The US Privacy Strategy

Timothy Edgar(✉)

Watson Institute for International and Public Affairs,
Brown University, 111 Thayer St., Providence, RI 02912, USA
timothy_edgar@brown.edu

Abstract. The hopes of privacy advocates that US president Barack Obama would implement digital privacy reforms have been largely dashed by revelations of extensive US government surveillance. Such revelations have added an acute sense of urgency among ordinary people to the debate over privacy, surveillance, and technology. Unfortunately, despite the existence of innovative cryptographic techniques to protect privacy, US policymakers have so far not taken advantage of them to enable signals intelligence collection in more privacy-protective ways. The problem is not limited to controversial surveillance programs. A once-promising US strategy for online identity, the National Strategy for Trusted Identities in Cyberspace (NSTIC), may also fall short on privacy because of a failure to use available privacy-protecting tools. There is no excuse of such ignorance of the cryptographic state of the art. There is a critical need for greater awareness of privacy-enhancing technologies among policymakers.

Keywords: Privacy · Surveillance · NSA · Privacy-enhancing technologies · Signals intelligence · Online identity

1 Introduction

This paper tells a tale of two privacy debates – a debate about surveillance, and a debate about online identity. The first debate concerns government access to data, and is related directly to the NSA surveillance programs disclosed in the past few years. The second largely concerns the practices of companies, not governments, as the private sector works to establish a new system of online authentication. Nevertheless, company misuse of personal information, no less than NSA spying, has raised widespread concerns among the public [1].

I participated in both the surveillance and the online identity debates while I served in the Obama White House as a privacy advisor. In both cases, we were aware of potentially groundbreaking technologies that could help us achieve our goals without sacrificing privacy. Nevertheless, we did not manage to make use of them. Unfortunately, little has changed: the hard work of implementing privacy-preserving technologies has barely begun.

D. Aspinall et al. (Eds.): Privacy and Identity 2015, IFIP AICT 476, pp. 19–29, 2016.
DOI: 10.1007/978-3-319-41763-9_2

2 Time for a Revolution – Or a Requiem?

The title of this year's IFIP summer school – "time for a revolution?" – is a fitting one. The world continues to grapple with the fallout from revelations that began in June 2013 of extensive surveillance by the United States National Security Agency and allied intelligence services. Although Edward Snowden, a contractor for the NSA, disclosed government surveillance programs, the debate he began has sparked a broader global conversation about digital privacy. Ordinary people have become acutely aware of privacy as a value that is in the process of being lost. Only a revolution, it seems, can reverse the process.

At the IFIP summer school venue in Edinburgh, the theme of privacy resonated well beyond dry conversations of academics in the fields of law, policy and technology. Surveillance, privacy, and a loss of trust were the themes of an evocative audiovisual performance at the Edinburgh festival, a work of music and visual art by Matthew Collings and Jules Rawlinson that explored these issues on an emotional level. The performance struck a deep chord.

The title of Collings' and Rawlinson's work, "A Requiem for Edward Snowden", captures a deep distrust of the US government and especially of its intelligence agencies. Explaining the title, Matthew Collings described his view that Snowden would not survive his break with the NSA. "I was convinced that he would shortly be dead", Collings said. Collings also explained that he conceived of his "requiem" in a broader sense. "The death of the excitement of the internet" was a theme of the piece, Collings explained. "It's about the death of privacy, too" [2].

Edward Snowden, of course, remains alive, although on the run. Perhaps the same may be said of privacy. While the causes for diminished privacy are numerous, one culprit is the ignorance of lawmakers, policymakers and business leaders. While they should know better, they continue to insist that we trade privacy for security and convenience. Many people are willing to accept the argument that we have no choice but to sacrifice privacy for other important values only because they are not aware of privacy-enhancing technologies. These technologies may mitigate such trade-offs – if we choose to deploy them.

3 From "Yes, We Can" to "Yes, We Scan"

The election campaign of Barack Obama in 2008 raised expectations in the United States and around the world for a season of progressive change. Perhaps the mood was captured best in the iconic poster created by artist Shepard Fairey, featuring a stencil portrait of Obama, shaded in red, white and blue. Obama gazes thoughtfully into the distance. Below, there is the single word: "Hope". Other versions featured Obama's campaign slogan: "Yes, we can!" [3].

As Barack Obama took office in 2009, privacy and civil liberties advocates had some reason to be optimistic. During his campaign, then-Senator Obama faulted President George W. Bush for excessive claims of executive power in the "war on terrorism". In remarks on the campaign trail, Obama denounced the NSA's "warrantless wiretapping" program, authorized by Bush shortly after September 11, for exceeding

Bush's constitutional authority. He promised that, if elected, he would ask his legal team to review NSA surveillance programs and would reverse excessive executive orders "with the stroke of a pen" [4].

While the stage seemed to be set for a major shift on issues of surveillance and privacy, careful observers noticed nuances in Obama's remarks that were lost on much of the general public. On the campaign trail, Obama did not echo his supporters in denouncing the USA PATRIOT Act, the much-maligned law that broadened surveillance powers. Instead, Obama reserved his sharpest criticism for the way in which Bush had authorized surveillance programs, not for the programs themselves.

Charlie Savage, a national security reporter for The New York Times, notes that Obama consistently advocated a "rule of law" critique rather than a civil liberties critique when discussing national security. Obama argued that the Bush administration's approach was a threat to the separation of powers between the executive, legislative, and judicial branches outlined in the U.S. Constitution, upsetting its system of checks and balances. Obama did not voice nearly as strong an opinion on whether Bush policies violated the individual rights guaranteed in the Bill of Rights [5, pp. 50–55].

What was lost on many Obama supporters was the fact that the "rule of law" critique had become less relevant as the Bush presidency was coming to a close. Bush's second term in office was marked by an effort to normalize counterterrorism powers. Bush administration lawyers had already stepped back from some of the maximalist positions that they had advanced in the early days after September 11. The NSA surveillance programs that Bush created in his first term by executive order were now authorized by orders of the Foreign Intelligence Surveillance Court.

Obama was briefed on these programs shortly after he took office. He learned they were no longer based on a theory that the president, as Commander-in-Chief, could override the will of Congress and bypass the federal courts in order to conduct surveillance of the enemy in a time of "war on terrorism". Instead, NSA surveillance programs were now firmly grounded in federal law, as interpreted by the surveillance court. The court had accepted the expansive interpretations that national security lawyers had urged to bring Bush's unilateral surveillance programs under the court's purview. As a result, Obama chose to continue these NSA programs without substantial change.

Obama turned his attention to a broader privacy agenda. The major items were strengthening consumer privacy and addressing the growing problem of cybersecurity. The privacy issues associated with cybersecurity monitoring were complex and difficult. Obama was the first U.S. president to devote a major address entirely to the subject of cybersecurity. In 2009, he announced an ambitious plan to strengthen security for government and critical infrastructure networks. As part of that plan, he ordered a new initiative to facilitate the development of a system of online identity management, led by the private sector, that would include significant privacy safeguards [6].

In Obama's cybersecurity address, he also announced that he would appoint a privacy and civil liberties official to the White House National Security Staff, serving its new Cybersecurity Directorate. I was chosen to fill that position. Obama's decision to create my position reflected how important privacy issues had become in national security policy. While the National Security Council had long employed a small staff to address human rights issues, I became the first privacy official to serve on the NSC staff.

In June 2013, the Obama administration was blindsided by an avalanche of unauthorized disclosures of NSA surveillance programs. Edward Snowden, a young NSA contractor then living in Hawaii, had absconded with a trove of highly classified documents detailing the United States government's aggressive world-wide signals intelligence collection operations. Snowden leaked his documents to Glenn Greenwald, Laura Poitras, and other journalists. Over a series of months, stretching into years, the public was treated to a series of alarming revelations of global surveillance operations.

For many of Obama's progressive supporters, already dismayed by his continuation of Bush counterterrorism policies, the revelations were a shocking breach of trust. A parody of the Shepard Fairey "Hope" poster captures the sense of betrayal. Obama's portrait is modified to show him as an eavesdropper. He is outfitted with headphones, and the slogan underneath the portrait mocks his promise of change: "Yes, we scan", it reads. Fairey himself shares the dismay. In an interview in May 2015, Fairey said that Obama had not lived up to the famous image he had created for him. "I mean, drones and domestic spying are the last things I would have thought" Obama would support, he said [7, 8].

The government confirmed many of the surveillance programs that Snowden leaked. The programs that have occasioned the greatest debate in the United States involve programs of domestic collection. They include bulk collection of telephone metadata under section 215 of the USA PATRIOT Act and collection of Internet and other communications content under section 702 of FISA, where the data is inside the United States but the direct targets are foreign. These programs involve oversight by the Foreign Intelligence Surveillance Court.

Other controversial programs include surveillance of foreign leaders, bulk collection of foreign communications and data, and NSA's efforts to undermine global communications security. These programs fall outside the Foreign Intelligence Surveillance Act. They are authorized by Executive Order 12,333, and are subject to looser oversight rules enforced entirely within the Executive Branch. They do not require oversight by any court.

The intelligence community's initial reaction to the Snowden revelations was based on the way it had responded to similar controversies in the past. Intelligence officials denounced Snowden for betraying government secrets, and defended surveillance programs by pointing to protections for the privacy of American citizens and residents – "United States persons", in the jargon of intelligence oversight rules. U.S. person information was protected, officials said, in all intelligence activities. For those programs subject to the oversight of the surveillance court, the rules were even stricter.

The strategy fell flat. According to opinion polls, a majority of Americans viewed Edward Snowden more as a whistleblower than a traitor. They did not trust the NSA's assurances that their data was protected by privacy rules. Congress was up in arms about bulk collection of telephone metadata. The backlash surprised an intelligence community that had become accustomed, ever since the attacks of 9/11, to receiving the benefit of the doubt when it came to programs said to be necessary to fight terrorism.

The reaction of the international community also put the Obama administration under considerable pressure. German chancellor Angela Merkel was deeply offended to learn that her communications had been a target of NSA spying, and the German public

shared her outrage. Brazilian president Dilma Rousseff was also angry when she found out the NSA had monitored her communications. Brazil organized an international conference on Internet governance, and raised awkward questions about U.S. dominance of the Internet's physical and economic infrastructure. Other friendly countries were likewise demanding explanations.

The administration also found itself under pressure from the technology industry. In late December 2013, executives from major technology companies, including Apple's Tim Cook, Yahoo's Marissa Mayer, and Google's Eric Schmidt, met with President Obama at the White House to press their concerns about NSA surveillance. The intelligence community's standard defense – our surveillance is directed at foreigners and we have rules to protect "U.S. person" information – was not addressing industry's concerns. If anything, the argument was counterproductive, as it implied that the privacy of foreign citizens did not count for anything. American technology companies were facing a real danger of lost business abroad. Estimates of lost business ranged from $35 billion to $180 billion, according to industry groups [9, 10].

4 Obama's Surveillance Reforms

The harsh reaction to the Snowden revelations made surveillance reform an imperative for the Obama administration. Obama's first step was to order his Director of National Intelligence, James Clapper, to increase the transparency of intelligence programs. Clapper had become infamous in the days after the revelations had begun in June 2013 for his denial at a public Congressional hearing that the NSA had records belonging to "millions or tens of millions of Americans". Clapper believed his answer was, in his words, "the least untruthful" statement he was able to give at the time, while preserving the secrecy of the NSA's programs.

Now, Clapper was put in charge of a drive to inform the public about how the NSA worked. He used a popular microblogging platform, "tumblr", to launch "IC on the Record", disseminating thousands of pages of declassified documents detailing the rules about how the NSA programs work. They included scores of once-secret surveillance court opinions. By the fall of 2013, one transparency advocate, Steve Aftergood, marveled, "Already we've seen a more extensive disclosure of classified information about current intelligence programs than we've seen for at least 40 years, and maybe ever." By March 2014, Obama's transparency reforms had resulted in the authorized disclosure of more than twice as many previously classified documents as Snowden had leaked [11, 12].

Advocates remained skeptical that the transparency reforms would last, viewing the initiative merely as a tactic to fight back against the Snowden leaks. Still, the intelligence community also put in place more permanent policies. They include an annual "transparency report" detailing the number of targets affected by orders of the Foreign Intelligence Surveillance Court. Previously, only the number of orders was released – a relatively meaningless number, given new legal authorities that allowed one order to cover tens of thousands of targets. The intelligence community also created an implementation plan to institutionalize its newfound commitment to transparency.

Obama's reforms went further than increased transparency. Obama also enhanced intelligence oversight to protect the privacy rights of foreigners. Presidential Policy Directive 28 (PPD-28), issued in January 2014, extends for the first time the mechanisms that the intelligence community uses to protect "U.S. person" information explicitly to protect information belonging to anyone, anywhere in the world. While the substance of the rules is relatively modest, the concept is revolutionary [13].

Retention and minimization limits that once applied only to U.S. persons now apply to all "personal information". Other protections have been codified as well. Signals intelligence cannot be used to disadvantage anyone, anywhere in the world, on the basis of race, gender, sexual orientation, or religion. The rules now explicitly prohibit such misuse of intelligence information – for example, by blackmailing a foreign leader who is gay.

PPD-28 also places limits on "bulk collection of signals intelligence". Bulk collection is not prohibited, but it is limited to six specific national security threats. The NSA may no longer collect signals intelligence in bulk unless it is to protect against espionage, international terrorism, proliferation of weapons of mass destruction, cybersecurity threats, threats to U.S. or allied military forces, or transnational crime. Broader foreign affairs objectives may now be achieved only through targeted intelligence collection.

Congress has also taken action to reform surveillance. In June 2015, section 215 of the USA PATRIOT Act was set to expire. As we have seen, it was an expansive interpretation of section 215 that was the legal authority for bulk collection of telephone metadata. The bulk collection legal theory was under fire. Although the Foreign Intelligence Surveillance Court continued to issue orders under section 215, civil liberties groups had challenged bulk collection in other federal courts. In a major blow to the government, the United States Court of Appeals for the Second Circuit ruled in May 2015 that bulk collection was not authorized by section 215 [14].

The Obama administration and a majority of both houses of Congress had negotiated an alternative to bulk collection, which was enacted shortly after section 215 expired. The principal sponsors of the reform bill, Senator Patrick Leahy (D-VT) and Representative James Sensenbrenner (R-WI), had been the original sponsors of the USA PATRIOT Act of 2001. Leahy and Sensenbrenner were responsible for that law's extravagantly Orwellian name, which is an acronym for the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act". Leahy and Sensenbrenner gave their bill to reform surveillance a similarly extravagant name, albeit one that leans in favor of civil liberties. The law that ended bulk collection is the USA FREEDOM Act of 2015, which stands for the "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act".

The USA FREEDOM Act extended the expiring provisions of the USA PATRIOT Act, including section 215, for another four years, while prohibiting its use for bulk collection. The USA FREEDOM Act replaces bulk collection with a system under which telephone metadata will remain with the companies, but is subject to rapid queries by NSA analysts. NSA analysts must use a "specific selection term" to retrieve data; much of the debate over the bill concerned the breadth of this definition.

Congress also enacted reforms to the Foreign Intelligence Surveillance Court. Congress required the court to issue declassified versions of significant opinions – such as opinions that would interpret "specific selection term". Congress also created a mechanism for the court to appoint a "special advocate" – a lawyer with a top security clearance who could potentially challenge government lawyers before the court.

5 Using Technology to Protect Privacy: A Missed Opportunity?

The debate over surveillance reform in the United States has largely been a debate about law, usually among lawyers. Does section 215 of the USA PATRIOT Act authorize bulk collection? Is it constitutional? What should be rules for surveillance of foreign targets under section 702 of the Foreign Intelligence Surveillance Act? Is section 702 constitutional? The assumption is that a more refined set of legal rules can better calibrate societal trade-offs between privacy and security.

In the legal debate, privacy is often on the defensive. Of course, civil libertarians argue for legal rules that restrict collection, retention and use of personal information as a bulwark against abuse. Nevertheless, the public is likely to discount such arguments if it is sufficiently fearful of terrorism, reasoning that preventing attacks may be worth some risk of privacy abuse.

Technology offers an opportunity to reframe the debate. Some of the trade-offs that the policy debate takes for granted have increasingly become obsolete. Advances in cryptography over the past decade now provide new alternatives to mass surveillance programs. Cryptography often gives us the opportunity to "have our cake and eat it too", according to Anna Lysyanskaya, a computer scientist at Brown University. She argues that, "at least in theory", we can "gain the benefits of the digital age without sacrificing privacy". The argument for privacy is far stronger if there are practical alternatives that meet government's legitimate objectives [15].

In PPD-28, President Obama tasked the Director of National Intelligence with providing a report "assessing the feasibility of creating software that would allow the [intelligence community] more easily to conduct targeted information acquisition rather than bulk collection". It was a hopeful sign. An organization within the DNI's office, the Intelligence Advanced Research Projects Activity (IARPA), had funded substantial research in the areas of cryptography that could be helpful in preserving the privacy of data. The DNI, in turn, assigned the task of writing the report to the National Academy of Sciences (NAS).

The NAS report was something of a disappointment. While it recommended new software "to more effectively target collection and to control the usage of collected data", it discounted the more ambitious goal of replacing bulk collection altogether.

For one thing, the report noted, unless information is collected in bulk, there was no guarantee that data about past events would be available when needed; the database owner might not retain it. No cryptographic technique can recreate data that no longer exists. Cryptography also requires more computational power than collection and analysis of the bulk data in unencrypted form, i.e., "in the clear" [16, pp. 9–10].

The report concluded that "there is no software technique that will fully substitute for bulk collection; there is no technological magic."

While the report's conclusion was valid, its tone sent the wrong message. The disparaging use of the term "magic" was especially unfortunate, as advanced cryptographic techniques can produce results that, to the non-specialist, seem precisely like magic! One example is private information retrieval. Imagine that one party, such as the NSA, would like to retrieve information from a large database held by another party, such as a cloud computing provider, under section 702 of FISA. Without private information retrieval, the NSA must either trust the provider with its highly classified list of selectors, or the provider must trust the NSA with unrestricted access to its database or provide it with a complete copy. Private information retrieval uses cryptography to allow the NSA to search the company's database without the company learning the NSA's query, but with complete confidence that only data matching those selectors will be provided to the NSA.

Similarly, bulk collection of metadata could benefit from the use of secure two-party and multiparty computation. Under the USA FREEDOM Act, the NSA may no longer use section 215 of the USA PATRIOT Act to obtain in bulk all telephone metadata maintained by the telephone companies. Under the new law, those bulk records will remain with the companies. The NSA, however, may rapidly query metadata about people in communication with its targets and also about people in communication with those people – out to two "hops". It would seem the NSA's only choice is to trust the telephone companies with its target list so they can retrieve the information, hopefully without leaking classified information.

If that trust turns out to be misplaced, would the NSA's only solution be to ask Congress to restore bulk collection so it can go back to doing this for itself? Secure multiparty computation provides an alternative. It would permit the NSA to find the records that it needs by posing an encrypted question to an encrypted database maintained by the telephone companies. The NSA would learn nothing about data that it did not need. The telephone companies would learn nothing about the NSA's queries.

Using such techniques would provide at least some of the benefits of bulk collection, without the cost to privacy. They are only effective if they can be made efficient and can work on a large scale. As early as 2008, there was a demonstration of large scale, real-world use of secure multiparty computation that permitted participants in the Danish sugar-beet market to agree on a pricing scheme. In 2014, computer scientists proposed a scalable system using secure two-party computation, "Blind Seer", that could be deployed by an agency like the NSA with little cost to efficiency. [17] IARPA funded the research on "Blind Seer".

The government has known about privacy enhancing technologies for many years – as we have seen, it funded much of the research that has made the use of such techniques practical. Policymakers, however, continue to be largely unaware of the ways in which technology can mitigate trade-offs that may otherwise appear to be unavoidable. The debate over bulk collection and mass surveillance since 2013 has, unfortunately, so far been marked by a missed opportunity to "have our cake and eat it too".

6 Online Identity

Surveillance is not the only problem in which ignorance of technology is potentially dangerous to privacy. In Obama's cybersecurity address of 2009, he announced that he would propose an ambitious strategy to facilitate a more secure and effective system of online identity management. We worked on the strategy for two years. In 2011, the White House released its "National Strategy for Trusted Identities in Cyberspace" (NSTIC), a plan to create a secure "identity ecosystem", led by the private sector. A major goal of the NSTIC initiative is to move away from passwords to more reliable forms of identity management, allowing people to engage in transactions that requires higher levels of identity assurance [18].

The Commerce Department has taken the lead on implementing NSTIC, launching a dialogue with companies and other stakeholders. NSTIC has significant privacy implications. A system of online identity could pose a real threat to privacy, especially if it permits companies or the government more easily to link together all of a user's individual Internet activities and transactions.

NSTIC contains ambitious privacy goals. NSTIC calls for "privacy-enhancing technical standards" that "minimize the transmission of unnecessary information", allowing transactions that are "anonymous, anonymous with validated attributes, pseudonymous, and uniquely identified." The drafters of NSTIC were aware of the work on "anonymous credentials" by Jan Camenisch and Anna Lysyanskaya and other computer scientists. Anonymous credentials employ zero-knowledge proofs to allow the holder of a credential to validate the attributes that another party needs to complete a transaction online without revealing anything more (see e.g. [19]; an excellent non-technical explanation can be found in [20]).

While NSTIC did not proscribe a specific technical solution, fully realizing its privacy goals would require the use of anonymous credentials. The alternative is to trust an "identity provider" to validate online transactions. Initial NSTIC pilots, however, appear to be following the "trusted third party" model. One start-up, "ID.me", touts itself as a "trusted intermediary" for verifying identity. The founders of ID.me are featured on the government's NSTIC website meeting with President Obama. Even if third parties such as ID.me have excellent privacy policies, consumers are being asked to trust yet another entity with their private information [21, 22].

As with surveillance reform, the implementation of the Obama administration's online privacy strategy has so far missed an opportunity to make use of an innovative technology that could enhance privacy. Instead, policymakers and businesses are insisting on trade-offs that we do not have to make.

7 Ignorance of Technology Is no Excuse!

Ignorantia juris non excusat. "Ignorance of the law excuses not" is an ancient principle that prevents the guilty from escaping the consequences of flouting society's laws. The law has proven to be a less-than-ideal guardian of our privacy. A contributing factor to the failure of law and policy has been the ignorance of lawmakers and policymakers

about innovative privacy-enhancing technologies. If we want to preserve our privacy, we must adopt a new principle – ignorance of technology is no excuse!

While the reasons for such ignorance are not entirely clear, the most likely explanation may be the loose and inconsistent rules that have allowed, at least in the United States, broad public and private sector use of large databases containing personal information without technical safeguards. If the use of privacy-enhancing technologies is regarded not as a necessary precondition for the use of such data, but only as a matter of academic interest, there is little reason for policymakers to become familiar with them. Compounding the problem, even informed and motivated policymakers may not know what questions to ask. Many privacy-enhancing technologies offer capabilities that are not obvious and may appear like magic to non-specialists.

The time has come for privacy-minded academics and advocates to evangelize on behalf of the benefits of privacy-enhancing technologies to a much broader audience. Privacy advocacy should move away from bemoaning the death of privacy towards offering a vision that breathes life into privacy.

As the performance of a "Requiem for Edward Snowden" was able to capture in image and music, we are at a crucial moment – a moment that calls for a revolution in privacy. If we fail to take stronger steps to accelerate real-world deployment of innovative solutions for preserving privacy, its legacy may best be celebrated by a singing a requiem for privacy – whatever the fate of the former NSA contractor hiding out in Moscow.

References

1. Cox, A.M.: Who should we fear more with our data: the government or companies? The Guardian, 20 Jan 2014 (2014). http://www.theguardian.com/commentisfree/2014/jan/20/obama-nsa-reform-companies-spying-data. Accessed 11 Feb 2016
2. Pollock, D.: How Edward Snowden inspired a musical vision of the future. The Scotsman, 20 Aug 2015 (2015). http://www.scotsman.com/lifestyle/culture/music/how-edward-snowden-inspired-a-musical-vision-of-the-future-1-3863946. Accessed 8 Feb 2016
3. Barton, L.: Hope – the image that is already an American classic. The Guardian, 9 Nov 2009 (2009) http://www.theguardian.com/artanddesign/2008/nov/10/barackobama-usa. Accessed 20 Feb 2016
4. Remarks by senator Barack Obama in Lancaster, Pennsylvania. CNN, 31 March 2008 (2008). https://www.youtube.com/watch?v=AzgNf9iZ2Bo. Accessed 11 Feb 2016
5. Savage, C.: Power Wars: Inside Obama's Post-9/11 Presidency. Little, Brown and Company (2015)
6. Remarks by the president on securing our nation's cyber infrastructure, 29 May 2009 (2009) https://www.whitehouse.gov/video/President-Obama-on-Cybersecurity#transcript. Accessed 20 Feb 2016
7. Patches, M.: Shepard fairey on the future of political art and whether Obama lived up to his "hope" poster. Esquire, 28 May 2015 (2015). http://www.esquire.com/news-politics/interviews/a35288/shepard-fairey-street-art-obama-hope-poster/. Accessed 20 Feb 2016

8. Jauregui, A.: Yes we scan: shepard fairey likes Obama NSA parodies, “Pleased” with subversive symbolism. Huffington Post, 23 June 2013 (2013). http://www.huffingtonpost.com/2013/06/28/yes-we-scan-shepard-fairey-obama-nsa_n_3517213.html. Accessed 20 Feb 2016
9. Rushe, D., Lewis, P.: Tech firms push back against White House efforts to divert NSA meeting. The Guardian, 17 Dec 2013 (2013). http://www.theguardian.com/world/2013/dec/17/tech-firms-obama-meeting-nsa-surveillance. Accessed 21 Feb 2016
10. Miller, C.C.: Revelations of N.S.A. spying cost U.S. tech companies. N.Y. TIMES, 21 March 2014 (2014). http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html. Accessed 21 Feb 2016
11. Aftergood, S.: ODNI rethinks secrecy and openness in intelligence, federation of American scientists. Secrecy News (blog), 20 March 2014 (2014). https://fas.org/blogs/secrecy/2014/03/litt-transparency/. Accessed 21 Feb 2016
12. Johnson, C.: Snowden’s leaks lead to more disclosure from feds. NPR Morning Edition, 11 Oct 2013 (2013). http://www.npr.org/2013/10/11/231899987/snowdens-leaks-lead-to-more-disclosure-from-feds. Accessed 21 Feb 2016
13. Presidential Policy Directive – Signals Intelligence Activities (Presidential Policy Directive 28/PPD-28), 17 Jan 2014 (2014). https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. Accessed 21 Feb 2016
14. American Civil Liberties Union v. Clapper, No. 14-42-cv (2nd Cir. 7 May 2015)
15. Lysyanskaya, A.: Cryptography is the future. In: Rotenberg, M., Horwitz, J., Scott, J. (eds.): Privacy in the Modern Age: The Search for Solutions, pp. 112–118. The New Press (2015)
16. National Research Council: Bulk Collection of Signals Intelligence: Technical Options. The National Academies Press (2015)
17. Pappas, V., et al.: Blind seer: a scalable private DBMS. In: 2014 IEEE Symposium on Security and Privacy, pp. 359–374 (2014)
18. The White House; National Strategy for Trusted Identities in Cyberspace, April 2011 (2011). http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. Accessed 21 Feb 2016
19. Camenisch, J.L., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
20. Lysyanskaya, A.: Cryptography: how to keep your secrets safe. Scientific American, Sept 2008 (2008). http://www.scientificamerican.com/article/cryptography-how-to-keep-your-secrets-safe/
21. www.nstic.gov/nistc/. Accessed 21 Feb 2016
22. ID.me Digital Credentials Now Accepted Across Government Websites. Business Wire, 3 Dec 2014 (2014). http://www.businesswire.com/news/home/20141203006149/en/ID.me-Digital-Credentials-Accepted-Government-Websites#.VSbEimZygTX. Accessed 21 Feb 2016

http://www.springer.com/978-3-319-41762-2

Privacy and Identity Management. Time for a Revolution?
10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Edinburgh, UK, August 16-21, 2015, Revised Selected Papers
Aspinall, D.; Camenisch, J.; Hansen, M.; Fischer-Hübner, S.; Raab, C. (Eds.)
2016, XII, 359 p. 78 illus., Hardcover
ISBN: 978-3-319-41762-2