DISCLOSURE AND ITS DISCONTENTS: PROTECTING PRIVACY IN A TIME OF SURVEILLANCE

Colin Agur (Columbia University)

Colin Agur is one of the eight 2014 Milton Wolf Emerging Scholar Fellows, an accomplished group of doctoral and advanced MA candidates selected to attend the 2014 Milton Wolf Seminar. Their posts highlight the critical themes and on-going debates raised during the 2014 Seminar discussions.

In the 1825 farce play *Paul Pry*, the title character spies on his neighbors by asking third parties for details of their lives and leaving objects (often umbrellas) behind so he has an excuse to return unannounced. His catch-phrase, “I hope I don’t intrude,” is as contrived as his reasons for monitoring his neighbors. In the years following *Paul Pry*, government efforts to read letters in the post and telegrams sent over the wires eclipsed the threat of a bumbling snoop.¹ Today, in the wake of the Snowden disclosures, these concerns seem quaint. With powerful agencies monitoring our electronic communication, ours is a world of frequent and deep intrusions. Nosy neighbors are the least of our worries.

Surveillance was a recurring theme at this year’s Milton Wolf Seminar, held at the Diplomatic Academy in Vienna. In formal sessions and social events spread over three days, the participants — an international mix of scholars and practitioners — explored how, in a time of increasing concerns about privacy and surveillance, diplomats, international organizations, the private sector, civil society, and the press can influence internet governance. The Snowden surveillance disclosures figured prominently in discussions about the capacities and intentions of national governments, and about the degree of privacy enjoyed by ordinary citizens.
For the growing number of people whose lives depend on the internet and global telecommunications infrastructure, the Snowden disclosures raise troubling questions about what sort of “reasonable expectation” citizens can have about privacy when government agencies are willing and able to monitor electronic communication and aggregate that information with other personal data. The uncomfortable truths that Snowden exposed force us to rethink what is and is not private. As Monroe E. Price has written, society is a mix of open and closed terrains of speech. In open terrains, discussion is free and uninhibited. In closed terrains, there are limits on speech. Surveillance means that these closed terrains are more open than we expected. This has prompted attention from scholars and activists who want clear limits on government surveillance.²

One particularly illuminating presentation at the Milton Wolf Seminar focused on the evolution of “privacy panics” from the 19th century — when citizens worried that British authorities were reading their mail and telegrams — to the present day. The historical lessons are worrying: consumers want convenience above all else, and many are willing to accept surveillance so long as it does not interfere with the ease of communication. In the 19th century, despite revelations of postal mail surveillance, more people sent more letters through the post. Today, polls show that many people are concerned about telephone and internet surveillance. At the same time, these tools offer enormous convenience and few users are willing to invest the time and effort necessary to encrypt their communications. If history is a guide, current outrage about mass surveillance will wane and many users will accept a loss of privacy in exchange for convenience. Given the aggregating power of current and emerging surveillance technology, we should be worried. When we give up aspects of our privacy, we rarely get that privacy back.

Of course, it is not just governments who have access to our data. When we sign up for a Gmail account, we allow Google to read messages we send as well as messages sent to us by others. Google is able to read those messages, regardless of whether those message senders provide their consent. For those concerned about Google storing and studying their email contents in conjunction with other user information (for example, web searches performed while the user is signed into a Gmail account), the answer is straightforward: use another email service. But we do not always have that choice. Many institutions have outsourced their email to Google, meaning that the internal correspondence of many universities, including the one where I am pursuing my PhD, is stored on servers in Mountain View, California. When an outsider emails a faculty member or student at Columbia, s/he may be unaware that the university’s email and all messages (incoming or outgoing) are subject to Google terms of use. Here we see the challenge of web-based services that offer us benefits in exchange for using our data. As one Milton Wolf Seminar participant stated: “We want the convenience of these services, but we also want to put the genie back in the bottle. How do we do both?”
This year’s seminar made a point of focusing on the future, on solutions for better governance of global communication networks. I see three aspects of surveillance that deserve our attention: laws, design, and practices.

The first is law. At the domestic level, there are major technical challenges. Surveillance technology is inescapably global; and the United States plays an outsize role. When surveillance activities cross borders, there is only so much that law enforcement can do. Another challenge is judicial. There are prior cases that touch on metadata. In the United States, for example, *Smith v. Maryland* (1979) set the precedent that telephone users cannot expect that the numbers they dial will remain private. Judges, however, have interpreted that case in different ways; and it is unclear how the Supreme Court would rule in a case on telephone metadata. While the NSA has sought to portray its actions as targeted efforts that isolate specific users, experts have suggested that the collection of “metadata” is a form of mass surveillance. In the US, there is a long history of government agencies finding ways around privacy laws and attempting to downplay the scale and significance of the data being collected. Internationally, the challenges are even greater than at the domestic level. Given the power disparity between the surveillance-haves and have-nots and the different attitudes national governments have toward binding treaties, it will be difficult to craft a meaningful and enforceable set of laws governing surveillance technology.

A second aspect of surveillance is design. It is important to promote laws that clarify what surveillance agencies can and cannot do with data and clearly outline the relationship between these agencies and internet and telecommunications firms. Good laws, however, are not enough. If communication networks are designed in such a way that it is possible for law enforcement and spy agencies to collect, store and use data—they will do so. In recent years, advocates of “Privacy by Design” have developed a core set of seven foundational principles for prioritizing privacy in the design of large technical systems:

1. Make design proactive not reactive and preventative not remedial;
2. Make privacy the default setting;
3. Embed privacy into design;
4. Avoid zero-sum dichotomies such as “privacy vs. security;
5. Emphasize end-to-end security;
6. Provide transparency on the design process; and
7. Keep design user-centric.

While these principles are laudable, they often exist in tension with the business models of network enterprises, whose profitability stems from their ability to aggregate users, services, and data. Privacy-by-design thus faces a central challenge—many of the institutions we would most like to see implement these principles have a financial disincentive to do so.
While law and design are important, a third aspect of surveillance—practices—ultimately determines the degree of privacy enjoyed by users. At several points during the Milton Wolf Seminar sessions, participants highlighted the ability of major players (especially internet and telephone service providers) to pursue practices that privilege users over mass surveillance. To be fair, major players face a delicate balancing act. Their business model depends on the trust of millions of users and support from government officials. In the months since the Snowden disclosures, big tech firms have struggled to answer criticisms regarding their complicity with surveillance programs. The question for internet and telephone service providers and social media giants is: How can they develop practices that strike a balance between national security and individual privacy? A large part of the answer involves empowering users to understand how their data is used and how to encrypt their communications.

In all three of these aspects of surveillance—law, design and practice—the mobile telephone should receive the greatest attention. The telephone has a long history as a tool of surveillance. Today, it is a more important tool than ever. A telephone is no longer just a fixed-line medium of communication. For a large and growing number of users, it is a mobile device that conveniently aggregates several different (and previously separate) forms of data. This data aggregation function—which users find so convenient—also allows institutions to track users’ location, monitor their phone usage, and access content on devices. As we think about the changing physics of search and seizure, the behavior of government institutions at home and abroad, and the evolving set of “reasonable expectations” that pertain to contemporary privacy, the telephone should have a significant place in our thinking.

In each of these aspects of privacy, good journalistic reporting is crucial. As more than one participant in Vienna pointed out, news organizations should not be intimidated by government requests to circumscribe coverage of surveillance issues. The existence of “honorable secrecy” between government officials and journalists does a disservice to democracy and to the rights of citizens. In the face of government pressure, news organizations need to develop and encourage best practices in the protection of data and sources.

As we think about surveillance in a changing technological context, informed and vigilant users are perhaps the actors who can make the greatest difference. In our communications laws and treaties, there is an implicit social contract: we accede power to the state and large corporations in exchange for the implicit promise that these institutions will respect our private lives. The surveillance we are learning about today is extensive, sophisticated, and unclear in its legality. By understanding terms of service and taking steps to protect correspondence and other data, we can have some control over how this information is used.
References


2 See the extensive set of articles at the Electronic Frontier Foundation. Available at: https://www.eff.org/nsa-spying. Also see The Guardian’s collection of articles. Available at: http://www.theguardian.com/world/the-nsa-files.


Colin Agur is a PhD candidate in Communications at Columbia University’s Graduate School of Journalism. His dissertation focuses on cultural and sociological aspects of mobile phone use in India. His research involves examination of policy documents (1991-present), interviews of policymakers, telecom executives and users, and observation of mobile phone use across India.

At Columbia, he developed and taught a course (“Mobile Revolutions: Markets, Politics, Journalism”) that explored contemporary issues related to the mobile phone.

Since 2011, he has been a Visiting Fellow at Yale Law School’s Information Society Project. His work there has focused on telephone surveillance and the Fourth Amendment. Twitter: @colinagur

Featured Photo Credit: Some rights reserved by jeffschuler