Does Post-9/11 Equal Post-Privacy?

by Shelly Warwick

Editor's Summary

The terrorist events of September 11, 2001, are commonly seen as a turning point, with security concerns justifying sacrificing a degree of privacy, but the tension between personal privacy and government need is longstanding. While the Supreme Court established the notion of a reasonable expectation of privacy, later legislation chipped away at it, from the Digital Telephone Act of 1994 to the PATRIOT Act of 2001. Under the guise of combating terrorism, the PATRIOT Act authorizes increasing levels of intrusion and data gathering, enabled by continuing technology advances, data aggregation and people living their lives intertwined with the Internet. We are left with little reasonable expectation of privacy and a diminishing right to be left alone. Yet while individuals cannot count on personal privacy, the government engages in secretive information gathering on a massive scale. One may wonder whether privacy is an outdated concept and ask if we are more secure for giving it up.

Keywords

privacy
personal information
government
public policy

It is popular to view 9/11 as a sort of singularity for privacy – a watershed moment when concerns about security trumped privacy. This point of view has been bolstered by the various laws, procedures and practices that have emerged since 9/11 which, if not curtailing privacy, have lowered the level of evidence needed for various government agencies to access personal data.

The tension between individual desires for personal privacy and the need of governments for detailed knowledge for the greater good is nothing new. Since the Doomsday Book governments have collected a plethora of information about each of us for tax purposes – starting with extent and value of land owned to number of people supported, how much we earn, if we buy a house or a car, if we earn capital gains or experience a business loss. Marriages require blood tests and licenses. Businesses, even unincorporated, require registration. Colleges and universities need to be accredited and meet reporting requirements to participate in programs funded by the government. Many professions require licensing as do certain types of businesses. While many of these data collection mandates act to protect the public interest (who would want to go to a doctor that didn’t meet the requirements for a license or eat in a restaurant that failed the public health inspection?) in a world where data is stored on computers the sum is greater than the parts.

Prior to 1967 wiretaps without warrants were constitutional based on Olmstead v. the United States, which was overturned with Katz v. United States in which Justice Marshall stated in a concurring opinion that “[m]y understanding of the rule that has emerged from prior judicial decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy; and second, that the expectation be one that society is prepared to recognize as reasonable.” This two-prong test has become the standard for judicial review in privacy issues. Here, I argue that as this “reasonable expectation” has eroded so has our privacy.

Even before 9/11, communications companies were required under the
encryption standard FIPS 185, 59 FR 5997 to use only technology that can be decrypted by the government, and the Digital Telephony Act required that those companies provide assistance to the FBI in securing data and use only technologies that can be tapped, including pen register data on all phone calls. There was a huge outcry by those concerned with privacy, and it took three different legislative sessions for the Digital Telephony Act to pass. Some of the provisions that were stripped from the originally proposed Digital Telephony Act were later incorporated into the Patriot Act.

An interesting aspect of the Patriot Act is how fast it was drafted and passed. In a Congress that normally takes months, if not years, to move legislation from committees to a floor vote and then from one house to another, usually resolving differences via conference, H.R. 3162 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, moved through eight committees on October 23, 2001, passed in the House on October 24th, passed in the Senate on October 25th, and was signed into law on October 26th. The timetable alone indicates that the elected legislators were unable to properly consider the provisions of the 342-page law. It is also obvious that such a lengthy and detailed document could not have been drafted in the approximately six weeks between September 11 and October 23 unless there were already drafts of many of the provisions existing as wish lists on the desks of security and oversight agencies. It is ironic to note that it took 10 years to pass the James Zadroga 9/11 Health and Compensation Act, which expanded the compensation to individuals or their families who suffered physical harm or were killed as a result of the terrorist-related aircraft crashes of September 11, 2001, or the debris removal efforts that took place in the immediate aftermath of those crashes. Most of the money allocated has yet to be distributed.

The Patriot Act provided the federal government a wide array of greater powers to combat terrorism, from increasing the type of data collected by and from financial institutions to permitting wiretaps based on a lower level of evidence and gag orders on those who were the subject of search warrants issued for national security (including libraries). Beyond the Patriot Act, however, an array of intrusive inconveniences has arisen, from body scans and shoe removal at airports to providing identifying information for formerly anonymous cash transactions, such as short interstate bus rides. The need to show some form of identification to enter almost any large office – and many university – buildings has become de rigor, and metal detectors and security screening at large gatherings is the new normal. Even some smaller venues require a search of carried items.

There are also laws requiring greater tracking and data gathering for international students and a need to show a passport between the United States and Canada. Beyond these and other generally publicized and publicly enacted laws and measures is the recent revelation that the U.S. government has used the Patriot Act to demand that telecommunications companies provide the National Security Administration (NSA) with calling data on all customers. The NSA has been monitoring the calling and Internet usage of hundreds of thousands of American citizens who have not been shown or even suspected as having any connection to terrorism.

It is easy to blame all this activity on 9/11, but we should also consider other contributing factors. What is done is limited by what can be done. The years since 9/11 correspond with a great expansion of computer speeds, network capabilities, Internet hosting and social networks, nearly making it possible for security agencies to do what one assumes they’ve always wanted to do – to know everything about everyone. The ability to learn about the behavior of individuals has also been greatly enhanced by the fact that many people now essentially live their lives online, posting GPS location, who they are with, what they are doing and pictures of everything from cats to sexual acts. Life has seemingly been reduced to a photo-op interspersed with instant messaging and tweets.

In addition to the collection of personal information by government agencies or that mandated of companies by law, there has been an increase
in the amount of data about individuals gathered by commercial groups. People are increasingly being offered free access to services or goods in exchange for information. Many of those pieces of information are themselves innocuous, but when aggregated with information from other sources may become intrusive. Many websites that collect information in exchange for access also use tracking software like DoubleClick to record such information as websites visited or search terms used. If we are what we search, marketers know us intimately.

Given all the information we know is collected about us, do we have any reasonable expectation of privacy? Perhaps not. However the type of privacy addressed in Katz might be referred to as data privacy, the right to keep information from others. There is also another type of privacy defined by another Supreme Court justice, Louis Brandeis, as “the right to be left alone.” While in some respects this right is supported by laws, such as those that created no-call lists, it is also challenged by the provisions of the Patriot Act that have legalized no-knock warrants and allow searches of homes and offices without informing the person who is the target of the search. Parallel to these developments is a more in-your-face culture where people talk loudly on cellphones in almost all settings and where refusing to interact with someone is seen as disrespectful and can lead to confrontation. I live in New York City, and four out of five mornings my quiet reading time during my 20-minute subway ride is abolished by performers (break dancers, mariachi bands, drummers, singers, poets) or religious zealots, many with amplification devices, who feel entitled to intrude. They certainly don’t recognize my right to be left alone. However, while construction of what is acceptable for individuals to do in public space appears to have expanded, there have been contractions of the rights of groups in public space. Pick a political gathering and see where the protestors are allowed to be and how police treat them. Likewise, meeting with more than 25 people in a New York City park requires a permit. Not only have we lost the reasonable expectation of data privacy, but also the expectation of the right to be left alone and the right to peacefully assemble.

Perhaps the question to ask is, “What is the harm in the loss of privacy?” Am I just a “so 20th century” old lady? When people lived in small villages everyone knew everything about their neighbors, saw their comings and goings and with whom they associated. Rituals and performances were done in the middle of the settlement without asking who may want to go to bed early. Maybe we should adjust to living in the global village. As has been observed regarding restraining freedom of speech, “the remedy is more speech, not enforced silence.” Perhaps the remedy for information is more information. If there are no secrets no one can be blackmailed. Perhaps privacy is an outmoded concept. Perhaps all information should live in the sunshine.

Oh, but wait. Bradley/Chelsea Manning has been convicted because he provided government information to Wikileaks, and Edward Snowden is being branded a traitor for revealing the NSA phone information-gathering program. So the government has a reasonable expectation of privacy while individuals don’t? Is the change in the privacy rubric a herald of a change of the relationship between citizens and government in democracy? While there have been claims that the powers granted to the government since 9/11 have enabled other terrorist attacks to be prevented, there is no hard data. We are told to trust that the government is only collecting data to protect us. And that if we’re not guilty, not to worry. We’re slowly moving to a world where every individual’s actions and utterances are scrutinized while the government’s actions are behind a firewall and where those that question the constitutionality of the government’s actions become outlaws.

I certainly understand the impact of terrorism (I live a mile and quarter from Ground Zero, and one of my neighbors died when the planes hit), but wonder if the privacy that we have surrendered makes me or any of us more secure?

A few months ago I suggested to one of my nieces that saving her passwords on her mobile phone, which could be easily lost, was not the best method to secure her privacy. Her response was, “Only old people like you care about privacy.” Maybe my niece has the right attitude, accepting that we live in a world where there is no guarantee of privacy and to live expecting everything about you to be publicly available, in fact aiding in making it publicly available yourself.

I would be happy if I thought all the shoes taken off, all the one-quart bags of toiletries removed from carry-on bags, all the driver’s licenses shown to buy bus tickets and all of NSA data collection has made us safer, but I doubt that it has.