By Policy or Design? Privacy in the US in a Post-Snowden World

Halbert, Debora; Larsson, Stefan

Published in:
Journal of Law, Technology and Public Policy

2015

By Policy or Design? Privacy in the US in a Post-Snowden World

Debora Halbert♦ & Stefan Larsson♣

Abstract

By drawing from a number of studies in the field as well as the Snowden revelations and the case of *MegaUpload/MEGA*, the article makes an analysis of relevant legislation on privacy in the digital context. The purpose of the analysis is to understand to what extent and how the current paradigm of privacy protection is, or is not, sufficient for contemporary needs. In particular, we ask how privacy is protected by policy in an American context and to what extent this is or is not insufficient in relation to an approach of "privacy by design". In short, we conclude that privacy by policy is necessary but not sufficient and that efforts should be made to further implement policy by design.

1. Introduction

In his recent book, *The Circle*, David Eggars writes about a fictional social media company that, through its ubiquitous presence and constant technological innovation, was changing the way its employees and people throughout the world perceived their on-line lives.[1] Through friendly interventions and constant digital interactions, the characters in *The Circle* come to realize the benefits of a fully transparent and digitally downloaded life. The goal for the circle, as envisioned by its corporate leaders, was full transparency because only then do we come to a point of true authenticity and public honesty.

The circle, as envisioned by Eggars, and perhaps being pursued by not-so-fictional social media companies, could also be understood as a form of friendly fascism, a term coined by Bertram Gross in the 1980s.[2] Gross argued that fascism would not come to the United States in the form of militarism and violence but rather, it would come in the form of government and corporate convergence. Such a convergence would create the legal structures necessary for

♦ Debora Halbert is a Professor of Political Science at the University of Hawaii at Manoa.
♣ Stefan Larsson is a Head of Lund University Internet Institute, and PhD in Sociology of Law as well as in Spatial Planning.
[1] DAVE EGGERS, THE CIRCLE (2013).
[2] BERTRAM GROSS, FRIENDLY FASCISM: THE NEW FACE OF POWER IN AMERICA (First Printing edition ed. 1999).

American capitalism to expand globally and to ensure that this economic system remained unthreatened. Thus, American fascism would be a type of corporatism without the charisma and violence associated with older fascists politics.

Such friendly fascism would (or could) embody constant surveillance, but if such surveillance is aligned with corporate goals and done with a smile, then the illusion of freedom can be maintained.

In other words, in the social media environment, we participate in our own surveillance by actively posting personal information, pictures, comments, and ideas. Furthermore, constant data is collected about our habits through the digital accumulation of information that is now associated with everything from library cards to grocery store coupon saving cards. This corporatist structure of constant surveillance is achieved not through oppressive force but through friendly and well-meaning efforts to make the world a better and more efficient place. We are heading towards the world of *The Circle* without putting up much of a fight.

In the post-9/11 world, America has justified the use of enhanced security and mass surveillance measures as essential to protecting the United States from all types of threats, real and digital.[3] According to this view, we must give government and industry the ability to fight those that would seek to attack our economic or political structures and if you have "nothing to hide," then such surveillance should be acceptable.[4] However, others might argue that the US, having now built back doors into key security software, has made the world less safe, or at the very least, many claim that enabling mass surveillance is not as helpful as the government claims it to be.[5] As Edward Snowden suggests regarding the trust we have in economic systems, "if we lose the trust of something like SSL, which was specifically targeted by the Bullrun program, we will live a less safe world overall. We won't be able to access our banks and we won't be able to

[3] Sejal H. Patel, *Sorry, That's Classified: Post-9/11 Surveillance Powers, The Sixth Amendment, And Niebuhrian Ethics*, 23 BOSTON UNIV. PUBLIC INTEREST LAW J. 287–311 (2014). (arguing that the Patriot Act and the revisions to the Foreign Intelligence Security Act make it far more possible for broader and enhanced state surveillance powers).
[4] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011). (arguing that there is an intrinsic flaw in the claim that having nothing to hide means citizens should embrace state surveillance).
[5] Tammy Bruce, *Terror Undeterred by Mass Surveillance*, THE WASHINGTON TIMES (2105), http://www.washingtontimes.com/news/2015/jan/19/tammy-bruce-terror-undeterred-mass-surveillance/ (last accessed May 29 2015); Janene Van Jaarsveldt, *Mass surveillance totally ineffective: Edward Snowden*, NL TIMES (2015), http://www.nltimes.nl/2015/01/22/mass-surveillance-totally-ineffective-edward-snowden/ (last accessed 29 May 2015).

access commerce without worrying about people monitoring those communications or subverting them for their own ends."[6]

In line with the tension produced between surveillance and privacy, the purpose of the article is to understand to what extent and how the current paradigm of privacy protection is or is not sufficient for contemporary needs in a post-Snowden and highly digitized world. We particularly ask for how privacy is protected by policy in an American context and to what extent this might be insufficient in relation to an approach that would instead protect "privacy by design". As will be detailed in the next section, the U.S. policy approach to privacy both endorses better privacy protection of Americans as individuals but requires mass surveillance and data collection on those individuals for national security reasons simultaneously. Americans themselves, hold inconsistent views on privacy, both fearing privacy loss, but doing nothing about it. The argument in the article draws from a number of studies in the field as well as the Snowden revelations and the case of MegaUpload, and makes an analysis of relevant legislation against this backdrop.

While there are distinct features that differ between governmental surveillance, the "Big Data" retention of online services, and ISPs for the sake of individualized marketing or service development, the focus of this article is on the similarities between them, not the differences. The purpose, as mentioned, is to understand more of the insufficiencies related to privacy as protected by policy, and how all of these approaches of retention of individualized data – be it for the sake of countering terrorism, selling shoes or assessing relevancy in a social media flow – speak of the challenges of policy as a well-entrusted mode for protection of privacy in a digital context.

Part Two introduces the American policy approach to privacy. Part Three introduces the concept of privacy by policy and attitudes towards privacy held by Americans. Part Four uses the case of *MegaUpload* and its re-visioning as a privacy/security company called MEGA in order to highlight how privacy by design might look in the context of contemporary privacy debates. Part Five offers a conclusion regarding US policy for digital privacy and highlights some of the most pressing insufficiencies we see with policy as the sole mode of protecting privacy in a digital

[6] Edward Snowden, HERE'S HOW WE TAKE BACK THE INTERNET, http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet (last accessed 29 May 2015) (SSL refers to secure sockets layer which allows for private communications on the Internet. Bullrun is the NSA decryption program).

context. These insufficiencies have policy implications for how we ought to protect privacy in the future. Given the global reach and focus of the Internet, the global context within which file-sharing occurs, the ways social media structures public and private relations, and much more, the implications of this work is arguably important not just within the U.S. context, but for the larger debate on the evolution of the Internet.

2. Americans and Privacy

Edward Snowden's revelations about massive government surveillance have heightened citizens' fears about U.S. surveillance, leading to a new round of debate over issues of privacy and security in a democratic society.[7] In the aftermath of the Snowden revelations, the 2013 Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, which recommends changes to its data collection and surveillance programs, best summarizes the challenge of private disclosure of information to third parties and the government's role in accessing that data. The report states:

> In modern society, individuals, for practical reasons, have to use banks, credit cards, e-mail, telephones, the Internet, medical services, and the like. Their decision to reveal otherwise private information to such third parties does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life. What they want – and reasonably expect – is both the ability to use such services and the right to maintain their privacy when they do so. As a matter of sound public policy in a free society, there is no reason why that should not be possible.[8]

As the report notes, the lack of explicitly-stated concerns about privacy and disclosure of personal information should not be understood as a justification for government surveillance of that data.

[7] Byron Acohido, *Snowden effect: young people now care about privacy*, USA TODAY (2013), http://www.usatoday.com/story/cybertruth/2013/11/13/snowden-effect-young-people-now-care-about-privacy/3517919/ (last accessed 29 May 2015).

[8] RICHARD A CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 111–112 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (last accessed 29 May 2015).

This can be compared to a recently approved Parliamentary Report of the Council of Europe (Committee on Legal Affairs and Human Rights, rapporteur Pieter Omtzigt) that comments on the US use of mass surveillance as a tool for preventing terrorist attacks as revealed by Edward Snowden. The report indicates that mass surveillance is a threat to privacy as it is regulated in the European Convention on Human Rights and addresses how adequate judicial control is failing:

> The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 European Convention on Human Rights (ECHR)), freedom of information and expression (Article 10, ECHR), and the rights to a fair trial (Article 6, ECHR) and freedom of religion (Article 9) – especially when privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated). These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law.[9]

The US policy approach to digital privacy is schizophrenic. On the one hand, it continues to seek out methods of enhancing surveillance capabilities of the US government. For example, the 2011 *Protecting Children From Internet Pornographers Act* would have required ISPs to keep IP-address logs for a minimum of a year. This bill was sharply criticized for the possible implications it held for Internet privacy and did not pass out of the House of Representatives.[10]

The 1986 Electronic Communications Privacy Act (ECPA) is the center of efforts to include data retention clauses like those included in the child pornography legislation.[11] So far not only have revisions been resisted, but in 2010 the 6th circuit found that warrantless searches of email (at the time legal under ECPA) were an unconstitutional violation of the 4th amendment. As a result, all major Internet companies now require a search warrant prior to letting the state

[9] Committee on Legal Affairs and Human Rights, rapporteur Pieter Omtzigt, MASS SURVEILLANCE (Parliamentary assembly of the Council of Europe, 2015) at A4.
[10] Conor Friedersdorf, *The Legislation that could Kill Internet Privacy for Good*, THE ATLANTIC (2011), http://www.theatlantic.com/politics/archive/2011/08/the-legislation-that-could-kill-internet-privacy-for-good/242853/ (last accessed 29 May 2015).
[11] Christopher Reynolds, *The Data Retention Disaster Heading to the US American Thinker* (2013), AMERICAN THINKER, http://www.americanthinker.com//2013/06/the_data_retention_disaster_heading_to_the_us.html (last accessed 29 May 2015).

access private emails.[12] The 1996 Electronic Communication Transactional Records Act requires that records be held for up to 90 days if requested by government.[13] The Obama Administration along with Republicans has said that the lack of data retention makes crime fighting harder because companies are not required to store records.[14] States also look towards data retention. In 2012, Hawaii introduced a mandatory data retention law for up to 2 years. Fortunately, this did not pass the legislature either.[15] Of course, the U.S. Patriot Act has long been a cornerstone of post 9/11 American surveillance systems.[16]

The schizophrenic approach to privacy policy becomes clear when one contrasts these data retention initiatives with efforts to further enhance individual privacy. Multiple legislative attempts have been made to create consumer protection that would make surveillance more difficult, not easier. Examples include the *Consumer Privacy Protection Act of 2011*, the *Do Not Track Me Online Act*, the *Geolocation Privacy and Surveillance Act*, the *Location Privacy Protection Act of 2011*, the *Electronic Communications Privacy Act Amendments Act of 2011* and the *Financial Information Privacy Act of 2011*.[17]

In the face of such massive and often contradictory federal legislation, Americans continue to engage in all forms of digital communication and economic transactions. While legislation intended to either protect citizens from surveillance (primarily economic) and/or enhance the ability of the state to engage in data collection at both the individual and the meta data level continues to be debated, American's privacy rights are currently protected by policy. In the next section we detail the policy strategy for privacy protection that exists in the United States and American attitudes towards their privacy.

[12] Declan McCullagh, *Appeals court: Feds need warrants for e-mail*, CNET (2010), http://www.cnet.com/news/appeals-court-feds-need-warrants-for-e-mail/ (last accessed 29 May 2015).
[13] Reynolds, *supra* note 11.
[14] Declan McCullagh, *Justice Department seeks mandatory data retention*, CNET (2011), http://www.cnet.com/news/justice-department-seeks-mandatory-data-retention/ (last accessed 29 May 2015).
[15] Reynolds, *supra* note 11.
[16] Patel, *supra* note 3; Elizabeth Atkins, *Spying On Americans: At What Point Does The NSA'S Collection And Searching Of Metadata Violate The Fourth Amendment?*, 10 WASH. J. LAW TECHNOL. ARTS 51–88 (2014). (arguing that the collection of metadata by the NSA violates the fourth amendment).
[17] ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE: A WHITE PAPER FOR REGULATORS, DECISION-MAKERS AND POLICY-MAKERS 31 4–5 (2011), http://www.privacybydesign.ca (last accessed 29 May 2015).

3. The Current State of Privacy Protection and the Failure of Privacy by Policy

As a defense against the ubiquitous surveillance of a technologically mediated world, there is the privacy policy and the legal structure designed to protect user privacy. The privacy by policy approach of "notice and choice," where the user is given notification of the privacy contract and then can choose to utilize the services or not, stands as the predominant privacy structure in the United States today.[18] When California passed its Online Privacy Protection Act of 2003, virtually all companies doing business via the Internet had to develop and deploy a privacy policy.[19] More generally, privacy policies are provided by banks, credit cards, doctors, schools, Internet companies and more – many are printed on paper and mailed directly to the individual. Most of these privacy statements are most likely immediately thrown in the trash. Studies have shown that most users are interested in how a company uses their data but that they do not read the privacy policies in part because they are written in legal language that is too complex.[20]

Furthermore, according to privacy scholar Helen Nissenbaum, to achieve clarity, a "privacy paradox" is created, meaning that to make the policy clear enough to be understood means it will be unacceptable to users, where "transparency of textual meaning and transparency of practice conflict in all but rare instances."[21] In other words, if people knew what they were agreeing to, they would most likely not agree. An informal analysis of the contents of 100 privacy policies from dominant Internet advertising agencies found that the vast majority of these policies were unclear, did not provide adequate opt out options, and did not prevent information sharing amongst third parties.[22] As constitutional legal scholar Wolfgang Shultz notes, these informed consent documents that we must agree to before downloading a given application do not suggest consumers have in any way been informed, but rather simply that they

[18] Kirsten Martin, *Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online*, 18 FIRST MONDAY (2013), http://pear.accc.uic.edu/ojs/index.php/fm/article/view/4838 (last accessed 29 May 2015).
[19] Stefanie Olsen Staff Olsen, *California privacy law kicks in*, CNET NEWS (2004), http://news.cnet.com/California-privacy-law-kicks-in/2100-1028_3-5258824.html (last accessed 29 May 2015).
[20] A.I. Anton, J.B. Earp & J.D. Young, *How Internet users' privacy concerns have evolved since 2002*, 8 IEEE SECUR. PRIV. 21–27, 24 (2010).
[21] Helen Nissenbaum, *A contextual approach to privacy online*, 140 DAEDALUS 32–48, 36 (2011).
[22] LORRIE FAITH CRANOR ET AL., ARE THEY WORTH READING? AN IN-DEPTH ANALYSIS OF ONLINE ADVERTISING COMPANIES' PRIVACY POLICIES (2014), http://papers.ssrn.com/abstract=2418590. [Abstract only].

have become part of the legal paradigm offered by the company at issue.[23] Thus while notice and choice approaches are suspect, this "privacy by policy" continues to dominate.[24]

This network of privacy policy statements can be called privacy by policy – and assures the consumer or citizen that while the data exists and is collected, it is only used according to the rules written in the privacy statements. These privacy policies are typically contracts of adhesion – we cannot negotiate them or opt out, but rather as with end user licensing agreements, we must opt in or use a difference service. Privacy by policy means that we must trust those who control the data collected from us because there is a policy that says they will manage our personal information with trust. In other words, privacy by policy is premised upon a basic trust in those collecting and managing data. In the United States, for example, ISPs retain data for times ranging from six months to a year and the ways this data might be used are not clear. Data retention is of interest to the U.S. federal government as well because it wishes to have better access to this data for its own criminal and surveillance purposes. However, despite concerns about both legal and illegal uses of personal information, a privacy policy is assumed to be sufficient assurance that nothing inappropriate can happen with this data.

While privacy policies may keep companies from sharing personal data unless they specifically state their intentions to do so, it cannot be assumed that data remains with the company collecting it.[25] Additionally, even without sharing, individual companies have amassed astounding amounts of personal data about their users. Facebook, for example, can access everything placed on its servers, even if they don't share it with a third party, which of course is not guaranteed.[26] Google has even more data that can be matched with an individual from the content of their emails and daily planners to the searches they complete using the Google search engine. There is also concern that anonymous data can be individualized.[27] And it was recently claimed by a ranking U.S. military official that big data, seemingly anonymous and aggregate

[23] Wolfgang Schultz, *Introduction*, *in* CAHIER DE PROSPECTIVE: THE FUTURES OF PRIVACY 47–53, 50 (Carine Dartiguepeyrou ed., 2014).
[24] Nissenbaum, *supra* note 21, at 34; Martin, *supra* note 18.
[25] Cranor et al., *supra* note 22; Dennys Marcelo Antonialli, *Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes*, 8 STANFORD JOURNAL OF CIVIL RIGHTS AND CIVIL LIBERTIES 323–368 (2012).
[26] Taylor Casti, *Facebook Knows Everything About You, And If You Don't Believe Us Here's Proof,* THE HUFFINGTON POST (2014), http://www.huffingtonpost.com/2014/04/22/watch-dogs-facebook-privacy-settings_n_5191237.html (last accessed 29 May 2015).
[27] Armen Aghasaryan, *The Place of Privacy-Enabling Technologies in the Evolving Value Chain of Personal Data*, *in* CAHIER DE PROSPECTIVE: THE FUTURES OF PRIVACY 107–113, 108 (Carine Dartiguepeyrou ed., 2014).

has been used to kill people.[28] While surveys suggest that Americans do not want to be tracked online, even with privacy policies, most websites engage in some sort of tracking.[29]

The digital world has also created the confounding situation where people are voluntarily monitored (even if they do not see it this way) in exchange for the services offered by commercial websites. Social networking has fundamentally changed individual practices in regards to disclosure of information and the divide between the public and private. We have entered the world of sociable surveillance – meaning that at least Americans seem to have decided that living their lives visibly on social networking sites such as Facebook, Instagram or Twitter is acceptable and mostly harmless. Anders Albrechtslund calls this participatory surveillance.[30] This is a form of surveillance that can and does exist because of the willing participation of those under watch.

Facebook is one example, but isn't alone in setting the stage for voluntary monitoring (in exchange for access to the service). Everything done via the Internet leaves a digital trace – Google searches, quizzes taken, emails written; it all becomes part of the vast quantities of collectible data on the individual or in the aggregate. It allows for better tracking of consumer desires and product placements. Even for those who opt out of social networks, virtually all consumer choices are mediated by data collection. Credit card transactions are monitored, library records are archived and can be requested by the government, biometric data is increasingly relevant. Customer loyalty cards are virtually required in the United States and create a wealth of consumer data. As Nils Zurawski points out, consumers willingly exchange personal data for coupons and shopping discounts, creating a form of surveillance consumption.[31] It takes serious exertion to get and/or stay off the grid.[32] So much effort in fact, that as Jessica Goldstein has noted, it is not worth the effort.[33]

---

[28] Mike Masnick, *Michael Hayden Gleefully Admits: We Kill People Based On Metadata*, TECHDIRT. (2014), https://www.techdirt.com/articles/20140511/06390427191/michael-hayden-gleefully-admits-we-kill-people-based-metadata.shtml (last accessed 29 May 2015).
[29] Martin, *supra* note 18.
[30] Anders Albrechtslund, *Online Social Networking as Participatory Surveillance*, 13 FIRST MONDAY (2008), http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2142 (last accessed 29 May 2015).
[31] Nils Zurawski, *Consuming Surveillance: Mediating Control Practices through Consumer Culture and Everyday Life*, *in* MEDIA, SURVEILLANCE AND IDENTITY: SOCIAL PERSPECTIVES 32–48 (Andre Jansson & Miyase Christensen eds., 2013).
[32] Jessica Goldstein, *Meet the Woman Who Did Everything in Her Power to Hide Her Pregnancy from Big Data*, THINK PROGRESS (2014), http://thinkprogress.org/culture/2014/04/29/3432050/can-you-hide-from-big-data/ (last accessed 29 May 2015).
[33] *Id.*

To the degree Americans are concerned about issues of privacy, research suggests they are primarily focused on information transfer, notice/awareness, and information storage.[34] Longitudinal studies suggest there has been a heightened sense of awareness about privacy on the part of individuals.[35] Even Millennials, studies suggest, care about privacy and manage their privacy settings accordingly, in part because they are seeking to avoid the constant surveillance of their parents rather than the government or big business.[36] However, despite the existence of privacy concerns amongst young people, research completed by the Annenberg School's Digital Future Project suggests that Millennials are more willing to exchange personal information in return for targeted advertising than other users.[37]

While American social media users are apprehensive about privacy in the abstract, far fewer do much about it in the reality.[38] A 2003 Annenberg report on American approaches to privacy found that while Americans were very concerned about privacy, their actual knowledge of how they were protected or how to protect themselves was quite low.[39] While they wanted privacy, they did not understand computerized data flows or what privacy polices actually protect against.[40] Facebook users, for example, demonstrate a gap between their stated privacy concerns and their online behaviors.[41] Other surveys have found that users worry that information they do not want to share is available to their friends and family networks, but more abstract threats of government access to personal data is not as significant to them.[42]

[34] Anton, Earp, and Young, *supra* note 20, at 21.
[35] *Id.* at 22.
[36] Jay Stanley, *Do Young People Care About Privacy*? AMERICAN CIVIL LIBERTIES UNION (2013), https://www.aclu.org/blog/technology-and-liberty/do-young-people-care-about-privacy (last accessed 29 May 2015); Danah Boyd & Eszter Hargittai, *Facebook privacy settings: Who cares?*, 15 FIRST MONDAY (2010), http://pear.accc.uic.edu/ojs/index.php/fm/article/view/3086 (last accessed 29 May 2015).
[37] The Center for the Digital Future, *Is online privacy over? Findings from the USC Annenberg Center for the Digital Future show Millennials embrace a new online reality*, USC ANNENBERG NEWS (2013), http://annenberg.usc.edu/News%20and%20Events/News/130422CDF_Millennials.aspx (last accessed 29 May 2015).
[38] Stephen Cobb, *Do consumers pass the buck on online safety? New survey reveals mixed messages*, WE LIVE SECURITY (2013), http://www.welivesecurity.com/2013/11/13/do-consumers-pass-the-buck-on-online-safety-new-survey-reveals-mixed-messages/ (last accessed 29 May 2015); Acohido, *supra* note 7.
[39] JOESEPH TUROW, AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 37 (2003), http://www.securitymanagement.com/archive/library/Anneberg_privacy1003.pdf (last accessed 29 May 2015).
[40] *Id.* at 19–24.
[41] Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. COMPUT.-MEDIAT. COMMUN. 83–108, 86 (2009).
[42] Boyd and Hargittai, *supra* note 36.

While the Snowden revelations about government surveillance did have an impact on Americans, by at least heightening their awareness of privacy concerns[43], it was not enough to change behavior. In a survey conducted in January 2014 by the Pew Research Center, a majority felt that their privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality.[44] The survey used a sample of 607 American adults, 18 years of age or older. The survey was conducted by the GfK Group using Knowledge Panel and its nationally representative online research panel. Although most are aware of government efforts to monitor communications, the awareness naturally differs. Some 43% of adults have heard "a lot" about "the government collecting information about telephone calls, emails, and other online communications as part of efforts to monitor terrorist activity," and another 44% have heard "a little." Interestingly enough, most respondents in the Pew survey say they want to do more to protect their privacy, but many believe it is not possible to be anonymous online. When asked if they feel as though their own efforts to protect the privacy of their personal information online are sufficient, 61% say they feel they "would like to do more", which is in line with studies on the global file sharing community where slightly over 50 per cent wish to be more anonymous online.[45] The Pew study also concludes that "Americans' lack of confidence in core communications channels tracks closely with how much they have heard about government surveillance programs".[46]

In conclusion, generally speaking, surveys have shown that Americans care about digital privacy but most do not take measures to protect it. While we are interested in the global dimensions of privacy protection, this article drills down into the American case, *MegaUpload*, in more detail since the Snowden revelations brought into public debate the issue of privacy over digital content.

[43] Acohido, *supra* note 7; Turow, *supra* note 39, at 19.
[44] The Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (2014) http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (last accessed 29 May 2015).
[45] Måns Svensson, Stefan Larsson and Marcin de Kaminski, *The Research Bay – Studying the Global File Sharing Community*, in INTELLECTUAL PROPERTY IN CONTEXT: LAW AND SOCIETY PERSPECTIVES ON IP (Gallagher and Halbert, eds., 2015); Stefan Larsson, Måns Svensson, Marcin de Kaminski, Kari Rönkkö and Johanna Alkan Olsson, *Law, Norms, Piracy and Online Anonymity – Practices of de-identification in the global file sharing community*, JOURNAL OF RESEARCH IN INTERACTIVE MARKETING 6(4): 260-280 (2012).
[46] Pew Research Center, *supra* note 44, at 4.

4. From Filesharing to Encrypted Privacy: Privacy by Design and the MegaUpload Case

If privacy is to be ensured for those who do not have the technological capacity or legal comprehension to affirmatively protect their privacy, it must be done by design. Privacy by design will embed privacy at the technological level.[47] As privacy expert Ann Cavoukian notes, privacy by design is "the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality. Privacy must be embedded in systems, naturalized as part of the process and easy to use."[48] We use the ongoing saga of Kim Dotcom's conflict with the U.S. government as a means to understanding the implications of privacy by design.

In January of 2012 Kim Dotcom, founder of MegaUpload, found himself the subject of an international policing activity that involved the collaboration of US law enforcement and New Zealand's. Dotcom's house was raided, his computer servers were seized, his assets were frozen, and his property was confiscated based upon an indictment filed in U.S. Federal Court charging him with a variety of US computer-related and copyright infringement crimes.

At the time of Dotcom's very visible legal troubles, MegaUpload was one of the world's leading storage locker services. It allowed users to upload and store personal files as well as share these files with others. As with many storage locker services, the site had both legitimate and illegitimate uses. To the US government and the US entertainment industry, MegaUpload was one of the largest pirate file-sharing sites in existence. Despite claims that the site adhered to US policy regarding notice and takedown of infringing materials, the US government asserted that the primary function of MegaUpload was profiting from piracy. The US District Court of Virginia identified MegaUpload as "an international organized criminal conspiracy."[49] As a result, when the service was shut down, all MegaUpload's members lost their files, legitimate or not.

Kim Dotcom has fought the US indictment since it was issued and has so far managed to avoid extradition and any ruling has been delayed until February of 2015.[50] In 2014, he was able

[47] Thibaut Kleiner, *The Future of Privacy in the Internet Age: A European Perspective*, *in* CAHIER DE PROSPECTIVE: THE FUTURES OF PRIVACY 83–92, 91–92 (Carine Dartiguepeyrou ed., 2014).
[48] Cavoukian, *supra* note 17, at 10.
[49] *United States v Kim Dotcom et al*, 1:12-cr-3 (2012). See also http://www.justice.gov/usao/vae/megaupload.html (last accessed 29 May 2015).
[50] Lucy Craymer, *Kim Dotcom Extradition Decision Delayed*, WALL STREET JOURNAL (Jul. 8, 2014), http://www.wsj.com/articles/kim-dotcom-extradition-decision-delayed-1404796195 (last accessed 29 May 2015).

to win back his cars in New Zealand and he filed a counter suit in Hong Kong.[51] He has also become galvanized as a privacy advocate and Internet activist, perhaps an unlikely evolution for a man who seemed primarily driven by profit prior to his indictment.[52] Not one to be dissuaded by a criminal indictment, Dotcom has re-envisioned his MegaUpload site, based upon the basic fact that the Internet is both a tool for connectivity and surveillance. His new website, Mega, subtitled "A Privacy Company," offers members a service that is designed specifically to avoid the legal pitfalls encountered by MegaUpload. It is designed with encryption technology as a baseline for interaction and has created a filesharing/storage locker website that cannot be placed under government surveillance.[53]

The website for Mega offers the following justification for its existence:

> When we launched MEGA early [sic] 2013, global mass surveillance by rogue governments under the pretext of fighting terrorism was still a wild conjecture and its proponents were often touted as conspiracy theorists. Edward Snowden's revelations 137 days later fundamentally changed public attitudes and it became excruciatingly clear that *security by policy* (we have access to your data, but we promise to keep it confidential and not misuse it") had not been good enough. Anything short of *security by design* ("we cannot gain access to your data without you being able to find out"), for which strong end-to-end encryption is an essential prerequisite, now seems grossly insufficient.
>
> MEGA was architected around the simple fact that cryptography, for it to be accepted and used, must not interfere with usability. MEGA is fully accessible without prior software installs and remains the only cloud storage provider with browser-based high-performance end-to-end encryption. The only visible signs of the crypto layer operating under MEGA's hood are the entropy collection during signup, the lack of a password reset feature and the novel (and browser-specific) ways file transfers are conducted. Today, millions of business and personal users rely on MEGA to securely and reliably store and serve petabytes of data and we

[51] *Kim Dotcom wins back cars and cash*, BBC NEWS (2014), http://www.bbc.com/news/technology-27067102 (last accessed 29 May 2015).
[52] The YouTube video produced by Dotcom positions him clearly as a political actor for the digital world. KIM DOTCOM - MR PRESIDENT, (2012), http://www.youtube.com/watch?v=MokNvbiRqCM&feature=youtube_gdata_player (last accessed 29 May 2015).
[53] For an analysis of the protections afforded cyberlocker services like MEGA by the DMCA, see Ali V. Mirsaidi, *Mega, Digital Storage Lockers, and the DMCA: Will Innovation Be Stifled by Fears of Piracy?* 12 DUKE L. & TECH. REV. 12 (2014): 151.

> believe that this success is the result of MEGA's low barrier to entry to a more secure cloud.[54]

Dotcom also quotes the UN Declaration of Human Rights, Article 12 regarding the individual's right to privacy, in justifying the logic of his new system.

What can we learn about trust, surveillance and the digital future from Kim Dotcom's struggle with the U.S. government and the destruction of MegaUpload? Aside from the collection of personal data by the US federal government from the numerous individuals using the MegaUpload site, and the surveillance required in the name of copyright protection of the private transactions of millions of individuals from across the world, one significant lesson is that in a global world of information exchange and state surveillance, privacy as policy is not sufficient protection.

Dotcom's new company Mega is a privacy company based upon easy to use encryption because, as Dotcom notes, only when we have *security by design* are we safe from the watchful eyes of the government. He makes it clear that we should not trust policy alone to withstand government intervention – only strong technological solutions designed into the system can ensure adequate privacy from prying eyes.

To adapt Dotcom's language of security to the concept of privacy, this article investigates the tension between privacy by policy, as developed and "protected" through legal statutes and private privacy policy documents and the growing desire for privacy by design – the use of encryption and other technological infrastructure as a way to ensure that private data is not used illegitimately by states or private actors.

Encryption is central to privacy by design. The starting assumption should be a high level of privacy with people opting out as they choose. This can be accomplished through different approaches including encryption or privacy by distribution where either the user or the system itself distributes information in a manner that does not allow for its aggregation.[55] While Dotcom was not the first to advocate for encryption based systems as the only way to avoid the surveillance of the state and corporate actors (both aligned in his case to halt what they see as massive copyright infringement), he has built a system that makes encryption easy and assumed as the first layer of doing business. Edward Snowden, unsurprisingly, has also come out as an

[54] MEGA, https://mega.co.nz/#about (last accessed 29 May 2015).
[55] Goldstein, *supra* note 32; Aghasaryan, *supra* note 27, at 112.

encryption advocate. He notes, "The biggest thing an Internet company can do today to protect rights of users is to enable encryption on every page you visit. The reason this matters is that today if you go to look at a copy of *1984* on Amazon.com – the NSA, the Russians, the Chinese, can all see a record of that. It isn't encrypted and you cannot choose to use encryption when browsing for books."[56] He goes on to say that there is a need to move to encrypted browsing habits by default because this increases privacy and rights worldwide. As he noted, we have a right to privacy because we recognize that trusting any government authority with human communications in secret without oversight is too great a risk to be ignored.[57]

Examples of security by design that are available as opt in systems include Tor, designed to protect user privacy from network surveillance and traffic analysis.[58] Other such programs exist such as the VPN Spotflux, or systems like Do-Not-Track, which allows the user to opt-out of tracking websites.[59] The innovators of PGP privacy are about to release a new encrypted telephone that is designed with security and privacy in mind. The creators are trying to make a smart phone whose whole purpose is to protect users privacy. Part of their logic is that privacy is a commodity now and the Blackphone is built on giving this back to the user.[60]

While there is significant debate about the use, value, and future of Bitcoin, its grounding in anonymity and privacy cannot be disputed. All of these systems focus on integrating encryption technology seamlessly into the user experience. In the case of Mega, Dotcom nor those working for Mega can even see what is exchanged, absolving them, you can say, from liability for future copyright infringement. By flipping the starting point and building in privacy by design, all users are more secure.

5. Conclusion

In *The Circle*, despite the concerns and resistance of one of the original founders of the company, the plan to make surveillance ubiquitous and fully collaborative prevails. It does so because it is wrapped in the friendly form of 'likes' and social networks. The company successfully shifts the social norm to disclosure and argues that only when we truly have nothing

[56] HERE'S HOW WE TAKE BACK THE INTERNET, *supra* note 6.
[57] *Id.*
[58] *Anonymity Online*, TOR PROJECT, https://www.torproject.org/ (last accessed 29 May 2015).
[59] Do Not Track - Universal Web Tracking Opt Out, , http://donottrack.us/ (last visited May 15, 2015).
[60] Matt Clinch, *Taking on BlackBerry: The Mobile that Promises Privacy*, CNBC (2014), http://www.cnbc.com/id/101337734 (last accessed 29 May 2015).

to hide can we be free. Those who try to resist living their lives publicly and being constantly surrounded by social media are now suspects. In other words, a form of friendly fascism where people happily consume and socialize under the constant scrutiny of the corporate world and the state has been realized.

Is privacy by policy sufficient? We would argue that it is necessary but not sufficient. Take, for example, the massive data breach and theft suffered by Target customers. Despite warnings that malware had infected their system, over 40 million credit card numbers and other user data were stolen.[61] Privacy policies did nothing to help the 40 – 70 million people with impacted or stolen data. Target can say "sorry" but their policy on privacy is just paper. Snowden's revelations also prove that policy-based privacy is not sufficient. In the name of national security, the US federal government has ensured that any paper commitment to privacy is merely that – paper with no real force. There are backdoors, secret wiretaps, secret courts, and an entire network of surveillance for the sake of national security that occurs despite laws on the books to protect citizens against such activities. The NSA programs created and enforced in secret require big business to be complicit with government acquisition of data and the American people to be in the dark about what is collected and about whom. Verizon's privacy policy, for example, is no protection against the national security state.

While Americans may change their privacy settings or shut off the applications they download to their phones if these apps raise privacy concerns, the underlying technologies are still ones of surveillance. This seems to suggest that there is, what Yong Jin Park calls, a second tier digital divide developing – between those who are technologically sophisticated enough to understand how to manipulate privacy settings to their advantage and the far larger segment of the population who does not understand how privacy operates in a digital environment.[62] There remains trust on the part of the consumer that privacy by policy is sufficient to protect their interests. However, as Park warns, making policy based upon the assumption that individuals are well informed about technology and privacy will lead to deeply flawed policy because the

[61] Adi Robertson, *Target's security system reportedly caught massive hack, but was ignored for weeks*, THE VERGE (2014), http://www.theverge.com/2014/3/13/5503952/targets-security-system-reportedly-caught-massive-hack-but-was-ignored (last accessed 29 May 2015).
[62] Yong Jin Park, *Digital Literacy and Privacy Behavior Online*, 40 COMMUN. RES. 215–236, 232 (2013).

assumption that individuals understand the technological and privacy issues is itself deeply flawed.[63]

Privacy by design is a crucial step in the ongoing digital revolution and one that needs to be taken up, publicly debated, and implemented. It is an idea that is gaining traction.[64] In 2012, the Federal Trade Commission issued a report in which they advocated for the inclusion of privacy by design principles into data practices.[65] Of course, conceptualizing privacy by design as a policy choice still requires technical solutions to be developed, an issue that will take time.[66] However, research completed by Rubenstein and Good revealed that, despite the benefits of privacy by design, it is unlikely that such a system can be implemented voluntarily and greater attention will need to be paid to how we envision such designs at a technical level.[67]

Based upon the fact that we must place trust in e-commerce and personal communication to make the modern economy function, debates over the depth and scope of privacy are important. Both government and private actors claim that privacy by policy is sufficient to protect the individual and that technological backdoors for spying, methods of collecting data, and constant surveillance of all Internet activities about the individual is simply not a problem, as long as the policy statement discloses how things are working. However, this article has argued otherwise. It may be time to flip the default privacy settings from one where our information is shared in exchange for services and ease of communication to one where each individual affirms consciously the choice to share their private information with private industry or the state. In other words, our policy discussion must be one that implements privacy by design.[68]

[63] *Id*. at 232.
[64] Antonialli, *supra* note 25, at 332. (arguing that privacy by design is increasingly popular in policy discourses).
[65] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 112 22 (2012).
[66] Ira A. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECHNOL. LAW J. 1333–1413 (2013).
[67] Federal Trade Commission, *supra* note 65 at 1407–1410.
[68] Acknowledgments: Swedish Research Council d.no. 437-2013-336.