see "DDoS Attacks" (n.d.), retrieved June 24, 2015 from https://www.incapsula.com/ddos/ddos-attacks/.

[3] In a 2008 report, for example, the OECD noted the difficulty of calculating the economic costs of malware and botnets. See: OECD (2008). *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy.* Paris: OECD. doi: https://doi.org/10.1787/9789264056510-en.

companies would lose more than $1million per hour (Neustar 2015).[4] In addition to the economic costs, DDoS attacks can affect political processes, as seen in the Canadian New Democratic Party leadership elections in 2012 (LeBlanc 2012). They also pose a significant risk to critical infrastructure; any infrastructure system that is connected to the internet (e.g., telecommunications, hydro-electricity, water, financial services, air traffic control, railways, and so forth) is at risk as a potential target (Ingersoll and Kelley 2013). Indeed, in 2011, CIA Director Leon Panetta commented that "the next Pearl Harbor we confront could very well be a cyber attack that cripples that cripples our power systems, our grid, our security systems, our financial systems, our government systems" (2011).

Botnets account for more than half of all internet traffic ("61.5% of Web Traffic Comes from Bots" 2013). Arbor Networks (2014), a major provider of protection against online threats, reports that it observes more than 2000 DDoS attacks worldwide each day. A report released in May 2015 found that DDoS attacks had more than doubled in the previous 12 months (Seals 2015). There is a thriving black market for botnets capable of initiating DDoS attacks. DDoS-capable botnets can be purchased or even rented for a few hours. For as little as USD $10, a person can rent a DDoS-capable botnet for 1 h; rates for renting a botnet for a week are as low as USD $150 (Goncharov 2012, p. 8). As the International Telecommunication Union (2009) has stated, "Bot-networks are…thus a real threat to all internet-connected systems and have a central role in the cybercriminal world" (p. 40). The OECD (2012) has echoed this concern, stating that botnets erode security and trust in online environments: "[t]heir growth and increased severity would do considerable damage to online commerce, electronic government services, and other online services, as consumers and citizens would become more reluctant to interact and transact online" (p. 10).

Trends in Consumer Protection Against Online Threats

While computers have existed for many decades, the public internet is a relatively new phenomenon. The public began to be able to access the internet in the 1990s, with the first web page being launched on August 6, 1991 (Rustad and D'Angelo 2011, para. 11–12). In the 25 years that the internet has been accessible to the public at large, governments and courts have struggled to keep up with the pace of technological innovation and change. As a result, consumer protection regimes are still evolving, and some consumer protection measures are woefully inadequate.

The consumer protection issues that typically arise in the context of the internet fall into four categories: privacy (including the use of personal information), accessibility (including quality of service), security, and property (including the ownership of one's own personal information). In each category, regulatory frameworks focus on protecting consumer interests, although such protection may require balancing consumer interests with other important concerns such as the interests of network providers and the public as a whole. The idea that stakeholders like network providers, online retailers, and even the government may need

[4] A 2014 Imperva study estimated that the average cost of a DDoS attack was $500,000 (Matthews 2014, p.8). This figure is based on the average business's loss per hour, which, according to this study, is approximately $40,000 and on the average length of a DDoS attack. According to this study, 49% of DDoS attacks lasted between 6 and 24 h. see Matthews 2014, p. 8. The Ponemon Institute found that the cost of a DDoS attack ranges from $1 to $100,000 per minute of downtime, with an average cost of about $22,000 per minute, with the average DDoS attack lasting just under 1 h (Ponemon and Radware 2012).

protection from infected computers of consumers is not yet a common or salient feature of consumer protection regimes.

At present, the typical consumer protection regime is vertical in nature, with government having the super-ordinate responsibility for overseeing and enforcing measures designed to advance consumer interests, and consumers situated as the largely passive recipients of these measures. Infrastructure and service providers occupy the middle ground between government and consumers, and carry the bulk of the obligations related to consumer interests. There are at least three different approaches to advancing consumer interests within this vertical paradigm: measures designed *to protect* consumers from risks online; measures designed *to equip* consumers to undertake activities online, especially e-commerce; and measures designed *to engage* consumers in the information society. Many regimes, especially in developed economies, feature a combination of all three approaches.

Protecting Consumers

Historically, consumer protection laws have been aimed at prohibiting certain types of unscrupulous commercial practices and creating a level playing field for consumers. For example, prohibitions on misleading advertising, rules about clauses in consumer contracts, especially standard form agreements, rules about the merchantability (or fitness for use) of consumer goods, product safety, protection against fraud, and the regulation of consumer debt are staples of a consumer protection regime in a developed economy. The internet has not changed the need for these types of protections, although it has required countries to ensure that their legislation and regulations take into account increasing online activities. So, in the case of prohibitions on misleading advertising, for example, governments have had to ensure that consumer protection laws include communications made on websites and social media and in commercial emails.

The internet has also given rise to new threats and consumer inconveniences, such as hacking, spyware, and spam. Some of these issues are addressed in criminal law, while others are the subject of consumer protection regimes in the ICT and privacy law sectors. Destructive activities such as computer-related fraud, hacking, and the distribution of viruses and malware tend to attract robust legislative prohibitions and, in fact, have led to the recognition of a new, modern vice: cybercrime. Many countries have adopted new legislation or revised existing legislation in order to criminalize activities associated with computer-related fraud, hacking, and the distribution of malware and viruses.[5]

One of the biggest consumer concerns in the internet age is the protection of personal privacy. Consumers' activities online can be tracked with relative ease, and their activities tell a great deal about an individual and that individual's personal interests. Companies have proven to have an insatiable appetite for gathering such data. Automated mass marketing (e.g., spamming) invades consumers' private lives. Participation on social media allows others to track where a consumer may be at any given time, for example, through geo-tagging functions. Spyware is even more invasive, as it allows remote operators to "spy" on an individual through

[5] For a good review of strategies adopted around the world to address cyber-crime, see Levin et al. (n.d.). Securing cyberspace: a comparative review of strategies worldwide. Toronto: Ted Rogers School of Management, Ryerson University, Privacy and Cyber Crime Institute. Retrieved from http://www.ryerson.ca/content/dam/tedrogersschool/privacy/AODAforms/Ryerson_cyber_crime_final_report%20AODA.pdf.

the internet connection on her computer, including the ability to watch the individual by accessing the camera function on the computer.

Consumer protection regimes feature a spectrum of different measures designed to address the personal privacy concerns of consumers in cyber space. On the more protective side of the spectrum, some jurisdictions have recognized rights held by individuals to their personal privacy. For example, in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, and Mario Costeja González* (2014), the Court of Justice of the European Union formally recognized the "right to be forgotten," that is, the right to have links to information about oneself removed from search engines where the related information is outdated, inaccurate, irrelevant, or excessive for its purpose. The EU Court's decision was based on rights established in the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281, Article 12).[6]

While there has been recognition of the consumer as a rights-holder where personal privacy is concerned, the more common approach to regulating internet issues where privacy may be affected is to recognize the agency of consumers by adopting consent-based mechanisms. This approach has been applied to matters such as the collection of personal data online, the installation of computer programs (including malware), the use of cookies,[7] and the use of automated mass-marketing tools such as robo-calls and spamming.

In some cases, a practice is prohibited unless the consumer is notified and consents in advance to the action. Consent in such cases must be fully informed and is typically "opt-in," where the consumer must do something (e.g., tick a box) to demonstrate that she does, in fact, consent.

The EU Data Privacy Directive (Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281) and the EU Directive on Privacy and Electronic Communications (Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201), for example, restrict all direct marketing communications, whether by automated telephone calling machines, fax, or email, and require that businesses obtain consent in advance of contact using an "opt-in" model.[8] In other cases, countries allow consent to be implied from a person's conduct (e.g., clicking on a link may be interpreted as consenting to some action); consent may also be presumed unless an individual explicitly "opts-out" by taking some action to request that a practice not be applied to her. Jurisdictions such as the USA, Australia, and New Zealand restrict activities such as spamming using an "opt-out" model for consent.

[6] Note that the Data Protection Directive is currently under review, as the EU seeks to update this Directive to address digital communications in the Internet age.

[7] A "cookie" is a text file that is downloaded onto a user's device (e.g., desktop or laptop computer) when the user accesses a website. Cookies are non-executable files and, as such, cannot contain malware or viruses. A cookie stores some information about the user's preferences and allows the website to recognize the user and the user's preferences if and when the user returns to the website.

[8] Note that there are limited exceptions to the requirement to obtain explicit consent in advance of communications; in some limited cases, businesses can rely on implicit consent, based on previous communications with an existing customer. Similar exceptions exist in Canada.

Equipping Consumers

In the internet-era, consumer protection regimes have evolved to include measures designed to equip consumers to participate in online activities, especially e-commerce. As countries have recognized the potential of e-commerce to drive economic growth and innovation, they have taken steps to ensure that barriers to e-commerce are addressed. A key step in this regard is ensuring that consumer protection legislation is updated so that its provisions clearly apply to e-commerce transactions. This ensures that consumers are not deterred from engaging in e-commerce by the fact that they have less rights in the online world than they would in brick and mortar retail outlets.

Aside from updating legislation so that statutory protections against things like misleading advertising, unfair contractual terms, and unsafe products apply to internet-based transactions, consumer protection regimes largely focus on facilitating e-commerce. This facilitation includes updating or creating law to address the nature of commerce on the internet. For example, as consumers began to enter into contracts online, it was necessary to clarify that electronic signatures carried the same legal weight as handwritten signatures.[9] Indeed, at a more basic level, it was necessary to clarify that parties could enter into contracts online! These types of legal measures are not prohibitive, restrictive, or prescriptive, per se.[10] Instead, they are designed to provide legal certainty about a new form of commercial activity and thus to equip consumers to carry on their lives in the internet era.

Consumer protection regimes also facilitate online activities such as e-commerce by educating consumers about a myriad on internet-related issues. These issues include, for example, consumer rights in cyberspace, how to protect oneself from scams online, how to avoid infecting one's computer systems with malware, how to protect privacy online, and how to reduce the risk of having one's identity stolen. Many governments, for instance, Canada (Industry Canada n.d.), New Zealand (Consumer Affairs New Zealand n.d.), and the USA (Federal Trade Commission n.d.) have developed consumer protection websites that include sections devoted to activities on the internet. By educating consumers, governments seek to help consumers protect themselves and thus to equip consumers for life in the internet era.

Engaging Consumers

As governments have recognized the need to protect critical infrastructure and the economy from cyber attacks, they have begun to engage with consumers as critical stakeholders in cyber space. While national cyber security strategies extend beyond just consumer protection, they are one of the best examples of measures that involve engaging consumers in efforts to mitigate the risk posed by malware.

[9] See, e.g., Singapore, *Electronic Transactions Act* (Cap 80), Act 16 of 2010; Japan, *Law Concerning Electronic Signatures and Certification Services*, 2000; Ghana, *Electronic Transactions Act, 2008,* Act 772 of 2008; US, *Electronic Signatures in Global and National Commerce Act,* 15 U.S. Code Chapter 96 (2000); UK, *Electronic Signatures Regulations 2002*, 2002 UKSI No. 318; and Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1999] OJ L13.

[10] One can, however, extrapolate certain "Best Practices" from these measures that should be followed in order to ensure that a contract created online will be fully enforceable. It is not the case that every click of a mouse will automatically bind a consumer to every single term in an online contract, just as it is not the case that a signature on one page of a contract will absolutely bind the signor to every single clause in the contract.

In general, most countries have not adopted top-down government regulations that mandate the use of proper protection against malware, screening for malware, or notification regimes to advise users that their devices have been compromised. Instead, many countries have relied on private industry to lead the way in reducing the risk of botnets and responding to infected devices. An OECD study on governmental responses to botnets found that regulatory mechanisms to address botnet attacks include industry codes of practice, self-regulatory covenants, and best practice guidance (OECD 2012, p. 9–10). There are no jurisdictions that require consumers to take active measures to protect their devices against malware infection, nor are there requirements imposed on consumers about how to respond when they discover their device has been infected. Countries do, however, tend to take measures to educate consumers about the risk of malware infection and the steps that consumers can take to reduce infection by malware (OECD 2012, p. 12).

Governments around the world are, however, being urged to develop and to implement National Cyber Security Strategies (NCS Strategies) by organizations such as the International Telecommunication Union (ITU), European Union Agency for Network and Information Security (ENISA), and the World Summit on the Information Society (WSIS).[11] As reports from both the ITU (Wamala 2011) and ENISA (2012) illustrate, trends in the development of NCS Strategies suggest that developing a "national culture" of cyber security awareness is an important theme, one which engages consumers as stakeholders in cyber security. Countries that have adopted an NCS Strategy, including, for example, the UK (2011), Kenya (2014), and Singapore (2013), have recognized the need to increase the public's understanding of cyber threats and how to protect oneself (and others) online. Some countries such as the Netherlands (2013), Japan (2013), and the UK (2011) have expressed the expectation that citizens should exercise some basic level "cyber hygiene" online, such as using reasonable care in installing updates and using strong passwords to protect devices.

NCS Strategies represent a potential tipping-point in how consumers engaged in online activities are viewed. NCS Strategies tend to recognize individuals engaged in online activities as stakeholders alongside of industry and the government. Moreover, these strategies have begun to discuss the fact that individuals, as stakeholders, also have a role to play in maintaining cyber security. As some countries have begun to discuss the idea of "cyber hygiene" and the expectation that individuals will exercise basic prudence online, it is possible that we are seeing the beginning of a necessary shift in how we conceptualize consumers in the internet era.

A New Model for Consumer Protection Against Online Threats

Existing approaches to consumer protection on the internet are largely top-down and regulatory in nature. They have evolved from an era when the threat to consumer interests largely sprang from industry, not other consumers, and when the threat itself could be relatively contained. And so consumer protection measures have focused on prohibiting or restricting certain types of activities, updating legislation to account for online activities, and educating

[11] Some academics have also made the case for adopting multi-stakeholder approaches to cyber security. Asllani et al. (2013), for example, argue that cyber security ought to be viewed as a public good. As such, individual internet users have an ethical obligation to implement good cyber security controls in order to help protect national security.

consumers about the risks they face online. A key focal point is the relationship between the consumer and the business entity with which the consumer is dealing.

The internet era has changed the risk profile of the consumer because the consumer now poses a potential threat to service providers, businesses, other consumers, public infrastructure, and government. Indeed, as concerns about cyber security grow, the threat could extend to affect national interests. Accordingly, the existing model of consumer protection, where the government oversees the relationship between consumers and businesses to ensure that the consumers' interests are adequately protected, must evolve to keep pace with life in the internet era. The vertical relationship between the government and the consumer as protector and protectee must, in some respects, flatten such that consumers are more directly engaged in safeguarding their own interests (as well as the interests of others who are affected by consumer activity). Indeed, given the nature of the internet itself, the way that we conceptualize ordinary individuals who access the internet must change. Rather than characterizing such individuals primarily as consumers (and therefore entitled to a myriad of considerations and protections), we must begin to understand such individuals as co-stewards of the internet. We must begin to shift our thinking to include the idea that consumers have a responsibility on the internet to act in ways that promote the health and good functioning of the internet as a global resource.

In this section, I will develop two arguments in support of adopting an approach to consumer protection on the internet that centers on treating the consumer as a co-steward of the internet in a horizontal, cooperative relationship with regulators. In particular, I will outline an ethical argument supporting this model and review key aspects of its legal dimensions.

The Ethical Argument

The ethical argument that supports a shift to a stewardship model for consumer protection on the internet is rooted in the intersection of internet ethics,[12] the internet invariants, and the ethics of consumer protection itself, including the concept of consumer social responsibility. To understand the nature of the ethical dilemma and the values that are at stake, we begin with internet ethics. Internet ethics can be understood broadly as the ethical expectations that govern how people should act when accessing the internet and the expectations about how the internet itself should be structured (Onyancha, 387). Moor's classic 1985 discussion of computer ethics[13] provides an important conceptual touchstone in the development of internet ethics. Moor defined computer ethics as the "analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology" (Moor 1985, p.266). Moor understood computer ethics to be a broad set of considerations encompassing both personal and social uses of computer technology (Moor 1985)

[12] It is important to note that there is ongoing discussion and debate about the meaning of the terms "internet ethics," "computer ethics," and "cyber ethics." While there is emerging consensus that these terms are not synonyms, the scope of each term is not clear and, consequently, the inter-relationship among the terms is a matter for debate. For the purposes of this paper, I will use Internet ethics to refer to the ethical expectations about how the internet should be structured and how people should act when accessing the internet. Moreover, internet ethics overlaps with computer ethics to the extent that there are ethical expectations about the devices that are connected to the internet. For a good overview of how the aforementioned terms are developing and being used in the academic literature and online, see: Onyancha 2015; also Spinello and Tavini (2004).

[13] Note that Moor wrote this essay before the public Internet became available. It would not have made sense for him to write about internet ethics or even to consider the ethical dimensions of the Internet given the time in which he was writing.

For Moor (1985), the computer revolution, and the novel ethical issues it raised, is driven by the logical malleability of computers, that is, that fact that computers "can be shaped and molded to do any activity that can be characterized in terms of inputs and outputs, and connecting logical operations" (p. 269). For Moor (1985), this trait means that the computer "is the nearest thing we have to a universal tool". Moor foresaw the ubiquity of computers in all aspects of our present lives, some 30 years later. He predicted, correctly, that computers would transform our basic institutions and practices, including our work. But Moor could not have foreseen the degree to which all devices would become interconnected and capable to communicating with each other.

Nevertheless, Moor did foresee that problems would arise from the internal processing of computers, which occur more or less invisibly to the average user. This invisibility allows unscrupulous users to engage in unethical conduct, such as the invasion of the privacy and property rights of others (p. 273). Concern for property rights and privacy has become a central feature (some might even argue *the* central feature) of computer and internet ethics.

Internet ethics has also been shaped by conceptions of the ethics of information technology (IT) and information systems (IS). Discussions of IT/IS ethics highlight the role of information in computer systems. Richard Mason (1986) has identified four central ethical issues in the information age. Mason takes a deontological approach to these issues, arguing that the social contract among people living in the information age must address these critical matters. Framing the core concern as one of protecting human dignity, Mason flags issues of property, accuracy, privacy, and accessibility (Mason 1986, pp. 5 and 11). Accessibility is particularly relevant; Mason articulates this issue as: "[w]hat information does a person or organization have a right or privilege to obtain, under what conditions, and with what safeguards?" (p. 5). Accessibility has become so critical to participation in modern society that in 2016, the United Nations passed a resolution declaring that access to the internet is a basic human right and is a necessary part of a comprehensive human rights framework; the resolution articulates the importance of the internet being "open, accessible, and nurtured" (G.A. Res. 32/L.20, *The promotion, protection and enjoyment of human rights on the Internet*., U.N. Doc. A/HRC/32/L.20 (June 27, 2016).)

The 2016 UN Resolution adds weight to a deontological understanding of internet ethics. As our daily lives intersect more and more with the internet and as access to the internet becomes increasingly important to being able to participate in civic life in the polity, rights to accurate information, our privacy, our digital property, and stable and safe access to the internet itself provide key touchstones for framing ethical obligations. And obligations are central to understanding the nature and scope of internet-related rights. Both Kant and Rawls, two of the most influential deontological thinkers, understood that there can be no rights without corresponding, reciprocal duties. The Kantian categorical imperative holds in part that rules must be universal: I cannot insist on a rule unless I would be willing to uphold that same rule for everyone else in parallel circumstances. The Rawlsian invisible curtain serves a similar function: what rights would I accept if I did not know what my station in life would be? Whatever rights I would accept in the polity in this conceptually blind-folded state must apply to all others.

With respect to a consumer protection model, a deontological internet ethics, then, supports a view that consumers have both rights and duties. Our right to the protection of our digital property, for example, implies an obligation to use the internet in such a way as to avoid infringing on the digital property rights of others. The same is true of accessibility rights. By extension, we ought to have an obligation to avoid doing things that could affect property

rights and accessibility rights (really all internet-based rights) of others. Such an obligation should extend to avoiding actions or omissions that could allow our devices to become part of botnets used to engage in DDoS attacks.

While a deontological framework supports imposing obligations on consumers as part of their internet rights, this framework alone does not fully explain why a change in the consumer protection paradigm is necessary. After all, it is possible to impose some obligations on consumers while still conceiving of a "consumer rights" or "consumer protection" paradigm. Supplementing a deontological understanding of internet ethics with a consequentialist approach cements the view that internet ethics requires a stewardship paradigm.[14]

The fact that a rights-based framework also emphasizes obligations provides a conceptual bridge to the need to draw on a consequentialist approach. Obligations related to rights on the internet, and for our purposes, especially those related to accessibility, require consideration of the possible consequences of certain actions in order to determine the nature and scope of the obligation. The harm that flows from the spread of malware is not trivial or merely inconvenient. Instead, as has been discussed above, the spread of malware and the growth of botnets put many people's personal data at risk, cause significant economic losses, and pose a real threat to a country's critical infrastructure. A successful DDoS attack could shut down a country's communications system, energy grid, water filtration plants, financial systems, government offices, and/or air traffic and other transportation control systems. The risk to national security from the spread of malware is very real.

The magnitude of the consequences that flow from malware support the position that consumers must take measures to safeguard against it. But again, why must consumers be cast as co-stewards of the internet in light of this harm? In this regard, it is helpful to take a step back to consider the nature of the internet itself. If we are to uphold a right to the internet (accessibility writ large) and a duty to take measures to mitigate the risk of harm, we must understand those core features of the internet that we protecting. For insight on this matter, it is helpful to consider the internet invariants. This discussion will also help to distinguish internet ethics from computer ethics and IS/IT ethics.

The internet invariants refer to a set of characteristics of the internet that have remained stable through time and that have allowed the internet to develop into the revolutionary "network of networks" that it is today (Daigle 2015). These features were identified by the Internet Society in 2012 as being what is "actually important and *unchanging* about the Internet" even as the internet itself has radically changed society (Internet Society 2012). The Internet Society argued that these features must remain constant as the internet continues to evolve or else the internet will become something less than what it currently is (Daigle 2015, p. 5). For the purposes of this discussion, the key internet invariants include:

[14] Moor (1999) argues that a unified theory of ethics that he calls "just consequentialism" is necessary to address the inherent weaknesses of the deontological and consequentialist approaches taken separately. While deontological and consequentialist approaches are often presented as "hopelessly incompatible" (p. 65), Moor argues that the complexities of computing require a blended approach that can take into account both justice and the possible consequences of a proposed policy. Moor suggests, "[w]e should develop computing policies in such a way that they are above all just. Then we can make the policies as good as reasonably possible. Our first priority should be to avoid unjustifiable harming of others by protecting their rights and then to increase benefit." (Moor 1999, p. 67). While I agree with Moor, I take a slightly different approach. I argue that it is necessary to consider the consequences of certain actions in order to understand and to define the extent of the duties we may owe to others.

- "Supports innovation without requiring permission (by anyone): Any person or organization can set up a new service, that abides by the existing standards and best practices, and make it available to the rest of the internet without asking permission."
- "Accessible—it is possible to connect to it, build new parts of it, and study it overall: Anyone can "get on" the internet—not just to consume content from others, but also to contribute content on existing services, put up a server (internet node), and attach new networks."
- "Based on interoperability and mutual agreement: The key to inter-networking is to define the context for interoperation—through open standards for the technologies, and mutual agreements between operators of autonomous pieces of the internet."
- **"**Collaboration: Overall, a spirit of collaboration is required—beyond the initial basis of interoperation and bilateral agreements, the best solutions to new issues that arise stem from willing collaboration between stakeholders. These are sometimes competitive business interests, and sometimes different stakeholders altogether (e.g., technology and policy)." (Internet Society 2012, emphasis in original)

The internet invariants point to a number of important features that should be reflected in any conception of internet ethics. First, the internet is not a "thing." It is, according to the Internet Society, "a global, interconnected network of networks" and "a global common resource and a highly interdependent system. Participation on the Internet means global interdependence" (Internet Society 2015, emphasis in original). Unlike computers and to a greater extent than Information Systems, the internet is characterized by this interconnectedness and interdependence. This means that the harm that is caused by deliberate or careless acts or omissions is magnified and is global in scope. The botnets that are used for DDoS attacks are only made possible because of this fundamental feature of the internet.

The history of the internet has been marked by collaboration and its preservation, and security require an ongoing commitment to robust, multi-stakeholder collaboration. The internet invariants point to the fact that no one is really "in charge" of the internet. The internet by its very nature is not national in character, and it resists efforts by a country to assert national sovereign jurisdiction over activities that occur online (Daigle 2013). For example, the internet's design includes large redundancies, a feature that flows from networks being added to existing networks. These redundancies build up the internet's resiliency. They also make it difficult, if not impossible, to put a "virtual fence" around a country, that is, to hive off a part of the internet and assert national sovereign jurisdiction over that part (Daigle 2015, p. 10).

Although no one is formally in charge of the internet, a baseline of order is maintained through collaboration and mutual agreement. A good example of this collaboration and mutual agreement in action is the work that has gone on to facilitate the adoption of IPv6 (Daigle 2015, p. 7; www.worldipv6launch.org n.d.). All stakeholders, including government, industry, and users, are in a flat, horizontal relationship with each other. When issues arise, stakeholders must work together in order to generate the most useful solutions to the problems. The default relationship among stakeholders is therefore one of cooperation and shared stewardship over the internet. As Daigle (2015) notes, "the spirit of collective stewardship of the network and collaboration to fix problems persists in today's heavily commercial, global Internet" (p. 7).

The Internet Society has warned that "any degradation of the Internet invariants could impact the economy, human rights, and even world security" (2016, p. 3). There is a strong consequentialist argument, therefore, that internet ethics should seek to maintain the internet

invariants in order to avoid the severe harm that could flow from a degradation of the current form of the internet.

The above discussion suggests that internet ethics should be informed by at least three principles: first, a view that the internet is a global common resource; second, that the internet is inherently interdependent in nature; and third, that managing the internet requires a multi-stakeholder collaboration and commitment to stewardship. The combination of these three principles with the deontological observation that consumer rights on the internet inherently require consumer obligations and responsibilities sets the stage for a shift in the paradigm of consumer protection on the internet. Internet ethics strongly suggests that consumers should be viewed as co-stewards of the internet rather than as passive and protected users.

Viewing consumers as co-stewards of the internet is also consistent with the emerging body of scholarship on consumer ethics and Consumer Social Responsibility (CnSR) (see Vitell 2015; Caruana and Chatzidakis 2014; Larsen and Lawson 2013). Vitell (2015) argues that from an ethical perspective, consumers have at least two responsibilities:

> …first toward other *stakeholders*, in their one-on-one dyadic relationships they have a responsibility to act ethically which usually involves the obtaining and perhaps use of goods and services, but could also involve *disposal*. We might call this responsibility, *consumer ethics*. Second toward *society* as a whole consumers have a responsibility to avoid societal harm and even to act proactively for social benefit which may involve all three facets of consumer behaviour—*obtaining, use and disposal*. We might call this responsibility, CnSR. (p. 768, emphasis in original)

From the perspective of consumer ethics and CnSR, when consumers use goods and services, especially when this use involves a common public good like the internet, consumers have responsibilities to act ethically. As I have already argued, the scope of these ethical responsibilities should be defined in light of internet ethics. Thus, recognizing and affirming consumer ethical and social responsibilities on the internet elevate the role of the consumer to a co-steward.

Legal Considerations

At present, there is no legal precedent for requiring consumers to adopt basic measures to protect their devices from malware infection. In some jurisdictions, ISPs have voluntarily committed to advising customers when they detect that a customer's devices have been infected. However, no jurisdiction requires consumers to take basic measures to protect themselves and others from the spread of malware and the risk of botnets and DDoS attacks. Moreover, in the private law realm, failing to maintain proper anti-malware protection and avoiding risky online behavior has not yet, to this author's knowledge, been found to be negligent or otherwise tortious. But law typically lags behind technology. In common law, liability in negligence is based in part on a failure to take a "reasonable" amount of care, and what is "reasonable" shifts over time. Thus, while public and private law have yet to recognize any legal obligation on the consumer to take basic measures to prevent infecting their devices with malware and becoming coopted into a botnet, this could change.

Nevertheless, it is unlikely that the parameters of private law would change in a way that would allow an individual consumer to be held liable for negligently failing to maintain proper protection against malware. The problem in private law is the potential scope of liability, which

is vast. Where DDoS attacks are concerned, it is essentially impossible to know in advance who might be the victim of an attack that makes use of one's devices. From a private law perspective, Anglo-common law is reluctant to impose liability when the possible victim of harm cannot be reasonably foreseen in advance. As the saying goes, there is no negligence in the air. There must be a relationship between the negligent actor and the victim that justifies imposing liability; the mere fact that someone has been careless and someone else was injured as a result is not enough.[15]

The vast and indeed unknowable scope of liability associated with negligently failing to protect against malware distinguishes this type of harmful act from other types of illicit behavior that do attract compensation. Illicit acts such as copyright violation, identity theft, and cyber stalking attract sanctions in many jurisdictions in private law, public law, or both. But these illicit acts are aimed at an identifiable target. The potential scope of liability is known and, in most cases, involves deliberate acts that infringe on the rights of the known, that is, identifiable, victim(s). There is a material difference, then, in illicit acts such as copyright violations, identity theft, and cyber stalking and carelessly failing to protect against malware, at least insofar as a private law cause of action is concerned.

From a public law perspective, there is increasing justification for placing basic regulatory obligations on consumers to ensure that their devices are properly protected against malware and botnets. As discussed above, regulatory approaches to cyber security and scholarship on this issue increasingly have adopted a multi-stakeholder approach in which consumers are treated as one of the parties that must collaborate in efforts to keep the internet secure. Thus, a stewardship model of consumer protection has already obtained a toehold in regulatory developments in the information-communications sector.

There are at least two important arguments that may pose obstacles to the further development of the stewardship model in public law, however. First, imposing regulatory obligations on consumers in the context of their internet-related activities may infringe on the right to freedom of expression. Second, it is not clear how effective anti-malware programs really are, which undermines any regulatory efforts to require consumers to use such programs. I will address each objection in turn.

In order to frame this discussion, it is helpful to outline what regulatory obligations might entail. For the purposes of this paper, I suggest that treating consumers as co-stewards of the internet reasonably requires the following: education about online threats, including botnets and DDoS attacks; avoidance of risky behavior such as clicking on suspicious links; maintaining strong passwords; and taking proactive measures such as installing and maintaining anti-malware protection on all devices and not accessing the internet on unprotected devices. Collectively, I will refer to these requirements as anti-botnet protection/obligations/requirements.

Infringement on the Freedom of Expression

Any regulations that require consumers to maintain adequate anti-botnet protection as a condition of accessing the internet run the risk of running afoul of the freedom of

[15] For two of the seminal Anglo-common law cases on the duty of care, which is the relational element of the negligence analysis, see: *Donoghue (or McAlister) v. Stevenson,* [1932] All ER Rep 1; [1932] A.C. 562 (H.L.) and *Palsgraf v. Long Island Railway Co.* (1928), 248 N.Y. 339, 162 NE 99 (NYCA). In *Palsgraf*, Cardozo JA wrote the following about the necessity of the foreseeability of harm to the victim: "if the harm was not willful, he [the victim-plaintiff] must show that the act as to him had possibilities of danger so many and apparent as to entitle him to be protected against the doing of it though the harm was unintended" ((1928), 248 N.Y. 339, p. 345).

expression. The centrality of the internet to modern life and the degree to which people now live their lives online mean that any constraints on access to the internet inherently restricts the freedom of expression. Nevertheless, that regulatory requirements related to anti-botnet protection would constrain the freedom of expression should not be fatal to the requirements. First, as I have discussed above, all rights involve correlated duties. Thus, one's right to exercise the freedom of expression by using the internet implies a corresponding duty to avoid interfering with other people's rights to do the same. Exercising due care to protect against malware (and thus against being drawn into a botnet) is arguably part of this duty.

The freedom of expression has never been an unfettered right. Long before the internet, private law sanctioned libelous and deceitful communication, and it continues to do so in respect of online speech. Legal restrictions related to defamation, deceit, harmful forms of speech, privacy rights, and copyright, for example, already constrain freedom of expression online. In *Lindqvist, Criminal Proceedings Against Bodil* (C-101-01) EU: C: 2003:596, for example, privacy rights protected in European Data Protection Directive 95/46 came into conflict with Mrs. Lindqvist's right to freedom of expression. Mrs. Lindqvist posted personal information of 18 colleagues on her personal website; she was subsequently charged under Swedish data protection law enacted pursuant to the Data Protection Directive 95/46. The European Court of Justice recognized that the case raised a legitimate interest in Mrs. Lindqvist's freedom of expression; however, it also recognized that Mrs. Lindqvist's freedom of expression had to be balanced with the protection of the privacy rights of the individuals whose personal details were published by Mrs. Lindqvist. The Court ultimately held that the Swiss data protection legislation (and hence the charges brought against Mrs. Lindqvist) appropriately balanced the competing rights at stake and did not constitute a disproportionate violation of the principle of the freedom of expression (*Lindqvist*, 82–87).

The European Court of Justice's decision in *Lindqvist* illustrates a second important consideration in the legal assessment of anti-botnet restrictions: when dealing with competing rights, the proportionality of an infringing measure is central to striking an appropriate balance. The relative importance of the rights that are at stake and the consequences associated with protecting or not protecting the rights must be weighed. Anti-botnet requirements would likely interfere with the exercise of the freedom of expression in a relatively minor way. Consumers would not be prevented from accessing the internet and thus they would not be subject to an outright prohibition on an important means of exercising their freedom of expression. Instead, exercising the freedom of expression on the internet would be subject to meeting some basic regulatory requirements related to preventing the spread of botnets. This is no different than, say, requiring a permit to hold a parade or a public concert. The public interest at stake is large and the regulatory obligation is tolerable, assuming that the requirements are not unduly onerous. In other words, so long as the regulatory requirements are reasonable and proportionate, it is likely that they would be a justifiable limitation on the freedom of expression, given the interests at stake.

The Effectiveness of Anti-Botnet Protection

The introduction of anti-botnet requirements would likely be met with concerns about the effectiveness of such measures in preventing the spread of malware and botnets.

While avoiding clicking on suspicious links and not opening suspicious email attachments are good practices, malware spreads through a variety of complex mechanisms, some of which are hard to prevent at the individual consumer level. Furthermore, although *Infosecurity Magazine* ("Survey Proves Effectiveness of Anti-virus" 2014) found one survey indicating the effectiveness of antivirus programs, other studies show that antivirus software (which includes programming aimed against malware) is nowhere near 100% effective at preventing infection. Indeed, one study suggested that antivirus software is only effective about 25% of the time, with a median detection rate of less than 20% (Krebs 2012; see also Horowitz 2012). However, care must be taken when considering such studies since the studies include a wide range of antivirus products, with varying levels of quality. Nevertheless, as Vigna (2014) and Wang (2014) note, because of the speed with which malware evolves and its complexity, even the best antivirus software typically will not catch all new forms of a virus immediately, leaving the user exposed to infection for a period of time.

If anti-botnet requirements are limited in their effectiveness, governments may be reluctant to impose them due to the regulatory and political costs involved. Moreover, the limited effectiveness of such measures may change the assessment of whether they are a reasonable limitation of the freedom of expression. Yet, the fact that the aforementioned basic precautions are not a guarantee of protection against malware does not mean that they should not be taken (Magnotti 2015; Rubenking 2015; "Survey proves effectiveness of anti-virus" 2014). Many experts in cyber security emphasize that it is not possible to offer complete ex ante protection against malware infection.

Instead, we must focus on developing a cyber security ecosystem, involving multiple stakeholders, each of whom has a role to play in the battle against malware, botnets, and DDoS attacks. Some stakeholders, including consumers, have responsibilities relating to reducing the risk of primary infection. The Online Trust Alliance (2013), a non-profit organization focusing on promoting online trust and the vitality of the internet, for example, has recognized that combatting botnets requires a multi-stakeholder approach that includes users of internet-accessible devices; users "need to take steps to protect their device and to stay safe online" (p.5), including maintaining up-to-date antivirus protection (see also Online Trust Alliance n.d.). Other stakeholders, for example, internet service providers, are well placed to detect and to initiate a response to malware infection, botnets, and DDoS attacks. Still others, for instance, Cyber Incident Response Teams (CIRTs), may have specialized roles to play once a DDoS attack is launched. In this ecosystem, the whole is greater than the sum of its parts. Thus, while one stakeholder's responsibilities may not be enough to prevent the spread of malware entirely, there is still good reason to require the stakeholder to meet those responsibilities insofar as it reduces the risk of infection without ultimately compromising the utility of remaining a part of the ecosystem.

Further support for imposing anti-botnet requirements notwithstanding the questions surrounding their ultimate effectiveness can be found by considering public health requirements for mandatory vaccinations. There are parallels between requiring vaccinations and requiring anti-botnet protection on devices. In both cases, the requirement is aimed not just at protecting the individual, but also protecting wider society from serious diseases/malware through "herd immunity." Both cases also involve impairments of an individual's personal autonomy and choice. Vaccinations involve a greater impairment of a person's autonomy, however, as they involve a person's bodily integrity as opposed to choice and control over one's devices. If an ethical and legal case can be made for requiring vaccinations to stem the spread of diseases and

biological viruses, then it is likely that a parallel case can be made for requiring anti-malware protection to stem the spread of digital viruses.

El Amin et al. (2012) consider a number of ethical arguments in the context of public health requirements to be vaccinated against certain diseases such as small pox, measles, mumps, rubella, whooping cough, and the human papilloma virus. The authors are able to conclude with relative ease that the default position should be that of requiring vaccinations. They apply a framework developed by Childress et al. (2002) that focuses on the ethical principles (or moral considerations) that are relevant to public health. Drawing on Childress et al. (2002), El Amin et al. (2012) note that there is some consensus about the nine most relevant ethical principles related to public health:

> 1) producing benefits; 2)avoiding, preventing, and removing harms; 3)producing the maximal balance of benefits over harms and other costs (i.e., utility); 4) distributing benefits and burdens fairly (distributive justice), and ensuring public participation, including the participation of affected parties (procedural justice); 5)respecting autonomous choices and actions, including liberty of action; 6) protecting privacy and confidentiality; 7)keeping promises and commitments; 8)disclosing information as well as speaking honestly and truthfully (i.e., transparency); and 9)building and maintaining trust (p. 3).

Recognizing that it is likely that these considerations will come into conflict with each other at times, Childress et al. (2002) proposed five "justificatory conditions" that provide guidance about when the considerations that weigh in favor of action to protect public health (e.g., mandatory vaccinations) can trump other public health goals (e.g, justice, respect for autonomy, and privacy) (see also El Amin et al. 2012, p. 3). These five "justificatory conditions," as summarized by El Amin et al. (2012), are:

> Effectiveness of the activity, proportionality of the activity (the probably health benefits outweigh the "infringed" other moral considerations), necessity of the activity, the extent to which the activity represents the least infringement of the other moral considerations, and lastly, the ability to publicly justify the activity in a transparent manner. (p. 3)

El Amin et al. (2012) conclude that "because vaccination activities are a key component of many public health programs" (p. 3), they fall within this ethical framework and are therefore justified.

A similar conclusion arises when we adapt the Childress et al. (2002) framework for ethical considerations in public health (as discussed by El Amin et al. 2012) for protecting the internet from botnet-enabling malware. This is true despite the fact that while the evidence concerning the effectiveness of vaccines at preventing the spread of disease is robust, the same is not true for anti-botnet protection. The Childress et al. (2002) framework for ethical considerations in the area of public health recognizes that trade-offs are necessary. While many vaccines are highly effective, they are not completely without physical risk or cost. Nevertheless, by applying the Childress et al. justificatory conditions, El Amin et al. conclude that mandatory vaccines are often worth the risk they pose to individuals in light of the important role they play in public health. Similarly, on balance, the measures prescribed for consumers as co-stewards of the internet are justified notwithstanding their relatively low level of efficacy. While antivirus software and other protections may not be very effective, they do not represent a tremendous infringement on the personal autonomy and freedom of consumers. Unlike vaccines, which compromise a person's bodily integrity, antivirus software is used on a thing quite detached from the consumer. Moreover, the cost of antivirus protection is not prohibitive,

and many institutions (e.g., academic institutions and banks) offer software for free. Another important consideration is the fact that the individual consumer also receives the benefit from taking precautionary measures in the form of reduced exposure to the risk of malware infection. On the whole, then, after balancing a number of important ethical considerations, it is evident that requiring consumers to take the aforementioned basic precautionary measures is ethically justified.

Applying the "precautionary principle," as articulated by Gostin et al. (2003) with respect to public health, offers additional support for this position. In the context of responding to a severe, potentially infectious disease threat, the precautionary principle imposes an obligation to "…protect populations against reasonably foreseeable threats, even under conditions of uncertainty….Given the potential costs of inaction, it is the failure to implement preventive measures that requires justification…" (Gostin et al. 2003, p. 3232). Although Gostin et al. (2003), wrote in the context of public health, the threat of a potentially severe infectious "disease" (or virus) also exists in cyberspace. Just as a serious communicable illness puts the public at risk and requires a response from public health authorities, so the spread of malware viruses online requires a response from internet stakeholders given that the spread of malware constitutes a serious, reasonably foreseeable risk to the internet and all critical infrastructures that is connected to it. Thus, while there may be uncertainty about how much harm will be prevented by requiring consumers to take measures such as installing antivirus software on all devices, the application of the precautionary principle suggests that such measures should be the default position. In light of the threat posed by malware, botnets, and DDoS attacks, it is the failure to require consumers to take basic protective measures that needs justification.

Conclusion

The development of the commercial internet has been one of the most (if not the most) disruptive technological accomplishments in the history of humankind. The internet has changed how we socialize, shop, learn, bank, and engage civically in society. It is not surprising that the internet should trigger a need to re-think how consumers are protected in an online world.

Existing approaches to consumer protection are ill-suited to address the nature of threats online. Accordingly, it is necessary to transition from a traditionally vertical and hierarchical structure for consumer protection to one that is more horizontal in nature. The consumer must be viewed as a co-steward of the internet, with responsibilities in the cyber security ecosystem.

I have presented an ethical and a legal justification for a stewardship model for consumer protection on the internet. However, cultivating a consumer protection culture that views the consumer as a co-steward of the internet will be challenging. A full discussion of the practical dimensions of moving to a stewardship model is beyond the scope of this article. Further scholarship is necessary to consider the respective roles of consumer education, institutional reform, and the scale and scope of the implementation of anti-botnet protection measures.

References

61.5% of Web Traffic Comes from Bots. (2013). *Info-security magazine*. Retrieved from http://www.infosecurity-magazine.com/news/615-web-traffic-comes-from-bots/.

Abel, R. (2015). Two Idaho students face charges after DDoS attacks against school district. *SC Magazine* (online edition). Retrieved from http://www.scmagazine.com/two-students-paid-for-ddos-attacks-may-face-felony-charges/article/415319/.

Arbor Networks. (2014). *2014 ATLAS Threat Report.* Retrieved from http://www.arbornetworks.com/resources.

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good. *Journal of Legal. Ethical and Regulatory Issues, 16*(1), 7–14.

Brandom, R. (2015). Last night, GitHub was hit with massive denial-of-services attack from China. Retrieved from http://www.theverge.com/2015/3/27/8299555/github-china-ddos-censorship-great-firewall.

Caruana, R., & Chatzidakis, A. (2014). Consumer social responsiblility (CnSR): toward a multi-level, multi-agent conceptualization of the "Other CSR". *Journal of Business Ethics, 121*, 577–592. https://doi.org/10.1007/s10551-0131739-6.

Chase, S. (2015). Cyberattack deals crippling blow to Canadian government websites. *The Globe and Mail* (online edition). Retrieved from http://www.theglobeandmail.com/news/national/canadian-government-websites-appear-to-have-been-attacked/article24997399/.

Childress, J. F., Faden, R. R., Garre, R. D., Gostin, L. O., Kahn, J., Bonnie, R. J., et al. (2002). Public health ethics: mapping the terrain. *Journal of Law, Medicine & Ethics, 30*(2), 170–178.

Consumer Affairs New Zealand. (n.d.). For consumers: internet shopping. Retrieved from http://www.consumeraffairs.govt.nz/for-consumers/shopping/where-you-buy/internet-shopping. (accessed 10 June, 2015).

Daigle, L. (2013). Provoking national boundaries on the internet? A chilling thought…[blog post]. Internet Society. Retrieved from http://www.internetsociety.org/blog2013/06/provoking-national-boundaries-internet-chilling-thought.

Daigle, L. (2015). On the nature of the internet. *Global commission on internet governance, paper series*, No. 7. Retrieved from https://www.cigionline.org/publications/nature-of-internet.

DDoS attacks. (n.d.). Retrieved June 24, 2015 from https://www.incapsula.com/ddos/ddos-attacks/.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). OJ 1995 L 281. (The Data Protection Directive). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

El Amin, A. N., Parra, M. T., Kim-Farley, R., & Fielding, J. A. (2012). Ethical issues concerning vaccine requirements. *Public Health Reviews, 34*(1), 1–20.

European Network and Information Security Agency. (2012). National cyber security strategies: setting the course for national efforts to strengthen security in cyber space [Report]. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.

Federal Trade Commission (USA). (n.d.). Hacked Email: what to do (video). Retrieved from https://www.ftc.gov/news-events/audio-video/video/hacked-email-what-do.

G.A. Res. 32/L.20, *The promotion, protection and enjoyment of human rights on the Internet.,* U.N. Doc. A/HRC/32/L.20 (2016).

Goncharov, M. (2012). *Russian underground 101.* Trend micro incorporated research paper. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

Google Spain SL, *Google Inc. v Agencia Española de Protección de Datos & Mario Costeja González*. Case C-131/12. Court of Justice of the European Union, 2014. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

Gostin, L. O., Bayer, R., & Fairchild, A. L. (2003). Ethical and legal challenges posed by severe acute respiratory syndrome: implications for the control of severe infectious disease threats. *JAMA, 290*, 3229–3237.

Horowitz, M. (2012). Defensive computing. *Computerworld.com*. Retrieved from http://www.computerworld.com/article/2472120/security0/how-useful-is-antivirus-software-.html.

Industry Canada, Office of Consumer Affairs (n.d.) Canadian consumer handbook: Consumer protection: Online shopping. Retrieved from: http://www.consumerhandbook.ca/en/topics/consumer-protection/online-shopping.

Ingersoll, G. & M. B. Kelley. (2013). There's only one thing stopping enemy nations from smashing America's power grid. *Business Insider* (US edition, online). Retrieved from http://www.businessinsider.com/nations-had-electric-wmd-for-years-2013-2.

Internet Society. (2012). Internet invariants: what really matters. Retrieved from http://www.internetsociety.org/interent-invariants-what-really-matters.

Internet Society (2015). *Collaborative security: an approach to tackling internet security issues.* Retrieved from Internet Society website: https://www.internetsociety.org/sites/default/files/Collaborative-Security.pdf.

Internet Society (2016). *Internet invariants, what really matters: an internet society public policy briefing*. Retrieved from Internet Society website: https://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-InternetInvariants-20160926-nb.pdf.

Japan, Information Security Policy Council. (2013). Cybersecurity strategy: Towards a world-leading, resilient, and vigorous cyberspace, Provisional Translation. Retrieved from http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf.

Kenya, Ministry of Information Communications Technology. (2014). Feel safe online: national cybersecurity strategy 2014. Nairobi, Kenya.

Krebs, M. (2012). A closer look: Email-based malware attacks. *Krebsonsecurity.com*. Retrieved from http://krebsonsecurity.com/2012/06/a-closer-look-recent-email-based-malware-attacks/.

Larsen, G., & Lawson, R. (2013). Consumer rights: An assessment of justice. *Journal of Business Ethics, 112*, 515–528. https://doi.org/10.1007/s10551-012-1275-9.

LeBlanc, D. (2012). Well over 10000 computers used in attack on NDP leadership vote. *The Globe and Mail* (online edition). Retrieved from http://www.theglobeandmail.com/news/politics/ottawa-notebook/well-over-10000-computers-used-in-attack-on-ndp-leadership-vote/article610503/.

Levin, A., Goodrick, P., & Ilkina, D. (n.d.). *Securing cyberspace: a comparative review of strategies worldwide*. Toronto: Ted Rogers School of Management, Ryerson University, Privacy and Cyber Crime Institute **Retrieved from http://www.ryerson.ca/content/dam/tedrogersschool/privacy/AODAforms/Ryerson_cyber_crime_final_report%20AODA.pdf.**

Magnotti, L. (2015). Is antivirus software still relevant? GCN. Retrieved from http://gcn.com/articles/2015/01/08/antivirus-software-still-relevant.aspx.

Mason, R. (1986). Four ethical issues of the information age. *MIS Quarterly*, March, 5–12.

Matthews, T. (2014) *Incapsula Survey: what DDoS attacks really cost businesses*. (Incapsula/Impervia, 2014). Retrieved from: https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266–275.

Moor, J. H. (1999). Just consequentialism and computing. *Ethics and Information Technology, 1*, 65–69.

Neustar. (2015). *Neustar DDOS attacks & protection report: North America*. Retrieved from https://www.neustar.biz/resources/whitepapers/ddos-attacks-protection-report-us-2015.

OECD. (2008). *Computer viruses and other malicious software: A threat to the internet economy*. Paris: OECD. https://doi.org/10.1787/9789264056510-en.

OECD. (2012). Proactive policy measures by internet service providers against Botnets. *OECD Digital Economy Papers*, No. 19. https://doi.org/10.1787/5k98tq42t18w-en.

Online Trust Alliance. (2013). Botnet remediation overview and practices. Retrieved from https://otalliance.org/system/files/files/best-practices/documents/ota_2013_botnet_remediation_best_practices.pdf.

Online Trust Alliance. (n.d.). Botnets. Retrieved from https://otalliance.org/resources/botnets.

Onyancha, O. M. (2015). An informetrics view of the relationship between internet ethics, computer ethics, and cyberethics. *Library Hi Tech, 33*(3), 387–408. https://doi.org/10.1108/LHT-04-2015-0033.

Panetta, L. (2011). Testimony to U.S. Senate, Committee on Armed Services, confirmation hearing for Secretary of Defence.

Ponemon Institute LLC & Radware. (2012) *Cyber security on the offence: a study of IT security experts*. Retrieved from: https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf.

Rubenking, N. (2015). The best antivirus for 2015. *PCMag* online edition. Retrieved from http://www.pcmag.com/article2/0,2817,2372364,00.asp.

Rustad, M. & D'Angelo, D. (2011). The path of internet law: an annotated guide to legal landmarks. Duke Law & Technology Review, 012. Retrieved from http://dltr.law.duke.edu/articles/.

Seals, T. (2015). DDoS attacks more than double in 12 months. *Infosecurity*. Retrieved from http://www.infosecurity-magazine.com/news/ddos-attacks-more-than-double-in/.

Singapore, Infocomm Development Authority of Singapore. (2013). National Cyber Security Masterplan 2018 (Brochure). Retrieved from https://www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-Security-Masterplan-2018.

Spinello, R. A., & Tavini, H. (Eds.). (2004). *Readings in cyberethics*. Sudbury: Jones and Bartlett.

Survey proves effectiveness of anti-virus. (2014). *Infosecurity Magazine,* online edition. Retrieved from http://www.infosecurity-magazine.com/news/survey-proves-effectiveness-of-anti-virus/.

Szary, W. & E. Auchard. (2015). Polish Airline, hit by cyber attack, says all carriers are at risk. *Reuters* (US ed.). Retrieved from http://www.reuters.com/article/2015/06/22/us-poland-lot-cybercrime-idUSKBN0P21DC20150622.

The Netherlands, National Coordinator for Security and Counterterrorism. (2013). National Cyber Security 2: from awareness to capability. Den Haag, the Netherlands.

Thielman S. & Johnson, C. (2016) Major cyber attack disrupts internet service across Europe and US. *The Guardian* (online edition). Retrieved from: https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

TRAI website down, Anonymous India claims responsibility. (2015). *The Times of India* (online edition). Retrieved from http://timesofindia.indiatimes.com/tech/tech-news/Trai-website-down-Anonymous-India-claims-responsibility/articleshow/47069767.cms.

U.K. (2011). The UK cyber security strategy: protecting and promoting the UK in a digital world. London, U.K. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Understanding DDOS. (n.d.). Retrieved May 5, 2015 from www.digitalattackmap.com/understanding-ddos.

Vigna, G. (2014). Antivirus isn't dead; It just can't keep up [blog post]. Lastline labs. Retrieved from http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up.

Vitell, J. C. (2015). A case for *Consumer* social responsibility (CnSR): including a select of consumer ethics/social responsibility research. *Journal of Business Ethics, 130*, 767–774. https://doi.org/10.1007/s10551-014-2110-2.

Wamala, F. (2011). *ITU National Cyber Security Strategy Guide*. Geneva: International Telecommunication Union **Retrieved from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.**

Wang, A. (2014). Is antivirus software ineffective? *PCMag.com*. Retrieved from http://securitywatch.pcmag.com/security/323973-is-antivirus-software-ineffective.

Warwick A. (2014). DDoS attacks hit Sony's PlayStation network and other gaming services. Retrieved from http://www.computerweekly.com/news/2240227479/DDoS-attacks-hit-Sonys-PlayStation-Network-and-other-gaming-services.

Woolf, N. (2016). DDoS attack that disrupted the internet was the largest of its kind in history, experts say. *The Guardian* (online edition). Retrieved from: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

www.worldipv6launch.org. (n.d.). World IPv6 Launch. Retrieved from http://www.worldipv6launch.org.