Privacy, Surveillance and Digital Trust in the American Case

Halbert, Debora

Published in:
DigiTrust: Tillit i det digitala. Tvärvetenskapliga perspektiv från ett forskningsprojekt

2014

Privacy, Surveillance and Digital Trust in the American Case

Debora Halbert

While generally kept out of sight, government surveillance ostensibly to ensure the security of the state from threats (both foreign and domestic) is a hallmark of the American national security state. What types of surveillance are legally allowable is constantly contested as new technologies emerge that must be tested against American constitutional principles and international law. In the wake of the Snowden revelations about the depth and scope of government spying, new concerns regarding protection of personal data have emerged and eroded trust in American government as well as private entities that have collaborated either willingly or unwillingly with the government.

In addition to the broader national security interests, other trends dominate the evolution of surveillance, privacy and trust in the United States. Among the many emerging surveillance techniques are first, predictive policing based upon metadata and surveillance systems. Using the same algorithm to predict earthquake aftershocks, Police in Santa Cruz have developed a predictive policing mechanism that helps to stop crime before it can happen.[1] The FBI has publicized this big data program as one of the next generations of crime fighting.

Second, persistent surveillance systems are being developed that offer a wide area visual surveillance to track crime in real time and offer additional information for criminal investigations. Third, while drones are primarily understood as playing a role in our national security outside the domestic territory of the United States, they have also begun to play a role in total surveillance within the United States as well. Fourth, facial recognition software can now function better than humans, suggesting new ways of capturing data in public places and documenting the movements of

[1] http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/April/predictive-policing-using-technology-to-reduce-crime

individuals (Lu & Tang, 2014). Finally, the Internet of everyday things, converging with RFID technologies that can track everything from books and clothing to passports to people brings additional layers of surveillance to play.

These technologies are built upon the assumption that crimes both cyber and real must be met with adequate scrutiny and that threats can be halted through surveillance. Furthermore, the lucrative future of the business of security continues to innovate surveillance technologies that make the Orwellian world of total surveillance closer than ever (Deibert, 2013). These technologies are sold off the shelf to democracies and dictatorships alike (Soghoian, 2013). Surveillance for profit is big business.

Privacy by Policy

In the face of persistent and extensive data surveillance, what protections exist for personal privacy?

In the United States, the predominant method for protecting privacy is for a company to issue a written privacy policy statement. Privacy by policy means that we must trust those who control 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 US federal government as well that 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 (Cranor et al., 2014). Additionally, even without sharing, individual companies have amassed astounding amounts of personal data about their users. While surveys suggest that Americans do not want to be tracked online, even with privacy policies, most websites engage in some sort of tracking (Martin, 2013). It takes serious effort to get and/or stay off the grid (Goldstein, 2014). So much time in fact, that as Jessica Goldstein has noted, it is not worth the effort (Goldstein. 2014). 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 (Anton et al., 2010, p.24).

Is privacy by policy sufficient? We would argue that it is necessary but not sufficient. Snowden's revelations prove that policy-based privacy is not sufficient as well. 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 is no protection against the national security state.

Privacy by design

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 (Kleiner, 2014, pp.91–92). 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 (Cavoukian, 2011, p.10)." Encryption is central to privacy by design. The starting assumption should be a high level of privacy with people opting out of privacy protections as they choose.

Examples of security by design include Tor, designed to protect user privacy from network surveillance and traffic analysis.[2] Other programs such as the VPN Do-Not-Track, which allows the user to opt-out of tracking websites are readily available for a monthly fee.[3] New devices taking privacy into consideration are also being innovated. The creators of PGP privacy are about to release a new encrypted telephone, the Blackphone, that is designed with security and privacy in mind (Clinch, 2014; Robarts, 2014).

Conclusion

Some might argue that without adequate security measures we face the potential failure of digital economic systems. Persistent attacks and criminal efforts to acquire personal data, data theft, and the like are becoming far more sophisticated and undermine the potential for digital commerce. While the argument is that we must

[2] https://www.torproject.org/

[3] http://donottrack.us/

give government and industry the ability to fight by keeping individual privacy settings low, others argue that the lack of privacy and the existence of US created built back doors into key security software has made the world less safe. As Snowden suggests, "if we loose the trust of SSL which was specifically targeted [by the NSA] we will live in a less safe world. We won't be able to access banks or do commerce without worrying if someone is monitoring us (Snowden, 2014)."

Based upon the fact 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. This report seeks to argue otherwise. It is 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.

References

Anton, A.I.; Earp, J.B. & Young, J.D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security Privacy*, 8(1), 21–27.

Cavoukian, A. (2011). *Privacy by design in law, policy and practice: a white paper for regulators, decision-makers and policy-makers*. Ontario: Information and Privacy Commissioner. http://www.privacybydesign.ca [2014-05-19]

Clinch, M. (2014). Taking on BlackBerry: the mobile that promises privacy. *CNBC.com*. http://www.cnbc.com/id/101337734 [2014-05-13].

Cranor, L.F. et al. (2014). *Are they worth reading? an in-depth analysis of online advertising companies' privacy policies*. Rochester, NY: Social Science Research Network. Available at: http://papers.ssrn.com/abstract=2418590 [Accessed May 7, 2014].

Deibert, R.J. (2013). *Black code: inside the battle for Ccyberspace*. Plattsburgh, NY: Signal.

Goldstein, J. (2014). Meet the woman who did everything in her power to hide her pregnancy from big data. *Think Progress*. http://thinkprogress.org/culture/2014/04/29/3432050/can-you-hide-from-big-data/ [2014-05-04].

Kleiner, T. (2014). The future of privacy in the internet age: a European perspective. In Dartiguepeyrou, C. (ed). *Cahier de Prospective: the Futures of privacy*. France: Foundation Telecom, Institut Mines-Telecom, 83–92.

Lu, C. & Tang, X. (2014). Surpassing human-level face verification performance on LFW with GaussianFace. *arXiv:1404.3840 [cs, stat]*. http://arxiv.org/abs/1404.3840 [2014-04-24].

Martin, K. (2013). Transaction costs, privacy, and trust: the laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*, 18(12). http://pear.accc.uic.edu/ojs/index.php/fm/article/view/4838 [2014-05-06].

Robarts, S. (2014). Updated specs released for the Blackphone secure smartphone. *Gizmag*. http://www.gizmag.com/updated-sgp-technologies-blackphone-specs/31852/ [2014-05-13].

Snowden, Edward. (2014). *Here's how we take back the Internet*, TedTalks. Available at: http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet [2014-04-24].

Soghoian, Christopher, (2013). *Government surveillance — this is just the beginning*. Ted Talks. http://www.ted.com/talks/christopher_soghoian_government_surveillance_this_is_just_the_beginning [2014-04-14].