Security and Privacy: Why Privacy Matters

Citation: Bird, Stephanie J. "Security and Privacy: Why Privacy Matters." Science and Engineering Ethics 19, no. 3 (July 27, 2013): 669–671.

As Published: http://dx.doi.org/10.1007/s11948-013-9458-z

Publisher: Springer Netherlands

Persistent URL: http://hdl.handle.net/1721.1/103787

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Editorial (for SEE Vol. 19, no.3)

Security and Privacy: Why Privacy Matters

Stephanie J. Bird

PO Box 2007
Wrentham, MA 02093
USA

E-mail: sjbird@mit.edu

A long-overdue discussion of security and privacy is taking place within the U.S. and among its friends and associates in many parts of the globe, in large part due to the revelations of Edward Snowden, the employee of a government contractor, who leaked secret information about the extent of U.S. government data collection on the calling habits of U.S. residents. Privacy is often pitted against security, thereby creating a false dichotomy that is a discussion for another time. However, if it is granted, for the time being, that security and privacy are at opposing ends of a continuum along which a balance point can and should be found, that is, that there is a theoretical point at which "enough security" is balanced against "enough privacy", then the tragedy of lives, hopes, and futures torn apart by the misplaced violent anger and frustration of others clearly elicits an immediate and deep-seated, visceral response, and underscores the importance of security. But does security outweigh or even trump privacy? More importantly, should it?

The frequent, simplistic response is "I am not worried about privacy. -- I don't have anything to hide." While there is much to be said for openness and transparency, they can nevertheless be over-rated and are seldom uncomplicated. For example, travelers

who are obliged to wear adult diapers for urinary incontinence would certainly rather not be patted down by an agent of the Transportation Security Administration (TSA) at the airport. Furthermore, almost everyone knows someone with whom they would not share a secret, their own or someone else's, and not just because it might be passed on and, as a result, hurt or alienate a third party (or worse, be passed along *for the purpose of* hurting or alienating another). Rather, secrets go unshared at least in part because almost everyone has learned that *any* bit of information is open to interpretation and misinterpretation, subject to conscious and unconscious assumptions and biases in the mind of anyone who has access to it -- It is the lesson of gossip and rumors. People tend to be prone to a number of well-known fallacies of thinking: over-generalizing; acting as if "might makes right"; assuming that correlation is causation; thinking that if something could be explained, it can be predicted; unconsciously and arbitrarily dividing the world into "us" and "them"; and many others (Bird 2012).

Characteristics that make us human, although not uniquely so, include curiosity, independence, intelligence and the capacity to see the familiar in new ways. These qualities lead to creativity, art and innovation. Yet these qualities and their products are also open to interpretation and misinterpretation that can make others fearful, jealous and spiteful, as well as inspired. In groups, people also have a tendency toward ‘group think’, peer pressure, social control and social order, and not always in a good way. As a result, errors that individuals make are compounded and can lead to majority factions (Madison 1787), poor policies and bad laws.

At a European Commission conference on bio-identification, a major issue discussed

by the attendees was the concern that a large set of data that individuals might provide voluntarily for one purpose (e.g., for banking, health care, or a credit card application) would or could be linked with another large set of data, intentionally or unintentionally, with or without authorization, for another purpose entirely. There are massive sets of data now being created for a variety of potentially justifiable reasons: phone logs revealing calling patterns, genetic makeup of individuals, voter lists, credit card purchases, shopping patterns, ... the list is long and impressive. Behind every algorithm and computer-generated list is a human mind, or group of them. The lists are created by humans for humans, often with the unfounded assumption that there will be safeguards to assure that the lists will only be used by a disinterested someone for an entirely acceptable purpose. What are these safeguards? Who will develop them? And who will interpret and enforce them? How will it be determined that the individuals with access to the data are "disinterested"? How will they be monitored? What is/are acceptable purposes? Who will decide? Both the private sector and governmental/public agencies may have a number of reasons, benign and otherwise, to be interested in the thoughts, plans and actions of citizens, residents and consumers, from selling a product to preventing an act of violence. At the same time, large data sets provide the raw materials that can be assembled to produce a Frankensteinian monster in the mind of anyone who is interested and able to look. In a democracy that respects its citizens and where government is of, by, and for the people, openness and transparency regarding the collection of individuals' information, by whom and for what purpose, are crucial.

Our high school English class read George Orwell's *Nineteen Eighty-Four* (Thank you Dr. Shulman!), a tale of a dystopian society where "Big Brother" monitored

everyone's every move, with the expectation of being able to monitor and manipulate everyone's every thought. The reality television program "Big Brother" (Columbia Broadcasting System - CBS) makes me wonder whether the participants in the program, and/or its viewers have read *Nineteen Eighty-Four*. Increasingly public space is arrayed with closed circuit television and security cameras. Now there are gadgets that monitor a user's eye movements and stop doing what they are doing when the user looks away, and new televisions are being equipped with cameras/sensors that can detect who is watching, whether the heart rate of the viewer(s) changes, who leaves the room and when, even when the television is turned off. Have the inventors or the intended buyers/users read *Nineteen Eighty-Four*? It is certainly time to re-read *Nineteen Eighty-Four* and speak up for privacy.

References

Bird, Stephanie J. (2012) Potential for Bias in the Context of Neuroethics. Commentary on "Neuroscience, Neuropolitics and Neuroethics: The Complex Case of Crime, Deception and fMRI". *Science and Engineering Ethics* 18 (3): 593-600. doi:10.1007/s1 1948-012-9399-y.

Madison, James (1787) The Federalist No. 10: The Utility of the Union as a Safeguard Against Domestic Faction and Insurrection (continued) *Daily Advertiser* November 22, 1787. Also available at http://www.constitution.org/fed/federa10.htm Accessed July 4, 2013.

Orwell, George (1949) *Nineteen Eighty-Four*. ISBN: 978-0-452-28423-4