TIP JAR

Does Anyone Really Expect Privacy?

Winter 2018
Issue 3

A small drone flies 350 feet above ground through the beautiful rust-colored mountains. A dusty road flows around the mountainside and opens up to a plateau of rock and sand. There sits a cluster of large industrial buildings, caked with red mountain dust. The buildings cover approximately a million square feet, the size of three football fields in each direction. The facility is shielded from the road by 10-foot concrete walls and a checkpoint with guards, dogs and guns.

Inside, the buildings hum with the whir of supercomputers that store gargantuan amounts of data, including emails, phone calls, Google searches and electronic communications from around the world. The machines download data at the rate of 20 terabytes—the equivalent of the entire Library of Congress—every minute. Is this a delusional conspiracy theory? A dark fantasy? An imagined dystopian future? This is the National Security Agency's $1.5 billion Utah Data Center, located in Bluffdale, Utah, the first place the government goes to search for terrorists, foreign and domestic.

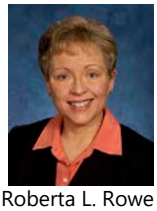
While our government hunts terrorists around the world, another battle rages within U.S. borders: The conflict between our government's obligation to protect America's homeland and each citizen's right to be free from government intrusion. That conflict is magnified when new surveillance technologies disturb the balance between privacy and safety. More importantly, that war is being fought locally, in our cities, counties and school districts.

Since 1998, Americans have increased their Internet use by over 42 percent, and 75 percent of citizens now access it regularly, for everything from telephone service and email to online shopping and schooling. What most Internet users often don't consider is that almost any electronic communication can be monitored, scanned and stored indefinitely without their knowledge. Their public activities can be watched and recorded in the finest resolution. Facial recognition software can identify people in public spaces almost instantaneously. Yet most of us move through the world with little concern for these technological intrusions.

But what happens when the line blurs between our personal freedom from government intrusion and our social contract to forgo personal interests, when necessary, for greater public security? As government use of technology advances exponentially faster, that line may disappear entirely, which begs the question: Do we have a reasonable expectation of privacy anymore?

A Brief History of Privacy

Though the right to privacy is revered as fundamental, the phrase never appears in the U.S. Constitution, nor in the Bill of Rights. The closest our founders came to a "right to privacy" is inferred from various constitutional amendments. In 1965, Justice William O. Douglas explained in *Griswold v. Connecticut*:



Roberta L. Rowe
Partner
Fresno Office
rrowe@lozanosmith.com

Lee Burdick
Senior Counsel
Fresno Office
lburdick@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

> Various [constitutional] guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one. … The Third Amendment, in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner, is another. … The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment.

Many court cases today address the privacy interests between private parties, involving issues like hacking personal data, identity theft and use of personal information for targeted marketing. In contrast, the U.S. and California constitutions were drafted to protect citizens from all levels of *government* intrusions into their daily lives. Whether it's federal, state or local agencies, or even school districts, government usurpation of individual freedoms has always been perceived as a threat. With the innovation of new technologies, that perception has only grown.

On the heels of the terrorist attacks on 9/11, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" or the "Patriot Act." It was unprecedented in its overhaul of the nation's surveillance laws and vastly expanded the government's authority to spy on American citizens, while simultaneously reducing the checks and balances on those powers. Following passage of the Patriot Act, U.S. intelligence agencies were allowed to collect the phone records and other electronic communications of millions of Americans and to store them at the NSA's Utah Data Center. In light of 9/11, most Americans were willing to concede some privacy interests to foster greater national security.

Several key provisions in the Patriot Act that allowed expansive surveillance expired on May 31, 2015, only to be revived and circumscribed two days later as part of the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act" or the "Freedom Act." That law now requires federal agencies to purge data regarding Americans' telephone calls after 90 days, but allows them to retain other electronic data—like emails and social media postings—indefinitely.

The Patriot Act and the Freedom Act triggered new debate over balancing privacy and national security. But this is not just a federal issue. Local agencies are dealing with video surveillance, monitoring of employees' computers, and drone issues, among others. Often, the battle lines are drawn no farther away than city hall or the school district office.

What Are "Reasonable Expectations of Privacy" Today?

As the framers debated the Fourth Amendment following the 1787 Constitutional Convention, the word "search" typically meant physically breaking into someone's house and searching it. It took the Supreme Court almost 200 years to articulate that an unreasonable "search" could be something more than just a physical intrusion. In 1967, the Court held in *Katz v. United States* that taping a microphone to the top of a phone booth and listening in on a call "searched" the phone booth, though there was no physical intrusion. In *Katz*, Justice John Harlan introduced the concept of a "reasonable expectation of privacy." He defined it this way: Is society prepared to recognize an expectation of privacy as reasonable? If so, a government intrusion into it would be patently "unreasonable" and (presumably) unconstitutional.

Since then, new technologies have presented new challenges related to privacy expectations. In 2012, Justice Samuel Alito opined for the Court in *U.S. v. Jones*:

> [T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. ... New technology may provide increased convenience or security at the expense of privacy, and many people may find the trade-off worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.

In contrast, U.S. District Court Judge Jeremy Fogel of the Northern District of California reminded us in a 2014 article for the American Bar Association's litigation journal that for "every inveterate user of social media who tweets random comments while standing in line at the grocery store, there is someone ... who is indignant when she learns that the cookies in her web browser permit all manner of advertisers to include her in their target audience." When individual norms vary so broadly on the terrain of constant technological change, what constitutes a "reasonable person's" expectation of privacy? Perhaps continued dialogue will create a standard adaptable enough to survive the challenges of new technologies. In the meantime, local agencies will have to walk this thin line carefully, and are advised to work closely with legal counsel on how best to do it, protecting their constituents' safety while respecting their privacy.