The Tension Between Privacy and Security

Susan Maret  
*San Jose State University*

Antoon De Baets  
*University of Groningen*

Follow this and additional works at: https://scholarworks.sjsu.edu/secrecyandsociety

Part of the History Commons, Law Commons, Political Science Commons, and the Public Affairs, Public Policy and Public Administration Commons

**Recommended Citation**  

This Documents is brought to you for free and open access by the School of Information at SJSU ScholarWorks. It has been accepted for inclusion in Secrecy and Society by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.
The Tension Between Privacy and Security

Keywords
human rights, national security, privacy, public policy, secrecy

The Report of the Special Rapporteur, written by Joseph Cannataci, who was appointed in 2015 by the U.N. Human Rights Council as the first Special Rapporteur on the right to privacy (United Nations Office of the High Commissioner, 2016).
Commissioner 2016). *Liberty and Security* is drafted by “five outside” experts that comprise the President’s Review Group on Intelligence and Communications Technologies. These experts, who each in their own way was connected to the U.S. national security policy establishment, are Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. The Group was appointed in August 2013 with a deadline of December 2013 to complete their task of reviewing National Security Agency data collection policies, both domestic and foreign. The Group called itself “the five guys,” after the Five Guys Burger and Fries chain, and for the “big book they’d soon be writing as 'The Five Guys Report'”(Kaplan 2016, 255). The 308 page unclassified report *Liberty and Security in a Changing World* is their final work product.

Neither the Special Rapporteur or the “five guys” reports formally acknowledges Edward Snowden’s June 2013 disclosure of the National Security Agency's (NSA) covert activities pertaining to bulk collection of domestic and foreign emails, phone calls, and telephone metadata. The Snowden revelations – as a symptom of secret profiling, surveillance, and intelligence sharing by many governments - is central to understanding the policy recommendations of both reports. In particular, the *Report* is a conversation in that it opens dialogue with those official bodies active in carrying out profiling and spying. To this end, the Special Rapporteur

“Has continued a programme of continuous engagement with law enforcement agencies and security and intelligence services world-wide in an effort to better understand their legitimate concerns and recognise best practices which could be usefully shared as well as to identify policies, practices and legislation of doubtful usefulness or which present an unacceptable level of risk to privacy nationally and world-wide.” (United
Both reports, at a distance of roughly two years apart, are concerned with the essential elements of human rights, civil liberties, and their deep connection to autonomy, expression, trust, citizenship, rule of law, and the "adequacy" of official oversight. Both reports are also concerned with the intersection of security-rooted measures (surveillance) and the right to privacy. *Liberty and Security in a Changing World* goes so far to identify “two different forms of security: national security and personal privacy” the U.S. government must protect (President’s Review Group on Intelligence and Communications Technologies 2013, 14). The Special Rapporteur's *Report* notes that “the ordinary citizen may often get caught in the cross-fire and his or her personal data and online activities may end up being monitored in the name of national security in a way which is unnecessary, disproportionate and excessive” (United Nations Office of the High Commissioner 2016, para 11); *Liberty and Security in a Changing World* suggests that “when government is engaged in surveillance, it can undermine public trust, and in that sense render its own citizens insecure. Privacy is a central aspect of liberty, and it must be safeguarded” (President’s Review Group on Intelligence and Communications Technologies 2013, 47). In this way, the two reports are a plea to broaden the concept of security so as to encompass the human dimension.

Both reports are also concerned with risk, not only of having one's information gobbled up into a cloud of Big Data, but risks to privacy by targeted
and mass surveillance measures in the protection of state security. Of the
President's Review Group of forty-six recommendations, the most connected to
the Special Rapporteur's Report are:

- The U.S. government “should not be permitted to collect and store all mass,
undigested, non-public personal information about individuals to enable
future queries and data-mining for foreign intelligence purposes”
(Recommendation 4)

- The “government should publicly disclose on a regular basis general data
about National Security Letters, section 215 orders, pen register and trap-
and-trace orders, section 702 orders, and similar orders in programs whose
existence is unclassified, unless the government makes a compelling
demonstration that such disclosures would endanger the national security”
(Recommendation 10).

The President's Review Group recommends adopting a risk management
approach that would serve to reduce risks to national security, as well as those
“risks to privacy, risks to to freedom and civil liberties, on the Internet and
elsewhere” (President’s Review Group on Intelligence and Communications
Technologies 2013, 15). In applying risk management, “the question is not
whether granting the government authority makes us incrementally safer, but
whether the additional safety is worth the sacrifice in terms of individual privacy,
personal liberty, and public trust” (President’s Review Group on Intelligence and
Communications Technologies 2013, 114).

The last word is with the Special Rapporteur's report, which suggests that
protection of privacy is a basic element of the Cyberpeace movement, thus linking
espionage, cyberwarfare, and state surveillance to the invasion of the right to
privacy\(^1\):

---

\(^1\) Cyberpeace, cyber peace, or cyber peacekeeping, is a security-centered concept discussed by
the U.N., U.S. military, and NATO. For example, the 2009 Tallinn Manual on the International

“Cyberspace can truly become a digital space where the citizen can expect both privacy and security, a peaceful space which is not constantly being put in jeopardy by the activities of some States over and above the threats posed by terrorists and organised crime.” (United Nations Office of the High Commissioner 2016, para 11)

References


---
