

On Privacy: Did Technology Kill the Fourth Amendment?

On September 17, 1787, the delegates to the Constitutional Convention gathered in Philadelphia's Independence Hall to sign the country's newly drafted founding document. Every year, the Cato Institute hosts a daylong conference to celebrate this momentous date in the history of liberty. At the 10th Annual Constitution Day event this year, the Hon. Alex Kozinski—Chief Judge of the U.S. Court of Appeals for the Ninth Circuit—delivered the B. Kenneth Simon Lecture on Constitutional Thought. Born in Bucharest, Romania, Judge Kozinski came to the United States when he was 12. He clerked for then-Judge Anthony Kennedy and Chief Justice Warren Burger before serving as the first U.S. Special Counsel under President Ronald Reagan. In his address, excerpted below, Judge Kozinski spoke about the introduction of new technologies and how changing cultural expectations of privacy have influenced judicial applications of the Fourth Amendment.

We've been trying to protect our privacy ever since Adam went off looking for a fig leaf. But, according to conventional wisdom, technology has made us care less and less about it. It's easy to see how someone might get that idea: we trade our privacy for convenience in small ways every day. When I drove to the airport earlier this week, I hooked up my GPS because I knew the trip would be less of a headache. At the airport, I overheard someone on a cell phone who evidently couldn't wait to tell his friend how he was recovering from a recent vasectomy. If you've seen an episode of *24*, you know that we probably all get captured on a piece of security footage when we walk into the hotel where we're staying. And almost no one here would be surprised to find photos of himself up on Facebook or Above the Law after a night out. I see some of you tweeting about it right now.

Technology has undoubtedly made it easier for others—including the government—to figure out what's going on in our lives. I've worried about this for quite some time, and I'm not the only one. Over 50 years ago, dissenting in a series of cases on undercover cops, government informants, and bugging, Justice William O. Douglas warned

us, "we are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government." More recently, CNN, NPR, and *Scientific American* all published stories on the coming end of privacy. Time sported a cover just a couple of months ago that read, "Everything about you is being tracked—get over it." And the CEO of Google sniffed, "If you have something you don't want anyone to know, maybe you shouldn't be doing it in the first place." Yeah, right.

I, for one, can't accept the idea that technology has killed all expectations of privacy. I'd like to make three points: First, technology that erodes our privacy often escapes criticism only because so few people are aware that it exists. Second, often we actually expect technology to increase our privacy. Third, it's possible to preserve a robust right to privacy in the current age of technology. But that effort will depend on educated citizens, legislative action, and courts willing to rethink current Fourth Amendment jurisprudence.

Private companies are constantly collecting information without our knowing about it. Take cell phones: Almost 90 per-

cent of Americans own them, but how often do we consider that they can be used to pinpoint where you are at all times? If you have a smartphone with a camera, then the phone will encode your location every time you take a picture. Let's say you visit the grandkids, take pictures of them playing in the yard, and then post the photos online where creeps can find them. You've not only shown them what the kids look like; you've told them where they live.

If you have an older "dumb" phone like I do, your carrier still knows where you are and where you've been. Between September 2008 and October 2009, Sprint Nextel "pinged" the locations of its customers on behalf of law enforcement more than 8 million times. The company even created a self-service web portal that allows law-enforcement agencies to track phones on the network. As Judge Douglas Ginsburg pointed out in a recent opinion, "a person who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, [or] an outpatient receiving medical treatment." We'll be in trouble if the authorities ping all of our phones tonight: they'll have finally found that vast right-wing conspiracy they've been looking for.

Why has there been so little outcry? Most people simply don't realize they're carrying a tracking device with them at all times. Judge Dolores Sloviter made exactly this point in a recent Third Circuit decision:

It is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, when a cell phone user makes a call ... there is no indication to the user that [this] will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.

This will be the case every time we buy products that transmit information about

us without giving us fair warning.

Like a pair of underwear from Walmart. The *Wall Street Journal* recently reported that the superstore plans to start attaching small, trackable RFID tags to individual pieces of clothing in order to keep better tabs on the company's inventory. One county in California has already begun implanting RFID chips in school uniforms to track preschoolers. They're in credit cards, passports, and even some ticket stubs. Soon they'll be in all our customer loyalty cards and driver's licenses, and we'll be transmitting a treasure trove of information every time we walk into a store or drive down the highway.

Smart electrical meters are another worry. In 2009, the federal government invested billions of dollars to develop a "smart grid" that will provide detailed information about home energy consumption. The technology transmits a large cache of personal information about what we do inside our own homes. This can include our most intimate activities. Imagine, for example, that Bruce's wife is out of town but the meter shows two cell phones plugged in and a curling iron on in the bathroom.

Our use of these new technologies doesn't signal that we're less interested in privacy. The idea of the government monitoring our whereabouts, our habits, our acquaintances, and our interests still creeps us out. We often just don't know it's going on until it's too late.

Sometimes we do understand that technology threatens our privacy. We may get an important phone call in a public place and decide we have to take it. Or we use a supermarket loyalty card even though we know the store is tracking our purchases. Examples like these are often trotted out as proof that we no longer care about privacy. But this overlooks how we use technology to control what others learn about us. Not so long gone are the days when stores made physical carbon copies of all your credit-card information. I still remember handling the case of Mr. Belisario, who made it his business to go through the trash can of the gas station where he worked and fish out the carbons. He then used the name, number, and expiration date imprinted there to

make charges on those accounts. No more. That kind of information is now encrypted and sent electronically.

Perhaps the most important protection we've developed is online anonymity. Instead of standing in line with a box of Preparation H, wondering if the checkout person is suppressing a snicker, you can have a discreet package sent to your home with just a few clicks on eBay. Rather than worry-

“The idea of the government monitoring our whereabouts still creeps us out. We often just don't know it's going on until it's too late.”

ing whether everyone on the plane can see what you're reading, you can download books to your Nook or Kindle. Technology has made it easier to conduct our business behind avatars, screen names, and secondary e-mail addresses. People are clearly still concerned about keeping some things to themselves. In a recent survey conducted by researchers at Berkeley and Penn, about 90 percent of the under-35 crowd agreed that there should be a law requiring websites and advertising companies to delete all stored information about them. A majority of the sample reported being more concerned about privacy issues than they were five years earlier.

So what can we conclude from all this? I think it's fair to say that privacy is not dead as an ideal. We still crave it and expect it, despite the inroads made by technology. In fact, people expect more privacy in the digital age. At the same time, it's clear that we are

willing to trade quite a bit of privacy for a little bit of convenience. No one here, I suspect, is going to stop carrying a cell phone, even though we're fully aware it's tracing our location just about every moment of the day.

The government is perfectly happy to take advantage of our devil's bargain by dipping into available stores of information about us. That brings us to the Fourth Amendment, which provides that people shall be secure in their homes, papers, and effects. As originally conceived and interpreted for most of our history, this provision was a protection against the invasion of property. If the government wanted to enter our homes or examine our things, it had to comply with the requirements of the Fourth Amendment. This all worked pretty well so long as life unfolded in the concrete spaces of the physical world. After all, you couldn't read my diary or business records without entering the building where I kept them.

This all changed with the advent of the telephone. In 1928, the Supreme Court heard *Olmstead v. United States*—a case involving a criminal prosecution based on evidence the police obtained by tapping the defendant's phone line. Officers never entered his home or office; instead, they climbed the telephone poles in front of the house. The Supreme Court made short work of the case: The police didn't trespass on the defendant's property and thus did not invade any interest protected by the Fourth Amendment. This didn't sit well with Justice Louis Brandeis, who almost 40 years earlier had coauthored a highly influential article in the *Harvard Law Review* entitled "The Right to Privacy." It continues to be one of the most frequently cited law review articles of all time.

In his dissent, Brandeis argued that the police had violated the defendant's right to privacy by listening to his private phone conversations. In effect, he was urging the Court to jettison static concepts of property rights as the benchmark for the Fourth Amendment. Instead, he argued, the Fourth Amendment protects the right to be left alone. Under this view, the Fourth Amendment didn't stop at our front door, nor was it limited to gaining physical access to the

content of communications. Rather, it protected an intangible concept of personal autonomy that defends us against much more than the physical invasion of our property rights.

If Justice Brandeis's 1928 dissent has a surprisingly modern ring to it, it's because the ideas he planted took root and eventually became the Fourth Amendment as we know it today. In 1967, the Court decided *Katz v. United States*, which involved the police taping a phone conversation. Katz was in a phone booth making illegal bets, and the police were on to him. So they placed a tape recorder on the outside of the booth and managed to record Katz's half of the call. The government argued that it faithfully complied with *Olmstead*. But in a world of ubiquitous telephones, tiny microphones, and tape recorders, the justices were no longer willing to limit the Fourth Amendment to invasions of property rights. Instead, the Court held that the police violated Katz's Fourth Amendment rights because he had a reasonable expectation of privacy when he closed the door of the phone booth. *Katz* overruled *Olmstead* and discarded the property-based foundation on which it rested. In its place came a new standard: the Fourth Amendment extends to whatever places and communications an individual can reasonably expect to keep private.

This new standard has three important features—one good, the second so-so, and the third pretty bad. The first is that the standard comports much more with the modern way of life. In a world where people communicate electronically, travel by public transport, and sleep outside their own homes, the new standard better reflects the values of the Fourth Amendment.

The not-so-good feature is that the boundaries of the new standard aren't very well defined. It's often hard to know in advance whether a particular invasion of privacy is also a constitutional violation. This leaves both the government and the public uncertain about their respective rights. They have to wait for courts to tell them after the fact whether someone's rights were violated. The issue often arises in cases where the police have seized highly incriminating evi-

dence, so that finding a constitutional violation might mean a guilty guy gets to walk. The incentive is to find that the police didn't conduct an illegal search.

The worst aspect of the new regime, however, is tied up with the word "reasonable." How do you determine whether something meets this definition? The test is whether we, as a society, recognize the privacy interest as

ation isn't just by phone—it's by e-mail, text message, Facebook, Twitter, Gchat, Skype, and who knows what's next. We no longer keep diaries locked with a key and hidden under a floorboard of our homes; we keep them on a server somewhere in the cloud. The world is changing very rapidly, and reasonable expectations are still in flux.

It is there that privacy seems to be least



one worthy of protection. The fact that I consider certain conduct private is of little consequence if most people act like it's not. The scope of my right to privacy thus depends on common expectations, which are shaped by the actions and attitudes of everyone else.

Let's say *Katz* were decided today. What would the Court say? These days, there are no public spaces set aside for having phone conversations, so people converse on the phone just about anywhere. Would the Court really say that a guy standing on a street corner shouting into his cell phone had a reasonable expectation of privacy? I'd guess no. They would say that people in general didn't value privacy very much when it came to phone conversations, and phone communications therefore aren't private.

I'm not too worried the Supreme Court will overrule *Katz*. But we've come a long way from those days, and most of our communi-

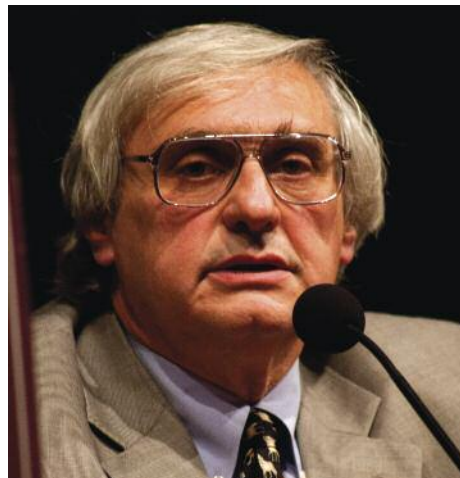
respected as a value. Many modern practices seem to suggest that people are not interested in privacy: People blog about their sexual exploits. They post immodest pictures of themselves on social-media sites. They promiscuously disclose their activities in e-mails and tweets. Of course, not everybody may be doing this; in fact it may be only a small minority. But they set the bar for the rest of us because they have a disproportionate impact on our perception of what is a reasonable expectation of privacy. What we think of as the prevailing view defines the zone of privacy we can reasonably expect to have for purposes of the Fourth Amendment. Remember that we are all tied together at the ankle, so the fact that you wish to preserve more privacy than society at large will make little difference because idiosyncratic views are perforce not considered reasonable.

So is there any way to prevent further erosion of our privacy and perhaps gain back some of the ground we have lost? I want to propose a three-part program for doing so. The first part calls for an education campaign that will make people aware that privacy, as a shared resource, is fragile. I propose that everyone here make an effort to object to behavior that erodes privacy. I, for example, have taken to staring at people who talk loudly in their cell phones in public. I nod when they say something that sounds positive, and laugh when they say something funny. I try to make them feel that I am part of their conversation—because, thanks to them, I am.

The second step involves the government. While I am always reluctant to suggest more regulation, I also believe individuals should make informed decisions. We often give up privacy because we are not aware of the privacy implications of the technology we use. Who really understood, when we first started using cell phones, that we were creating maps of our movements that would be preserved in some database forever? It's much harder to give up an innovation once we've gotten used to it. The time to learn about the privacy implications of some new technology is before we come to rely on it.

Finally, the courts must take a far more realistic view of what is a reasonable expectation of privacy. Right now, the standard mode of analysis is that if you knowingly expose information to third parties, you can have no reasonable expectation of privacy. If you have a pile of cash and hide it in your mattress, the government needs probable

cause and a warrant to seize it. But if you deposit that money, the bank records are fair



“Make an effort to object to behavior that erodes privacy.”

game. Much of this case law traces its roots to *United States v. Hoffa*—the famed president of the Teamsters, who one day disappeared and was never heard from again. Before his disappearance, he was prosecuted and convicted of jury tampering based in part on evidence adduced against him by a government informant who spied on his activities. According to the *Hoffa* majority, “[t]he risk

of being overheard by an eavesdropper or betrayed by an informer ... is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.”

This strikes me as an extraordinarily broad rationale for what it means to give up one's right to privacy. If speaking to friends, putting money in a bank account, and receiving telephone calls waive the privacy of that information, then very little indeed can remain private today. The Supreme Court must reconsider the rationale of *Hoffa* and similar cases. Living in an electronically interconnected world cannot be the basis for concluding we lack an expectation of privacy as to the information we disclose to third parties as part of our normal daily living. This would make the *Katz* standard as unworkable as the *Olmstead* trespass standard before it.

Fortunately, I don't think it's too late to turn back the clock. As Justice Kennedy cautioned in the *Quon* case from last term, “The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment. . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.” But we must do our share, by becoming aware of the privacy implications of many of the things we do—by starting to impose a measure of discipline on ourselves and those around us—to ensure that this notion of a reasonable expectation of privacy retains some real meaning. ■



Holiday Gifts from the Cato Institute at Cato.org/Store

For yourself or as a gift—the Cato Online Store offers a vast range of merchandise. From Cato's renowned Pocket Constitution and acclaimed books, to apparel, bags, Cato-brand Lands' End apparel, and gift sponsorships, it's the perfect way to support Cato and demonstrate your commitment to individual liberty. Cato Sponsors receive a 35% discount on all purchases (except Lands' End). Become a Sponsor when you check out of the Cato Store to immediately receive this discount off your entire purchase.

