Privacy in public

Avner Levin

"Always eyes watching you… Asleep or awake, indoors or out of doors, in the bath or bed—no escape. Nothing was your own except the few cubic centimeters in your skull."

—*George Orwell*, 1984

This dystopian vision, written almost 60 years ago about a future predicted for a time that is now over 30 years in the past, is closer than it has ever been to becoming a reality. Even mind-reading technology is currently being developed and refined, leading us to an even-more dystopian reality in which our physical bodies will become vessels of surveillance. Überveillance, (omnipresent surveillance) will of course mean the end of privacy as we know it and as we have grown to value it. If we wish to have privacy in the future, we must embark on several courses of action in the present before, as a society, we are too late.

Technology and its unintended consequences

The likelihood of überveillance has increased due to a number of recent technological developments. First, there is a rapidly increasing number of information-capturing devices that are either used or to which we are exposed. One such device, for example, is the camera, which primarily captures visual information that can then be used to identify and locate individuals. Cameras can now be found on phones, which are in turn ubiquitous. Cameras can also be found in closed-circuit television systems, which are installed in increasing numbers to oversee public and semi-public spaces, such as city squares and commercial malls. Cameras can now be body-worn by law enforcement officials and are found on drones (unmanned aerial vehicles), which are in use by governments and increasingly by corporations and individuals for a variety of interests.

As a result, there has been an enormous increase in the overall number of cameras in the public and semi-public sphere, which has led to a corresponding increase in the number of public images available for government, corporations, and individuals to use to identify, locate, and track individuals as they move throughout public spaces. Imagine this ability multiplied by the information-capturing abilities of other real-world devices, such as motion sensors, smart doors, and global positioning systems (GPSs), and you will begin to understand the future of omnipresent surveillance.

A second technological development that has created additional sources of personal information has been social media. Social media

Digital Object Identifier 10.1109/MPOT.2016.2569726
Date of publication: 8 September 2016

0278-6648/16©2016IEEE

corporations profit from the sharing of personal information and continuously encourage individuals to increase the amount of information that they share. Individuals routinely share the minutia of their lives in the form of photographs, messages, and audio-video files. All of this information is parsed by corporations for its commercial value. The emphasis on sharing and socializing at the expense of privacy and seclusion has also turned formerly simple social transactions, such as the purchase of a cab ride or the rental of a hotel room, into complicated, information-rich transactions in which financial information is retained by social media corporations. Personal information is then generated in the forms of ratings and rankings of both the service provider and the service user, personal information without which such transactions cannot be carried out.

As more members of society socialize online, social media itself has become a public forum and a public, or at the very least semi-public, space. Information generated on social media, therefore, is a form of information about individuals that is available in public and that contributes to the monitoring, tracking, and surveillance of individuals for commercial and governmental purposes. The two technological developments described so far—the creation of more information about individuals through new real-world devices and through new online media—enable surveillance in both the real and digital realms. Whether government or corporate, the surveillant is omnipresent.

Our understanding of a potentially dystopian future is incomplete without considering another recent technological development—the increase in computational power and sophistication of algorithms, colloquially known as the rise of big data analytics. It is this further development that provides government and corporations with the tools that "make sense" of the increasing amount of personal data captured by cameras and other sensors, and generated online, and to compile information from a variety of seemingly discrete sources to create a "mosaic" about individuals.

The meaning of privacy in public

To preserve privacy in this near-present, dystopian future, we must first better understand what the term *privacy* means and what values it serves. A notoriously vague idea, privacy takes on different meanings in different contexts. For adolescents online, protecting their privacy mostly means protecting their ability to develop their personal identity. For Americans, protecting privacy mostly relates to protecting their freedom from government—their liberty. And for Europeans, privacy equates to dignity, reputation, and social standing.

These basic values served by privacy—of liberty, dignity, and autonomy—do not disappear in public. The idea of privacy in public is not an oxymoron. These values have been served, until now, by the related concepts of anonymity (in the real world) and by the principles of information protection (online). However, in light of the coming omnipresent surveillance, anonymity and online information protection need to be enhanced both legally and technologically.

It must be said that the existing legal framework has already offered some protection for privacy in public. For example, the Canadian equivalent of the American Fourth Amendment, Section 8 of the Charter of Rights and Freedoms, states that "Everyone has the right to be secure against unreasonable search or seizure." Unlike the Fourth Amendment, Section 8 is not limited to certain locations or artifacts, and it revolves solely around the notion of reasonableness, which potentially could evolve to counter technological developments. As early as 1998, the Canadian Supreme Court decided that a woman photographed outside her house on her front steps had a right to privacy, dignity, and autonomy that translated into a right to receive compensation when her photograph was published in a magazine without her permission and against her wishes.

The principles of information (data) protection have also been utilized in Canada, Europe, and around the world to offer individuals some measure of control over the use of their personal information and its processing for commercial purposes. The traditional cornerstones of the information protection regime have been the closely connected ideas of notification and consent. Individuals must be, at the very least, notified about the ways in which their personal information is collected and the purposes for which it is used, and individuals should ideally consent (agree) to this usage.

If we wish to have privacy in the future, we must embark on several courses of action in the present before, as a society, we are too late.

Notification and, in particular, consent have been under added strain to offer meaningful protection to individuals in this era of an increasingly information-based economy, continuous, long-term commercial relationships between individuals and businesses, and the ability to extract commercial value from mundane personal trivia. The consent "regime" is viewed as offering protection not to individuals but to corporations, protecting them from liability for their information use through notorious mechanisms of "click-wrap" agreements, terms of use, and privacy policies that are neither read nor meaningfully accepted by the multitude of individuals that click "I accept" to download or access the latest version of their favorite digital service or application.

The mosaic theory of privacy

Legally, a framework needs to be created to prevent and constrain the

big data analysis that turns separate pieces of information into a rich tapestry. One such framework is the mosaic theory of privacy. The main point that the mosaic theory makes is that the law should adapt and evolve to offer protection from surveillance to individuals on the basis of the totality of information collected about them, rather than limit the evaluation of whether legal protection should be offered to discrete instances of surveillance.

Legally, a framework needs to be created to prevent and constrain the big data analysis that turns separate pieces of information into a rich tapestry.

For example, a police officer may observe a person at an intersection uptown early in the morning, and another police officer may observe the same person at an intersection downtown around noon. A third officer may happen to observe that person enter a residence in the evening. Each act of observation may not trigger legal protection on its own—after all, each time the person was in a public location and seen by many others. However, the totality of these observations, including the technological ability to combine and analyze them, creates a mosaic from which the police can determine the whereabouts of that individual throughout the day that they could only have otherwise obtained by actively tracking that individual. The mosaic theory argues that since that "old-fashioned" manner of surveillance would have required legal (judicial, in many cases) authorization, so does the new manner of technologically enabled surveillance.

That, in fact, was the conclusion of the United States Supreme Court when it was asked to determine the constitutionality of placing a GPS on a vehicle and then tracking the vehicle's location for a month. The police argued that the surveillance was acceptable and did not require judicial preapproval since the vehicle was in public spaces at all times. The court, however, disagreed on the basis (at least partially) of the mosaic theory.

The mosaic theory applies not only to real-world surveillance but to online information collection and tracking as well. Cellular phone owners are familiar, by now, with the manner in which over a few days their device learns to associate its location at various points of time with familiar labels, such as "home" (for the overnight location) and "work" (for the nine-to-five location). This commercial act of surveillance similar in every significant aspect to the GPS-location-tracking attempted by the police against Mr. Jones. It, too, should be curtailed by the mosaic theory of privacy.

Many individuals find it easier to accept commercial surveillance of their activities, since they appear to receive tangible benefits in return in the form of free social media services or information relevant to them. Government surveillance encounters more resistance since its benefits ("safety and security") are not as immediate and specific. The notice- and consent-based information protection regime has facilitated this acceptance by enabling multiple uses and disclosures of personal information on the basis of one initial interaction between individual and business.

In line with the mosaic theory and the significance it places on the mosaic of information over the individual data-"stones" that comprise it, a revised set of information protection principles would constrain not only the initial collection of information but place restrictions upon the repeated use and disclosure of information as well. It is this repeated use that allows corporations to create ever-more-detailed profiles (i.e., mosaics) of their users for commercial purposes. One version of such principles, *Data Protection Principles for the 21st Century*, has been suggested by the Oxford Internet Institute.

Technological solutions for unintended consequences

A mosaic theory, and revised information protection principles, could prove to be valuable legal tools, but they most likely will offer insufficient protection if they only create judicial- and complaint-based remedies for individuals to pursue. We must seek technological-based solutions and tools for the privacy concerns raised previously that will not be based on the judicial activism of a few privacy advocates but rather on the patterns of technology use of society.

A good example of such a solution can be found in the European Court's decision against Google, ordering the company to remove search results that were in violation of a Spanish individual's privacy. The significance of that decision is not only in the results of one course of litigation by one determined individual but in the online interface that Google has had to create, begrudgingly, for individuals in Europe that would allow people to apply for the removal of their personal information online, freely and without the need for costly litigation. Hundreds of thousands of such requests have already been filed.

Other technological measures for the protection of privacy are already available as well. Encryption protects the security of information and the privacy of its users, as is evident from the dispute between major technological corporations (such as Apple, Google, and Facebook) and the American government over the elimination of "backdoors" to their encryption systems. Anonymity is increasingly a feature of social media apps, not always in a manner welcomed by society (think Whisper, Secret, and Yik Yak) but demonstrating that it is possible to limit and control the generation of personal information

online. Drones and other devices based on GPSs and location can be bound and limited by geo-fencing—limiting through software the ability of the drone to leave a certain area (such as a park) or to enter certain areas (such as a residential area or the airspace above the White House).

The widespread adoption of such technological measures would be important and significant as a direct response to increasing surveillance and equally as means to combat the erosion of privacy and anonymity as social norms. Technology can shape expectations and norms around privacy and the reasonableness of commercial and governmental surveillance both negatively and positively, and we cannot expect to win the battle over privacy in public and privacy in general through legal means alone.

Conclusion

Are we hurtling toward a future in which we fritter our anonymity and privacy away, in which we sell our dignity and liberty for commercial goods and the promises of a political leadership to keep us safe and secure? Do we take our basic freedoms for granted? Is our future one of omnipresent surveillance, both corporate and governmental, that is "not only 'always on' but also 'always with you'"? Are we destined to a dystopia that would be the combination of *1984* and *Brave New World* wrapped into one? Will this future be the unintended consequence of technologies that aim to connect us, allow us to socialize, and provide us with the ability to make instantaneous informed decisions?

Social media, drones, and ubiquitous cameras and sensors, supported by big data analytics, are rapidly transforming our privacy in public. The increasing availability of personal information, and our increasing ability to analyze this information, are leading us to a society where we will no longer be anonymous when we step outside our doors. This loss of anonymity will subject us to omnipresent surveillance by governments as well as by corporate giants, such as Facebook, Google, and Apple. Our current legal frameworks are increasingly ineffective, and the values of liberty and dignity, served by privacy, will irreparably erode.

Laws by themselves will not work; we must incorporate privacy and anonymity as a feature of emerging technologies and ensure that our societal norms are supported by technology and not undermined.

We can only reverse this worrisome trend and preserve anonymity, and therefore some measure of privacy in public, if we initiate legal and regulatory changes that emphasize restrictions on data use and recognize that surveillance is the product of many seemingly innocuous acts of information collection and processing, and that these acts must be curtailed to prevent the emergence of rich mosaics and tapestries that expose the private lives of individuals irreversibly. Laws by themselves will not work; we must incorporate privacy and anonymity as a feature of emerging technologies and ensure that our societal norms are supported by technology and not undermined.

In *Brave New World*, Aldous Huxley wrote, "Most human beings have an almost infinite capacity for taking things for granted." Let us hope our privacy, anonymity, liberty, and dignity are not among such things.

Read more about it

- G. Orwell, 1984. London, UK: Harvill Secker, 1949.
- M. G. Michael and K. Michael, "Toward a state of überveillance," *IEEE Technol. Soc. Mag.*, vol. 29, no. 2, pp. 9–16, June 2010.
- The Canadian Charter of Rights and Freedoms. (1982). [Online]. Available: http://laws-lois.justice.gc.ca/eng/const/page-15.html
- *Aubry v. Éditions Vice-Versa*. 1 S.C.R. 591. (1998). [Online]. Available: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1608/index.do
- O. Kerr, "The mosaic theory of the Fourth Amendment," *Michigan Law Rev*, vol. 111, no. 3, pp. 311–354, 2012.
- *United States v. Jones. 565 U.S.* (2012). [Online]. Available: http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf
- F. H. Cate, P. Cullen, and V. Mayer-Schönberger, *Data Protection Principles for the 21st Century*. Redmond, WA: Microsoft Corp., 2013.
- Google v. Gonzalez. ECLI:EU:C.2014:317. (2014). Available: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=667631
- M. G. Michael and K. Michael, "A note on überveillance," in *The Second Workshop on the Social Implications of National Security: From Dataveillance to Überveillance and the Realpolitik of the Transparent Society*, Katina Michael and MG Michael, Eds. Wollongong: Univ. Wollongong, 2007.
- A. Huxley, *Brave New World*. London, UK: Chatto & Windus, 1932.

About the author

Avner Levin (avner.levin@ryerson.ca) is a professor in the Department of Law and Business, Ted Roger School of Management, Ryerson University, Toronto, Canada.