Engaging the Public in Ethical Reasoning About Big Data

Justin Anthony Knapp [1,*]

Email justinkoavf@gmail.com

[1] Free culture and digital liberties advocate, Indianapolis, USA

Abstract

The public constitutes a major stakeholder in the debate about, and resolution of privacy and ethical issues in Big Data research about human affairs. Thus, scientists must learn to take public concerns about Big Data research seriously and how to communicate messages designed to build trust in specific big data projects and the institution of science in general. This chapter explores the implications of various examples of engaging the public in online activities such as Wikipedia that contrast with "Notice and Consent" forms and offers models for scientists to consider when approaching their potential subjects in research. Drawing from Lessig, *Code and Other Laws of Cyberspace*, the chapter suggests that four main regulators drive the shape of online activity: Code (or Architecture), Laws, Markets, and Norms. Specifically, scientists should adopt best practices in protecting computerized Big Data (Code), remain completely transparent about their data management practices (Law), make smart choices when deploying digital solutions that place a premium on information protection (Market), and, critically, portray themselves to the public as seriously concerned with protecting the privacy of persons and security of data (Norms). The community of Big Data users and collectors should remember that such data are not just "out there" somewhere but are the intimate details of the lives of real persons who have just as deep an interest in protecting their privacy as they do in the good work that is conducted with such data.

Ethical concerns in Big Data are of particular interest to a variety of professionals, researchers, and specialists. As the volume and variety of such data continue to grow rapidly, individuals from fields as different as geography and biomedical sciences to software engineering and sociology will have a wealth of new material available to further their academic and financial interests. All of these fields will have to adapt to the unique ethical issues related to digital privacy rights and the management of previously inconceivable amounts of data.

AQ1

But researchers are not the only stakeholders in these issues. Certainly, academics and other professionals will have to devise new guidelines for their internal use and public policy may have to change rapidly but these modifications will be of limited value if the public at large does not understand or engage with the broader community of those who are gathering and using such data. Both to maintain the integrity of such data sets and to protect possibly vulnerable individuals, it is imperative that the ethical reasoning behind Big Data decision-making is a transparent and intelligible process. This chapter will attempt to discuss what some of the ethical issues are in Big Data collection and a theory of how to think about privacy rights. Throughout, examples will be given from both academic literature and everyday life which will hopefully encourage researchers to think about how they can communicate with the public about Big Data. A theoretical approach is adopted and applied to several intersecting segments of society with an emphasis on civic actors. Finally, a few practical suggestions will be given that may prove useful for ensuring the integrity of the data themselves as well as providing confidence to the public who are giving the data.

Theoretical frameworks for understanding violations of privacy and consent can come from civil liberties and social justice movements. One early approach can be taken from American lawyer Lawrence Lessig, whose 1999 book *Code and Other Laws of Cyberspace* was written for a lay audience and published at a time when there was little existing legislation or public discussion on digital civil liberties. In that work, he suggests that there are four main regulators of online activity: Code (or Architecture), Laws, Markets, and Norms. There are inherent technical features of what technology we have and how they function which can generally be referred to as “Code”. In the case of Big Data, that infrastructure has exploded into realms which were science fiction in 1999. For instance, security research firm Trend Micro created “GasPot” which is a digital honeypot used to simulate a gas pump (in computing honeypots are deliberately unsafe traps designed to attract malicious agents such as identity thieves or spammers). They found that this digital gas pump had 23 attacks on it in the course of a few months in early 2015 simply by virtue of being connected to the Internet. The clear implication is that actual gas pumps which accept our credit card information and have connections to security cameras are possibly just as vulnerable and definitely far more dangerous if compromised.

Big Data are collected, analyzed, and sometimes disseminated by private and well as public actors. For instance, the accumulation of market research data through social media has made it possible for ad companies such as Facebook and Google to create vast digital empires using business models that would have been impossible a decade ago. Additionally, government agencies collect huge quantities of data through telecommunications for the purposes of law enforcement, surveillance, epidemiology, and a host of other concerns. The technological tools that have allowed these organizations to gather and analyze these data are simply too sophisticated and change too rapidly for the public at large to give informed consent about the collection and use of such information. This requires the public to give a greater level of trust to these institutions than ever before, including many instances of implicit approval or simple blind faith in the best intentions of corporate and governmental organizations.

To use a simple example, virtually no users read software end user license agreements (EULAs) (Bakos et al. 2014). This problem has been apparent for over a decade and has resulted in serious breaches of privacy on the part of users who have made unwarranted assumptions about software providers being well-intentioned and who have also been intimidated by increasingly dense legalese used for increasingly long agreements. As this software becomes more deeply embedded in everyday life, it is unreasonable to expect that the average user will have a true understanding of what kind of information is being collected about him and how it will be used. The terms of such EULAs almost invariably favor sellers over users and buyers (Marotta-Wurgler 2011).

In the United States, many researchers could be considered members of the civic sector—they do not have the same priorities as private business interests nor public state actors, although at times have features of both or work with either. Civic sector organizations such as non-profits and co-operatives generally have greater degrees of trust placed in them in part due to the legal and practical demands of transparency that are placed upon them. Problems of trust are particularly acute amongst voluntary associations by their very nature as they cannot compel compliance like a state actor and they typically cannot provide the compensation of businesses. Since trust is a key element in the efficacy of institutions to perform (Newton and Norris 1999), it is necessary that researchers engender that trust by actively engaging the public when it comes to privacy concerns about Big Data; otherwise, they risk losing out on possible sources of data through non-compliance and disinterest.

Public perceptions of Big Data, privacy, and digital civil liberties in the United States can be dated to pre- and post-Edward Snowden whisteblowing. Reports vary about the ways in which Americans have modified their online habits as well as the extent to which they are concerned about issues related to pervasive surveillance. For instance, Preibusch (2015) concludes that although, “media coverage of [American domestic spying program] PRISM and surveillance was elevated for the 30 weeks following PRISM day, many privacy behaviors faded quickly”. Alternatively, Schneier (2014) point out that over 700 million Internet users worldwide have taken some steps to change their behavior to avoid National Security Agency surveillance. The survey data conclude that in the United States and abroad, average Internet consumers definitely have concerns about personal privacy in Big Data from governmental (CIGI-Ipsos 2014 ; Rainie and Madden 2015) as well as corporate sources (Fisher and Timberg 2013). One possible explanation for this seeming disjunct between attitudes and behaviors is how difficult it is for typical Internet users to understand complex tools for protecting privacy. Since the polling data and common sense tell us that online services as well as portable and wearable computers are such ordinary devices for millions, they are unwilling or unable to forgo their convenience and ubiquity in spite of genuine, rational concerns about Big Data collection and retention.

In the face of this, some providers of online services have offered or mandated tools which are intended to make Internet users more secure. This is one part of reaching out to the public about ethical concerns in Big Data: using “push” technologies that force users to be more privacy-conscious. For instance, in 2015, the Wikimedia Foundation (WMF)—operators of several online educational resources, including Wikipedia—filed suit against the NSA and Department of Justice with representation by the American Civil Liberties Union. Their argument was that the hundreds of millions of users of the encyclopedia were harmed by indiscriminate collection of upstream data by the United States federal government. The case was dismissed due to lack of standing with the court arguing that the plaintiffs could not prove they were subject to upstream surveillance. How in principle they could prove this when the surveillance program is secret was not explained by the court. ~~T~~hey appealed in 2016 and comparable filings by non-profits such as *Clapper v. Amnesty International US* have been dismissed on similar grounds.

The ~~WMF also~~ implemented HTTP Strict Transport Security (HSTS) on all Web traffic starting later that year, which is the culmination of a process begun years prior to Snowden’s whistleblowing activities. This technology requires users to access to the site using an encrypted connection rather than plain HTTP which allows intermediary agents like Internet service providers (ISPs) to view traffic in plain text. Previously, users were simply given the option of viewing the encyclopedia with HSTS and in 2013, logged in users were required to use it as a part of editing. The average reader would not notice any difference aside from a small icon changing in a web browser but this policy seriously decreases the possibility of “man in the middle” attacks which allow faking of credentials. These attacks had become increasingly common across the Web in the first decade of the encyclopedia’s existence.

As a 501(c)(3) charitable organization, they regularly publish transparency reports which inform users of federal government demands for data. They also helped to generate significant political action in 2012 by blacking out Wikipedia to protest SOPA and PIPA—proposed Congressional legislation that would have had a chilling effect on online communication and which would have imposed mandated snooping of users by ISPs. Subsequent attempts by law enforcement to deputize ISPs have been introduced regularly and have been defeated by a combination of political will and public outcry.

These attempts to engage the public on digital privacy are not limited to non-profits. One such example of a large Internet community operated as a for-profit is link-sharing message board Reddit, which is run as an independent company with former direct owner Advance Publications as a large shareholder. The site also participated in SOPA/PIPA blackouts and began publishing transparency reports in 2015, explicitly acknowledging privacy concerns related to online surveillance. They have also taken a hardline stance on harassing behavior including doxxing—the intentional leaking of personally identifying information about users. These details are published in order to shame or threaten others into silencing them from discussing controversial topics. Sometimes, this is done purely as prankery and other times it is to gain privilege to someone’s real life, such as sending threats in the mail. The tension between free speech to share information and the concerns of vulnerable individuals and groups which require anonymity has played out in controversial message boards which site administrators deemed to be excuses for harassment and trolling. The site has banned user accounts and boards which existed solely to mock minority groups or which attempted to spread nude celebrity photos after high-profile data breaches. Similar struggles between free expression which culminates in abuse is not purely theoretical or confined to cyberspace—protests on college campuses about safe spaces and allegedly bigoted policies ha~~s~~ve been increasing in the United States for years. This is another valuable method of engaging the public: creating community norms and rules which demand respecting others’ privacy. As it becomes understood as a part of simple etiquette that others have a reasonable expectation of privacy, the ethical principle behind that rule can be more easily enforced and encouraged.

A unique hybrid of a state agency cooperating with a non-state actor is the TOR Project. This organization was created in 2006 to manage the TOR Browser as well as other online communication projects which are based on “onion routing” initially developed by the United States Naval Research Laboratory. The history and technical specifications of the technology can be complicated but simply put, onion routing passes Internet communications through several encrypted layers—hence the metaphor of an onion. Since the data are bounced around many agents before reaching their final destination, it is extremely difficult to determine where a request originated and the only way to reliably de-anonymize this traffic is if a user does it himself, such as by accidentally associating his personal e-mail address with activities performed on the TOR software network. The initial purpose of the technology was for military intelligence but it has since grown into a vast network which runs a kind of parallel Internet sometimes known as the Dark Web which includes sites that can only be accessed via the TOR Browser. The Dark Web includes the same type of mundane information that anyone would anticipate on the Internet such as chat and search services but also allows for new opportunities for illicit drug sales, gun smuggling, fraud, and other illegal or gray market activities. It also allows for very secure communication between whisteblowers and news agencies, especially when it is paired with SecureDrop which lets users share files with one another.

The ironic twist is that law enforcement not only monitors this traffic heavily and conducts sting operations using it but actually provides much of the architecture that allows for this communication in the first place with computers that connect to the TOR network know as “exit nodes”. Intelligence agencies are in the curious position of both making this highly secure communications technology and constantly trying to undermine its integrity. For instance, in 2014 a number of international law enforcement agencies cooperated to shut down Dark Web drug markets, particularly Silk Road 2.0 which usually operated by trading designer drugs for Bitcoin. In the process, it is suspected that the FBI paid researchers at Carnegie Mellon University to try to break the anonymity of the TOR network. The relationship between the public and civic sectors here becomes as complicated as the technical aspects of the software itself but the take-away for researchers who have highly sensitive data is that TOR paired with SecureDrop is an excellent way to transfer information. Additionally, it is very user-friendly, unlike other secure systems such as PGP for e-mail. In the words of the NSA itself, TOR is “the King of high-secure, low-latency Internet anonymity” with “no contenders for the throne in waiting”.

Such attempts to engage the public are also not limited to online service providers. Manufacturers of mobile devices have also promoted more secure communication—for instance, Apple has included end-to-end encryption in recent models of iPhones and had a high-profile dispute in 2016 with the FBI regarding attempts to decrypt a phone associated with a mass shooting. The other major smartphone vendor is Google, whose Android operating system comes in several varieties across many devices, so their approach to encrypted communications cannot be as uniform as Apple but they have also insisted to the public as well as law enforcement agencies that the company has no way of accessing the content of messages sent on Android devices (and these claims are easier to substantiate since Android is made of free software that anyone can modify or audit for security concerns). They have issued similar warnings to users of their Chrome web browser and other services they provide. This is in the interests of both the end user and the company, who can claim plausible deniability about being liable for the content of any messages sent using these devices and services. If they cannot in a technical sense snoop on users, then they cannot be mandated to do so legally. This frees up resources that the company can use to be profitable rather than be deputized for surveillance.

One large lacuna in this discussion is connected devices which are not personal computers per se. Wearable devices including fitness trackers, home furnishings such as thermostats, and even the increasingly sophisticated computers in automobiles are all connected to Internet cloud service providers through the Internet of Things (IoT). It is possible that this vast array of mundane objects will provide far greater and more intimate information about users than even personal computers and smartphones. They also have unique vulnerabilities: researchers have shown through controlled tests that these devices can be hijacked remotely by third parties to cause motorists to lose control of their vehicles and critically important medical devices can be caused to malfunction. Fear of malicious hackers (i.e. “crackers”) who want to take control of these systems may cause members of the public to be skeptical of helpful and professionally gathered data. The ironic side effect is that users will have given up masses of information involuntarily in their day-to-day lives but will not be willing to trust researchers who have good intentions for gathering data and professional standards for maintaining confidentiality. This can literally start from birth with connected devices such as baby monitors. Gao (2015) has shown that Americans already believe overwhelmingly that they want to control their personal information but cannot. This problem could be particularly acute as responsiveness to polling has been falling in America for several years prior to concerns about snooping. (Christian et al. 2012) Researchers who use wearable computers are encouraged to consider whether or not real-time data collection is necessary or appropriate for their projects. Some of these devices can collect and store data on the device itself and that data can be retrieved once the gadget is returned rather than broadcasting it.

These problems are apparent even to agencies which traffic in Big Data—in 2012, the NSA internally promoted a staffer to be the “Socrates of the National Security Agency” and write a column on ethical issues for other employees. One serious question already raised is that of consent. It is taken for granted in professional fields that handle private data that consent must be given to acquire such data and that a subject must be informed in order to give that consent, such as in Health Insurance Portability and Accountability Act (HIPAA) requirements for medical investigators and practitioners. But HIPAA requirements break down when paired with Big Data, as insurers and third parties can easily de-anonymize such data by comparing it to public records. And since such data are held by a variety of hospitals and health plans, they are vulnerable to attack by identity thieves who have a thriving market for pilfered medical records. (Chideya 2015) Vendors such as Microsoft are working on entirely new encryption and data management schemes specifically for the medical industry.

Returning to Lessig’s framework, legal challenges to protecting digital civil liberties have become increasingly necessary in the United States. The executive and legislative branches either struggle to keep up with a changing landscape for digital privacy or are simply too invested in mining such data to want to constrain themselves from getting it—consider that the CIA even spied on Congress under provisions of the Patriot Act. Founded in 1990, the Electronic Frontier Foundation (EFF; which has included Lessig on its board) is one of the oldest digital rights organizations and has participated in several legal challenges to surveillance and other breaches of digital privacy. Although U.S.-based, they work globally to challenge repressive laws and partner with other such non-profits. There has perhaps been no other organization as successful in reaching the public regarding digital rights issues.

Lawsuits do not only target government agencies and outreach to the public must also include market-based solutions. The commercial world is deeply invested in Big Data and this creates an inherent tension between personal privacy and efficiency in firms. This dichotomy has been challenged by Calo (2015) who argues that markets actually rely upon privacy to function and that the Federal Trade Commission "has emerged as the de facto privacy authority in the United States". There need not be a disjunct between privacy and profitability in Big Data, especially since innovative products and services are created in market situations in order to *preserve* the integrity of such data. It is important to balance critiques of government surveillance with market reform in order to make a robust and durable culture of digital rights. (Paterson 2014) The division between legal- and market-based solutions also breaks down when we consider the great extent to which private and public entities cooperate on collecting and trading Big Data. One such collaboration is police departments in dozens of states which pay for the rights to databases generated by repo firms using license plate scanners. These devices take millions of pictures of license plates in parking lots and compare them to records that the company has to determine where a delinquent customer is in order to tow an automobile. These data are collected with virtually no effort and can be used to track the movements of almost anyone with an automobile.

But cultures do not exist based solely on tools, legal codes, and commerce. The final piece of Lessig's framework is norms—which by their very nature are not codified. As Lessig puts it in *Code*, "we live life subject to these norms… [they] constrain us in ways that are so familiar as to be all but invisible". These tacit feelings regarding privacy are sometimes the strongest ways of reaching the public regarding their digital rights. For instance, once a member of the public is shown how trivial it can be to de-anonymize Big Data or to make inferences based on what has been collected, this can cause a sense of having been violated. These inchoate expressions of outrage have been manifested in public demonstrations like Restore the Fourth rallies which were held throughout the United States roughly overlapping the Occupy movement but also come up in mundane situations such as when one swipes to view the next picture on someone's smartphone without permission. In order to effectively reach the public, it is necessary to capitalize on these justified perceptions which take abstract and sometimes overly complicated arguments about end-to-end encryption or monitoring of air-gapped laptops through heat signatures and makes these ethical concerns salient. Harnessing such feelings and making them persist into something more substantial is imperative.

What does this all mean for the research community? Academics do not have the power or resources of multinational corporations or governments, so the concerns raised above may seem irrelevant. For that matter, institutional review boards and professional standards act as watchdogs against malfeasance—they are not perfect instruments but they generally work well and create an ethical culture amongst academia. Big Data problems can still exist through misperception and a simple lack of understanding of best practices. If the horizon of the digital landscape moves too quickly for the public, then it certainly can for researchers as well who are deeply invested in their work and the systems that they have in place. Well-intentioned and competent investigators still have to be able to communicate to the public as well as their peers that Big Data are secure and that best practices are followed.

This chapter has largely focused on the United States but there is a serious tension between Americans and Europeans characterized by Kerry (2014) as, "conventional wisdom in Europe that Americans do not care about privacy~~”.~~ This can cause a serious rift and have legal implications. Take the example of Boston College and “The Belfast Project”—an oral history on The Troubles in Northern Ireland which was created in 2001. Researchers interviewed former IRA members whose personal stories included details about illegal activity. The interviewers assured the subjects that their stories would remain confidential until they died but those tapes were requested by the Police Service of Northern Ireland leading to a legal battle that has lasted for years. It is further complicated by the fact that the College has distanced itself from the Project organizers and the History Department claimed to be largely ignorant of it even existing until the 2010 publication of the book *Voices from the Grave*. The precedent this sets legally and culturally can have serious implications for researchers but it is a microcosm of a larger issue of trust between American and European institutions.

To use the framework that Lessig created, researchers can discuss Big Data privacy with the public by referring to Code, Laws, Markets, and Norms. In terms of Code, researchers can make sure that they are using best practices by consulting EFF publications and using some of the digital tools that they make available at no cost. Another excellent resource for electronic privacy is the Electronic Privacy Information Center (EPIC), which is a Washington, D. C.-based research center. Similar digital rights organizations exist globally such as Bits of Freedom in The Netherlands, South Africa’s Right2Know, and the United Kingdom’s Open Rights Group. One radical solution may involve simply not using digital records in the first place or digitizing print records for the purposes of analysis and then destroying the digital copies but retaining the print ones. This measure may prove impractical for many researchers but even simply having the computers which store Big Data be disconnected from the Internet is enough to make these records far more secure. Alternately, researchers can store large datasets on optical media or thumb drives. This division between devices which are connected and those which are not is not only a practical concern but one that helps to ease the fears of members of the public—as Hogan and Shepherd (2015) found, “control of the physical location of data centers shapes the possibilities of data agency and ownership”. If you can display to the public how Big Data are stored in a different place and disconnected from the Internet, it can increase feelings of security in addition to the actual level of security itself.

In terms of Law, compliance is actually a double-edged sword. Since one of the main reasons for apprehension about Big Data collection is government snooping, it is important to communicate to the public that you have a transparency policy and explain what you do with data and with government requests for data. Researchers may wish to publish a warrant canary and similar statements about data integrity aimed at informing the public about the seriousness with which the academic community takes data sensitivity.

Regarding Market-based changes, researchers are encouraged to look for alternatives to common technologies which provide greater security and lower cost. Using computers which have free operating systems can allow for more flexibility and control over the settings of the device—examples include BSD and GNU/Linux rather than Mac OS X and Windows. This has the added bonus of encouraging further use of safer computer systems. The more common it is to use these operating systems, the more tools will be developed for them. Additionally, these software communities have volunteers who work on making fixes and taking suggestions on how to improve their work, so if there is a feature that you would like to see, you can suggest it. (Note that the free database program PostgreSQL is slated to include Big Data functionality.) Not all researchers will be able to invest the time in learning new operating systems nor will they always be able to control which devices they can use but it is worth discussing which options are legitimate with someone in an IT department who can likely offer some alternatives.

Finally, normative outreach to the public is powerful and can be accomplished through subtle means. The attitudes that Big Data researchers have are as important as any tools or laws. As Boyd (2010) has suggested, “the biggest methodological danger zone presented by our collective obsession with Big Data: *Just because data is accessible doesn’t mean that using it is ethical*~~”~~. [emphasis in the original] Having a friendly and approachable manner when discussing privacy engenders greater trust. There is a human element to Big Data that can sometimes be overlooked by an obsessive focus on computers and smartphones as well as assumptions that more data are always better (recall the problems of finding needles in haystacks).

Conducting research today is an exciting and dangerous prospect. Big Data exists in virtually every form about almost all of us and it is used in ways that were unimaginable in the past. It is paramount that the community of Big Data users and collectors remember that such data are not just “out there” somewhere but are the intimate details of real persons’ lives and they have just as deep an interest in protecting their privacy as they do in the good work that is conducted with such data. It remains to be seen if the world has the wisdom and forbearance to follow the advice of Wau Holland: protect private data, use public data.

References

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies, 43*(1), 1–35. doi: 10.1086/674424 .

Boyd, D. (2010). Privacy and Publicity in the Context of Big Data. Retrieved from http://www.danah.org/papers/talks/2010/WWW2010.html .

Calo, R. (2015). Privacy and Markets: A Love Story. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2640607 .

Chideya, F. (2015). Medical Privacy Under Threat in the Age of Big Data. Retrieved from https://firstlook.org/theintercept/2015/08/06/how-medical-privacy-laws-leave-patient-data-exposed/ .

Christian, L., Dimock, M., Doherty, C., Keeter, S., & Kohut, A. (2012). Assessing the Representativeness of Public Opinion Surveys. Retrieved from http://www.people-press.org/files/legacy-pdf/Assessing%20the%20Representativeness%20of%20Public%20Opinion%20Surveys.pdf .

CIGI-Ipsos. (2014). CIGI-Ipsos Global Survey on Internet Security and Trust. Retrieved from https://www.cigionline.org/internet-surveyl .

Fisher, M. & Timberg, C. (2013). Americans Uneasy About Surveillance But Often Use Snooping Tools, *Post* Poll Finds. Retrieved from https://www.washingtonpost.com/world/national-security/americans-uneasy-about-surveillance-but-often-use-snooping-tools-post-poll-finds/2013/12/21/ca15e990–67f9-11e3-ae56-22de072140a2_story.html .

Gao, G. (2015). What Americans Think About NSA Surveillance, National Security and Privacy. Retrieved from http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ .

Hogan, M., & Shepherd, T. (2015). Information ownership and materiality in an age of big data surveillance. *Journal of Information Policy, 5*, 6–31. doi: 10.5325/jinfopoli.5.2015.0006 .

Kerry, C. (2014). Missed Connections: Talking with Europe About Data, Privacy, and Surveillance. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2014/05/20-europe-privacy-surveillance-kerry/kerry_europefreetradeprivacy.pdf .

Marotta-Wurgler, F. (2011). Some realities of online contracting. *Supreme Court Economic Review, 19*(1), 11–23. doi: 10.1086/664560 .

Newton, K., & Norris, P. (1999). Confidence in Public Institutions: Faith, Culture, or Performance? Retrieved from http://www.hks.harvard.edu/fs/pnorris/Acrobat/NEWTON.PDF .

Paterson, N. (2014). End user privacy and policy-based networking. *Journal of Information Policy, 4*, 28–43. doi: 10.5325/jinfopoli.4.2014.0028 .

Preibusch, S. (2015). Privacy Behaviors After Snowden. *Communications of the ACM, 58*(5), 48–55. doi: 10.1145/2663341 .

Rainie, L., & Madden, M. (2015). Americans' Privacy Strategies Post-Snowden. Retrieved from http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf .

Schneier, B. (2014). Over 700 Million People Taking Steps to Avoid NSA Surveillance. Retrieved from http://www.lawfareblog.com/over-700-million-people-taking-steps-avoid-nsa-surveillance .