THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
September 2011 • Volume 11 • Number 7

How 9/11 changed privacy

By Mathew J. Schwartz

On the tenth anniversary of Sept. 11, The Privacy Advisor *looks back on how the events of that day changed privacy.*

How did the events of September 11, 2001, change privacy? To answer that question, it helps to identify just how much privacy has evolved over the past decade. In that timeframe, "you have the growth globally of an interest in privacy—including consumer privacy—and that's reflected in many ways," said Jim Dempsey, vice president for public policy at the Center for Democracy & Technology (CDT), a civil liberties group based in Washington, DC. "The fact now that there is a career track called privacy, and all the major corporations now in the United States have privacy officers, and there is this global community of privacy professionals, is remarkable."

Indeed, privacy is today part of the business, consumer and legislative lexicon. Numerous companies now employ chief privacy officers who guide their data privacy efforts. On the consumer front, the widespread buying and trading of people's personal information has also led to legislative attempts to secure people privacy rights. In Europe, the "right to be forgotten" seeks to counterbalance privacy in an index-everything world.

Of course, the past decade has also featured the rise of more Internet-savvy government surveillance systems. According to Dempsey, "the most important change in privacy has been certainly the rise of the national security state" or what some now call the industrial surveillance complex in a digital allusion to President Eisenhower's 1961 warning about the emergence of the "military-industrial complex."

People Demand Data Protection

In the wake of such realities, perhaps it's not surprising that more people now demand that their personal information be secured.

"There has been a perceptible shift now in understanding why the protection of personal information is important. We've seen it in the United States, Central and South America and Europe. It's hardly controversial to say that now," said Richard Thomas, London-based global strategy advisor for the Hunton & Williams think tank the Centre for Information Policy Leadership.

But from 2002 to 2009, when he served as information commissioner for the United Kingdom—with responsibilities that included regulatory powers under the country's Freedom of Information Act of 2000 and the Data Protection Act of 1998—the privacy story was largely different.

"When I started as commissioner in 2002, the subject was seen as a little technical, a little dry, perhaps a little theological," said Thomas.

Likewise, back then, UK residents ranked data protection as their number-four social concern. But by 2009, people reported that data protection concerned them more than healthcare, education or the economy and was second only to crime.

Data Breaches Break Consumer Trust

That rise in data protection awareness was no doubt driven by the explosion in data breach disclosures.

"There was a step change in this country when the government had to confess to losing 25 million child benefit [recipient] records," said Thomas.

That 2007 incident, as well as many other high-profile data losses, for example by the UK Ministry of Defense, helped awaken people to the issue in Britain.

Similar disclosure laws and results in North America and Europe have likewise boosted awareness. For example, in the United States, California's SB 1386 privacy law mandated data breach disclosures, inaugurating regulations that may eventually apply in all 50 states and highlighting the extent to which people's personal data was being bought and sold, as well as lost and stolen.

What Sept. 11 Hath Wrought

How the Patriot Act affected privacy

By Peter Swire, CIPP

Just six weeks after the attacks of September 11, 2001, Congress passed the USA PATRIOT Act. The Patriot Act has become the symbol of all the privacy changes after 9/11, but its actual provisions were only part of those changes.

Some parts of the act were already being considered before 9/11 due to technological changes. For instance, some language in the wiretapping laws referred to hardware "devices" but didn't seem to apply to software. Also, as people began using more ways to communicate—mobile phones, Blackberries and so on—it made sense to allow "roving" wiretaps on a suspect and not require a separate court order for each telephone number.

Perhaps the biggest privacy changes concerned the Foreign Intelligence Surveillance Act (FISA). Since that law's passage in 1978, there had been a "wall" between law enforcement and foreign intelligence investigations, with strict rules that governed how foreign intelligence wiretaps could be used for criminal prosecutions. The Patriot Act made a simple but important change. Previously, foreign intelligence had to be "the" reason for the wiretap; after the Patriot Act, it only had to be "a significant purpose," and domestic law enforcement purposes could generally be served by the same wiretap.

Another change to FISA concerned National Security Letters (NSLs). These were rarely used before 2001 and were allowed only for counterintelligence purposes. Their use exploded after the Patriot Act, however, giving the government access to records about finances, e-mails, and telephone records. The Patriot Act contained a "gag rule," later held unconstitutional, that prohibited the record holder from disclosing that the records had been accessed. A 2007 report by the Justice Department Inspector General found "widespread and serious abuse of the FBI's national security letter authorities," and NSLs have operated since then under significantly stricter rules.

The Patriot Act contained quite a few other provisions that affected privacy, such as: (1) government access to more financial records to fight money laundering; (2) the open-ended language in section 215 about government access to business records; (3) authorization for "sneak and peek" warrants, which allow law enforcement to enter the premises first and give notice only later, and (4) computer trespasser rules, which in some instances allow the government to access computer systems without a court order in order to try to catch computer hackers.

The 2001 statute thus certainly made important changes to U.S. privacy law. The Patriot Act, however, became a symbol of thebroader changes wrought by what the administration called the "Global War on Terrorism." After 9/11, the National Security Agency began warrantless wiretaps under its Terrorism Surveillance Program. The Pentagon considered the controversial Total Information Awareness program, designed to provide the military with unprecedented access to data about individuals. In 2002, Congress created the Department of Homeland Security, a new cabinet agency with more than 200,000 employees, organized around the mission of protecting the homeland.

These other initiatives were not part of the Patriot Act, as enacted in October 2001. But the name of the "Patriot Act" became a symbol of the broader changes in privacy after the attacks of 9/11.

Peter Swire, CIPP, is the C. William O'Neill Professor of Law at the Ohio State University.From 1999 to early 2001 he served as the Clinton Administration's Chief Counselor for Privacy.

Without a doubt, notions of data privacy have changed dramatically over the past decade. But was Sept. 11 the catalyst for that change? "I do not think that 9/11 has been a major factor in that," said Thomas. Rather, he said, it's been driven by the "growth in technology"—the spread of the Internet and e-mail, the ubiquity of computing and the reduced cost of both storage and computing power.

But governments' responses to Sept. 11 arguably did have an impact on people's privacy.

"We're worse off in terms of our privacy from government, thanks to the 9/11 attacks," said Jim Harper, director of information policy studies for The Cato Institute—a Washington-based think tank—as well as a founding member of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

According to Harper, who recently co-edited the book *Terrorizing Ourselves: How U.S. Counterterrorism Policy Is Failing and How to Fix It*, "9/11 launched a thousand security ships that have serious, negative privacy consequences, and most of those ships don't have a destination, meaning they don't actually improve security commensurate with the their cost—or value."

Take the rise of the Transportation Security Administration, warrantless wiretaps and the Western Hemisphere Travel Initiative—or the Real ID national identity card movement. "Security benefit? Slim to none. Cost: billions of dollars," he said. "And the privacy costs are huge, and the consequences for society are huge. If you're creating a society where IDs can be checked easily, then they will be."

Government Surveillance and Civil Liberties

Interestingly, however, according to CDT's Dempsey, these government initiatives, or at least their predecessors, didn't begin after Sep. 11.

"My own view, and it may be a minority one, is that 9/11 accelerated trends, and bent the curve, but did not generate anything new," he said.

For example, no-fly lists, metal detectors and x-ray machines already featured at airports. Reviewing airline passenger manifests prior to departure improved on doing it after they landed. Meanwhile, warrantless wiretapping meant no longer having to use submarines to eavesdrop on ocean-bottom submarine communications cables after fiber optic cables began routing much of the world's IP traffic—some of it generated by U.S. citizens, some of it not—through the United States.

While any of these types of activities could adversely impact people's privacy, unless carefully managed, they didn't appear suddenly after Sept. 11.

"Some of our specific rules may have changed, but our fundamental principles have remained the same," said Alexander W. Joel, CIPP/G, the civil liberties protection officer for the Office of the Director of National Intelligence (ODNI), which was created in response to the events of Sept. 11 to lead and integrate the 16 groups that comprise the U.S. intelligence community.

Privacy inevitably involves tradeoffs—with security or even just convenience. The question is, have those tradeoffs been made correctly? "Looking back, I believe that this civil liberties protection infrastructure has been working as intended, focused on maintaining the balance between pursuing national security missions and protecting civil liberties and privacy," said Joel. "It's not perfect, of course—there is always room for improvement. But having been in this job for the past six years, I have seen firsthand how the intelligence leaders and operators I advise understand that in order to have the authorities and tools the government needs to keep the country safe,

we must have the trust of the people, and we can only have that trust if we follow the rules and protect people's privacy."

Looking Ahead: Privacy 2021

People love to point the privacy finger at the government, but one interesting change has been what CDT's Dempsey calls "the democratization of surveillance." For example, millions of people now willingly use and carry devices that record and share not just voice and data but also images. "They can take a photograph, geotag and timestamp it, upload it to the Internet instantaneously—and share it widely—and it can be facially recognized and searched, and so on," he said.

How should this consumer-generated information, which could easily be used in ways that impact other people's privacy, be treated? While data privacy rules already exist for businesses and government, there's little in case law about "surveillance by the masses," said Dempsey. "It's a development we've barely begun to grapple with."

Ten years after Sept. 11, don't expect the privacy changes to stop.

Mathew Schwartz *reports on information security and privacy issues for* InformationWeek *and* The Privacy Advisor.