# Has Technology Killed the Fourth Amendment?

*Alex Kozinski* and Eric S. Nguyen***

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. And it's easy to see how someone might get that idea: We trade our privacy for convenience in small ways every day. When you're driving to the airport, you hook up your GPS because you know it'll be less of a headache if something can tell you exactly how to get where you're going. And at the airport, it's no surprise when you overhear someone on a cellphone who evidently can't wait to tell a friend (and everyone at the gate) how he's doing after a recent vasectomy. If you've seen an episode of *24*, you probably expect that we all get captured on a piece of security footage when we walk into a hotel. And almost no one here would be surprised to find photos of himself up on Facebook or *Above the Law* after a night out—especially one spent with a well-known judicial superhottie. Some of you are tweeting about it right now.

Technology has undoubtedly made it easier for others to figure out what's going on in our lives. And that means it's easier for the government to do the same thing. This has been a worry for quite some time. Over 50 years ago, writing separately 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.''[1] More recently, CNN,

* Chief Judge, United States Court of Appeals for the Ninth Circuit. This is an edited version of remarks delivered as the 10th annual B. Kenneth Simon Lecture in Constitutional Thought at the Cato Institute on September 19, 2011.

** Former law clerk to Chief Judge Kozinski.

[1] Osborn v. United States, 385 U.S. 323, 341 (1966) (Douglas, J., dissenting).

NPR and *Scientific American* all published stories on the march toward the end of privacy.[2] Not to be outdone, *20/20* ran a segment on the *death* of privacy.[3] *Time* sported a cover last year that read, ''Everything about you is being tracked—get over it.''[4] 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.''[5]

We shouldn't accept the idea that technology has killed all expectations of privacy. First, technology that erodes our privacy often escapes criticism only because so few people are aware that it exists until it's too late to do anything about it. Second, we actually expect technology to *increase* our privacy far more than is conventionally recognized. 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. Cato has long defended the right to privacy, and it's an honor to discuss it with you here today.

**I**

Here's the vicious cycle that worries many of us: First, a private company creates some hot new product that everyone picks up, like a cell phone or GPS device, or maybe a piece of software or a supermarket loyalty card. The company uses the technology to collect information about its customers. Doing so is perfectly constitutional because the company isn't a state actor. But soon the government asks for the information, or just uses the technology to start monitoring us itself. All of this happens while most of us have no

[2] See Nat'l Pub. Radio, The End of Privacy, http://www.npr.org/series/114250076/the-end-of-privacy; Daniel J. Solove, Do Social Networks Bring the End of Privacy?, Sci. Am., Aug. 18, 2008, available at http://www.scientificamerican.com/article.cfm?id=do-social-networks-bring; John D. Sutter, The Internet and the ''End of Privacy,'' CNN.com, Dec. 13, 2010, http://articles.cnn.com/2010-12-13/tech/end.of.privacy.intro.

[3] See John Stossel et al., ABC News, The Death of Privacy, Apr. 28, 2007, http://abcnews.go.com/2020/story?id=2752636.

[4] See Joel Stein, Your Data for Sale: Everything About You Is Being Tracked—Get Over It, Time, Mar. 21, 2011.

[5] Junichi P. Semitsu, From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance, 31 Pace L. Rev. 291, 318 (2011).

clue it's going on. The government finally uses what it's discovered against you in court, and when you object, it says you didn't have a reasonable expectation it would be kept private. After all, the technology is ''in general public use'' and reveals information you've already shared with a third party.[6]

Private companies are constantly collecting information without our knowing about it. Take cell phones: Almost 90 percent of Americans use them, and it'd be surprising if there's anyone in the room who doesn't have one right now. But how often do you consider that they can be used to pinpoint exactly 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.[7] So 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 but also told them where they live.

But let's say you've got a dumbphone like I do. Your carrier still knows where you are and where you've been. Your phone constantly announces your location by ''pinging'' nearby cell towers. The phone company can also get a location by pinging your phone. Between September 2008 and October 2009, Sprint Nextel pinged its customers on behalf of law enforcement more than eight million times.[8] The company even created a web portal that allows law enforcement agencies to track any phone on the Sprint network by self-service pinging. This kind of surveillance appears to have increased dramatically in recent years, and it implicates serious privacy concerns.[9] As

[6] See Kyllo v. United States, 533 U.S. 27, 39–40 & n.6 (2001) (''[W]hether or not the technology is in general public use may be a factor.''); Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (conveyance of dialed phone numbers to the telephone company).

[7] See Francine Kopun, Posting Pictures Online Reveals More than You Know, Toronto Star, Aug. 2, 2010, at E1.

[8] See Kim Zetter, Feds ''Pinged'' Sprint GPS Data 8 Million Times Over a Year, Wired.com, Dec. 1, 2009, http://www.wired.com/threatlevel/2009/12/gps-data; see also Noam Cohen, It's Tracking Your Every Move and You May Not Even Know, N.Y. Times, Mar. 26, 2011, at A1.

[9] See Eric Lichtblau, Wireless Firms Are Flooded by Requests to Aid Surveillance, N.Y. Times, July 8, 2012, at A1 (''The surging use of cell surveillance was also reflected in the bills the wireless carriers reported sending to law enforcement agencies to cover their costs in some of the tracking operations. AT&T, for one, said it collected $8.3 million last year compared to $2.8 million in 2007, and other carriers reported similar jumps in billings.'').

Judge Douglas Ginsburg (Cato's first B. Kenneth Simon Lecturer[10]) pointed out in a recent opinion, ''[a] person who knows *all* of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.''[11] 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.

There's been very little outcry about cell phone tracking, but it's not because we don't expect information that can be collected from our phones to remain private. What's going on is that 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:

> [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, ''[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.''[12]

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,

[10] See Douglas H. Ginsburg, On Constitutionalism, 2002–2003 Cato Sup. Ct. Rev. 7 (2003).

[11] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (emphasis added), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[12] In re Application of U.S. for an Order, 620 F.3d 304, 317–18 (3d Cir. 2010) (second alteration in original) (emphasis omitted); see also United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissental) (''Most targets won't know they need to disguise their movements or turn off their cell phones because they'll have no reason to suspect that Big Brother is watching them.''); Maynard, 615 F.3d at 563 (''A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.' '' (citation omitted)).

trackable radio-frequency identification (RFID) tags to individual pieces of clothing in order to keep better tabs on the company's inventory.[13] One county in California has already begun implanting RFID chips in school uniforms to track preschoolers.[14] They're in credit cards, passports and even some ticket stubs.[15] 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.[16]

Smart electrical meters are another worry.[17] In 2009, the federal government invested billions of dollars to develop a ''smart grid'' that will provide detailed information about home energy consumption.[18] Like cell phones and RFID chips, the technology transmits a large cache of personal information about activities within the home. Let's say Bruce's wife is out of town, but the meter shows two cell phones plugged in and a new curling iron on in the bathroom. Or, no, wait: It's not a curling iron after all; it's another man's electric shaver. Sally claims she had to miss work to be at a funeral, but her blender and television were on all day.

Our use of these new technologies doesn't signal that we're less interested in privacy. The idea of the government's 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. It's like one of those nightmares where you suddenly realize you've been walking around naked and people are pointing at you and laughing.

[13] Miguel Bustillo, Wal-Mart Radio Tags to Track Clothing, Wall St. J., July 23, 2010, at A1.

[14] Alejandro Martínez-Cabrera, Concern over Privacy as ID Tags' Use Expands, S.F. Chron., Sept. 6, 2010, at D1.

[15] See Liz F. Kay, Information Tags Along Everywhere You Go, Balt. Sun, May 11, 2008, at A1.

[16] See also Jim Harper, Cato Institute, Online Privacy (Part 1), http://www.cato.org/publications/commentary/online-privacy-part-1 (''Unaware of how internet connections, browsers, websites, plug-ins and various other technical tools work, lots of people do not know what information they share when they go online, how much of it, or how revealing it is. Obviously, this deprives them of the opportunity to do anything about it.'').

[17] See Sonia K. McNeil, Privacy and the Modern Grid, 25 Harv. J. L. & Tech. 199 (2011).

[18] See Cheryl Dancey Balough, Privacy Implications of Smart Meters, 86 Chi.-Kent L. Rev. 161, 161–62 (2011).

## II

Of course, sometimes we do understand that new technology threatens our privacy. We may get an important phone call in a public place and decide to go ahead and talk, even though we know others might overhear us. Or we use a supermarket loyalty card, even though we know that Ralph's or Safeway is tracking our purchases. Examples like these are often trotted out as proof that we no longer care about privacy.

But this understanding overlooks how we use technology to control what others can learn about us.[19] 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 imprinted name, number and expiration date to make charges on those accounts. No more. That kind of information is now encrypted and sent electronically. And remember when someone was able to listen in while Prince Charles and Camilla Parker Bowles had a naughty conversation on their cell phones back in 1989? That can never happen anymore, which is too bad in some ways. When reporters from *News of the World* found a way to access voicemail accounts of unsuspecting people, the hacking itself became an international scandal.[20]

We all secure the information in our phones, computers and online accounts by keeping it behind a series of passwords. Other times we use technology to make it difficult for others to know where we are and what we're doing. For example, we can make calls from our cell phones and make it look like we're in the office even though we're at home watching reruns of *Seinfeld* with our feet propped up on a stack of briefs.

[19] Cf. James Gibson, Doctrinal Feedback and (Un)Reasonable Care, 94 Va. L. Rev. 1641, 1712 n.279 (2008) (''[I]f privacy-eroding technologies proliferate more quickly than privacy-preserving technologies, our expectations will inexorably diminish—or at least doctrine will interpret them as having diminished, and our constitutional rights along with them—making it easier for the next, more intrusive technology to gain a toehold in the realm of reasonableness.'').

[20] See Sarah Lyall, Murdoch Closing Tabloid Linked to British Hacking, N.Y. Times, July 8, 2011, at A1.

Perhaps the most important protection we've developed is online anonymity, which allows us to keep private many activities we'd otherwise do in public. You used to stand in line to buy the extra-strength Rogaine or Preparation H and wonder if the checkout person was giving you a friendly smile or suppressing a snicker. You can now have those things sent to your home in a discreet package with just a few clicks on Amazon or eBay. Buy books online and download them to your Nook or Kindle and no one will know what you're reading on the plane. Or maybe you felt the judgmental eyes of the ushers the third time you walked into *Alvin and the Chipmunks: The Squeakquel* alone at the movie theater. Netflix or Vudu. Online subscriptions let us do even more, like secretly catch up on celebrity gossip or get the latest from the robot world. We can easily look up medical information at the Mayo Clinic website before deciding whether to go to the doctor about a pain in the, uh, neck. And, like the authors of *The Federalist Papers* and their opponents, we can engage in political debate without having to reveal our true identities.[21] Technology has made it easier to conduct our business behind avatars, screen names and secondary email addresses.

Of course, this online activity generates information that *could* be linked back to us. Sites like Amazon and Netflix keep a record of which pages you've viewed in order to help recommend things you'd like to view next—or maybe so they can sell information about you to purveyors of targeted advertising. But we go to those pages with the expectation that this is all done using algorithms and that there isn't really anyone at the other end snooping into our individual purchases or movie selections. Here's how Google explains this: ''It's important to note that our scanning and indexing procedures are 100% automated and involve no human interaction.''[22] Having a machine know your habits and use the information only to show you other products somehow seems a lot less intrusive

[21] See McIntryre v. Ohio Elections Comm'n, 514 U.S. 334, 342–43 & n.6 (1995).

[22] Google Apps Administrator Help: Security and Privacy, Google.com, http://support.google.com/a/bin/answer.py?hl=en&answer=60762 (last accessed May 30, 2012) (included in response to the question, ''What kind of scanning/indexing of user data is done?''); see also Gmail Help: Ads in Gmail and your personal data, Google.com, http://support.google.com/mail/bin/answer.py?hl=en&answer=6603 (last accessed May 30, 2012) (''Ad targeting in Gmail is fully automated, and no humans read your email in order to target advertisements or related information.'').

than having some employee at Google deciding to recommend a local divorce lawyer or a subscription to the *Advocate*.

The public has fiercely protested similar violations of anonymity. Take, for example, the response to the way Facebook has pushed the envelope from time to time. In 2007, the site launched an online ad system called Beacon that tracked user activity on partner sites, such as nytimes.com and fandango.com.[23] Comment on a story or buy a movie ticket and Facebook would instantly know about it—and spread the message to all your friends. People decided that it wasn't such a great feature when they started buying their Christmas presents: *Why is my best friend wearing the diamond earrings my boyfriend bought online?* Faced with tens of thousands of people protesting and a class-action lawsuit, Facebook eventually scrapped Beacon.[24] The company caused another uproar when it switched many items on users' profiles from private to public.[25] Facebook again had to cut back on what information is made public and to simplify its privacy controls.[26] More than two million people joined a Facebook group called ''Millions Against Facebook's Privacy Policies and Layout Redesign.''[27]

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.[28] A majority of the sample reported

[23] See Louise Story & Brad Stone, Facebook Retreats on Online Tracking, N.Y. Times, Nov. 30, 2007, at C1; Jessica Guynn, Saving Face Over Facebook Faux Pas, L.A. Times, Dec. 6, 2007, at C1; Ellen Nakashima, Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy, Wash. Post, Nov. 30, 2007, at A1.

[24] See Ylan Q. Mui, In Shoppers' Web Networks, Privacy Has No Price Tag, Wash. Post, May 22, 2010, at A1.

[25] Editorial, Facebook Responds, N.Y. Times, May 25, 2010, at A26.

[26] See Wailin Wong, Intersection of Personal, Private Keeps Shifting, Chi. Trib., May 27, 2010, at C25 (''It's become a familiar pattern: Facebook rolls out changes. A backlash ensues, and the social networking giant makes further changes to quell the unease.'').

[27] Facebook appears to have deleted all of the group's members in February 2012, but the group is back up to a few thousand members as of the date of this publication.

[28] See Chris Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies 11 tbl.5 (Apr. 14, 2010) (unpublished manuscript), available at http://papers.ssrn.com/sol3/papers.cfm?abstract;usid=1589864; see also Laura M. Holson, Tell-All Generation Keeps Some Things Offline, N.Y. Times, May 9, 2010, at A1.

being more concerned about privacy issues than they were five years earlier.[29]

So what can we conclude from all this? It's fair to say that privacy is not dead as an ideal. People still crave it and expect it, despite the inroads made by technology. In many ways, people expect more privacy as a result of technology and feel resentful and angry when they learn that technology has betrayed them. At the same time, it's clear that people are willing to trade quite a bit of privacy for a little bit of convenience. It's unlikely that anyone here 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.

**III**

The government is perfectly happy to take advantage of our devil's bargain by dipping into available stores of information about us. It will also create databases of its own to keep track of our movements and habits in an effort to solve past crimes and deter future ones. Indeed, immediately after 9/11 much blame was laid on law enforcement for its failure to uncover the criminal conspiracy before it had a chance to achieve its nefarious goals. One might say that Americans are a bit schizophrenic or perhaps hypocritical in this regard: We resent it bitterly when the government snoops around in our lives, but we are highly critical when it fails to detect criminal activity by monitoring would-be criminals and terrorists. How is the government going to figure out who the terrorists are unless it studies the habits of a lot of ordinary people so it can spot the unusual behavior? In a very real sense, the government can't watch out for the terrorists among us unless it keeps an eye on all of 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.[30] If the government

[29] Hoofnagle et al., *supra* note 28, at 15 tbl.10. But see Mary Madden & Aaron Smith, Reputation Management and Social Media 21 (Pew Internet & American Life Project 2010), available at http://www.pewinternet.org/reports/2010/reputation-management.aspx (finding decreased concern about availability of personal information online).

[30] See, e.g., Arianna Kennedy Kelly, The Costs of the Fourth Amendment: Home Searches and Takings Law, 28 Miss. C. L. Rev. 1, 6 (2009).

wanted to enter our homes or read our papers or examine our things, it had to comply with the requirements of the Fourth Amendment. This system 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 and then getting hold of the notebook or ledger itself.

This all changed with the advent of the telephone. In 1928 the Supreme Court heard a case involving a criminal prosecution based on evidence the police obtained by tapping several phone lines.[31] Officers never entered the defendants' homes or their main office; instead, they used wires in the basement of the office building and in the streets near the houses. The Supreme Court made short work of the case: The police didn't commit a trespass onto the defendants' property and thus did not invade any interest protected by the Fourth Amendment. This ruling 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.''[32] It continues to be one of the most frequently cited law review articles of all time.[33]

Justice Brandeis dissented in *Olmstead v. United States*, the wiretapping case.[34] He argued that the police had violated the defendants' right to privacy by listening to their private phone conversations. In effect, Brandeis 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 the front door of our house or business, nor was it limited to restricting physical access to the content of communications. Rather, Brandeis argued, the Fourth Amendment 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

[31] See Olmstead v. United States, 277 U.S. 438 (1928).

[32] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

[33] See Fred R. Shapiro, The Most-Cited Law Review Articles Revisited, 71 Chi.-Kent L. Rev. 751, 767 (1996).

[34] 277 U.S. at 471 (Brandeis, J., dissenting).

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.[35] Charles 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 the recording involved no physical penetration of the booth and therefore did not violate the Fourth Amendment. But in a world of ubiquitous telephones, teletypes, telegraphs, 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.[36] *Katz* overruled *Olmstead* and discarded the property-based foundation on which it rested. In its place came a new standard: The Fourth Amendment protects an individual's reasonable expectation of privacy. The protection 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 stay in places that are not 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 as well-defined as property rights. 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 afterward whether someone's rights were violated. And the issue often arises after the police have seized highly incriminating evidence, so finding a constitutional violation might mean a guilty

[35] 389 U.S. 347 (1967).

[36] *Id.* at 352 (''One who occupies [a telephone booth], shuts the door behind him, and pays the tolls that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.'').

guy gets to walk. This creates an incentive 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.'' The courts will not protect an individual's expectation of privacy if it's not reasonable, and how do you determine whether something is reasonable? The test is whether we, as a society, recognize the privacy interest as one worthy of protection. When it comes to privacy, what you and others in society think and do has a profound effect on my rights. The fact that you consider certain conduct private is of little consequence if most people act like it's not. The scope of your 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? Judges and justices live in the world and understand how it works. Today, there are no public spaces set aside for having phone conversations, so people converse on the phone just about anywhere, at any time, and usually in an extra loud voice: at the airport, at the grocery store, in the doctor's office, in restaurants and even in movie theaters. 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 wouldn't be private.

There's little reason to worry that the Supreme Court will overrule *Katz*. But we've come a long way from the days of *Katz*, and most of our communications these days aren't just by phone—they're by email, text message, Facebook post, tweet and who knows what's next. We no longer keep diaries locked with a key and hidden under a floorboard in our homes; we keep them on a server somewhere in the cloud, or on a laptop or an iPhone. The world is changing very rapidly, and what constitutes a reasonable expectation of privacy when it comes to newer kinds of technology is still in flux.

And it is there that privacy seems to be least 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 appear on shows like *Jerry Springer* and air their dirty laundry; they discuss intimate subjects within full hearing of a roomful of people; they

promiscuously disclose their activities in emails and tweets. Of course, not everybody is 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. To understand why, imagine that out of a group of 100 people, 90 guard their privacy jealously while 10 are exhibitionists. You would know right away that there were 10 who didn't care about their privacy, but unless you knew beforehand about the other 90, you would have no way of knowing what their practices were, or how many of them there were; the 10 visible ones would therefore exert a disproportionate influence on our perception of people's preferences.

And what we think is 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 your 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? Here is a proposed three-part program for doing so. The first part calls for an education campaign that will make people aware that privacy is a fragile shared resource, and that failure to respect and enforce privacy boundaries by even a few will erode privacy for all of us. We have had any number of such education campaigns in the last few years, and they have changed many aspects of our lives: Not so long ago it was perfectly acceptable to smoke in all manner of public and private places, but as we have become aware of the dangers of smoking, it started to disappear from airplanes, restaurants, bars and music events. Our eating habits have changed, as we consume less fat and more nutritious foods; we recycle; we wear helmets and seat belts. Some of these changes have come about as a result of legislation, but the legislation itself was the result of changing perceptions and attitudes.

Everyone reading these remarks should make an effort to object to behavior that erodes privacy and help educate others to its dangers. You might, for example, take to staring at people who talk loudly into their cell phones in public. Nod when they say something that sounds positive, and laugh when they say something funny.

Give them the thumbs up when they say something exciting. In general, try to make them feel that you are part of their conversation—because you are. They made you part of it by talking loudly enough for you to overhear.

There are many such techniques to alert people when they are committing a self-invasion of privacy and thereby eroding everybody else's privacy as well: Leave a message on somebody's Facebook wall, or object to obnoxious blog posts. And let people know *why* you are doing it. Spread the word and let people know that this kind of behavior is destructive and will only make it easier for the government to spy on all of us.

The second step involves the government. We give up much by way of privacy, especially when dealing with electronic devices, because we are not aware of the privacy implications of much 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? Or who knew about the ability to track our movements on the Internet when we first started web surfing? Or about GPS metadata in photographs? Or about the fact that the RFID chip embedded in our FasTrak or E-ZPass device could be read at other locations to track our movements? Many electronic devices, from smartphones and FasTraks to Internet browsers and electric meters, have huge privacy implications that we know very little about. We are often sold on the convenience and ease of using them but are told nothing about what we are giving up by way of privacy by embracing the new technology. It's much harder to give up technology once we've gotten used to it and it becomes a part of how we conduct our daily business, so the time to learn about it is before we come to rely on it.

While I am always reluctant to suggest more government regulation, there is an important value in having individuals make informed decisions. I think the government can help by adopting standards for how breaches of privacy are to be disclosed, and mandating their disclosure in an easily accessible way before the new device is bought and put into use. Doing so will not only help us make more informed choices, it will also set up a competition among manufacturers to give us devices that eliminate or minimize the privacy implications.

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.[37] Thus, if you have a pile of cash and hide it in your mattress, it's private and the government needs probable cause and a warrant to seize it. But if you deposit money with a bank, you have no constitutional right to have the information kept private.[38] Or if the phone company keeps a record of calls you've made, then you have knowingly disclosed to a third party the people you were calling—and that information is not protected by the Fourth Amendment.[39]

Much of this case law traces its roots to a case by the name of *Hoffa v. United States*, involving the famed president of the Teamsters who disappeared one day and was never heard from again.[40] Before his disappearance, Hoffa was prosecuted and convicted of jury tampering, based in part on the testimony of an informant used by the government to spy on Hoffa's activities. According to the *Hoffa* majority, ''[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.''[41]

That is 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 making telephone calls routed through a phone company waive the privacy of information so disclosed, then very little indeed can remain private in a world that is rapidly becoming more electronically interconnected. The courts—and specifically the Supreme Court—must reconsider the rationale of *Hoffa* and similar cases. Living in an interconnected world cannot be the basis for concluding that we lack an expectation of privacy as to information we disclose to third parties as a routine part of a normal day. If the courts continue to apply this rationale, then pretty much

[37] See generally Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561 (2009).

[38] See United States v. Miller, 425 U.S. 435, 442–43 (1976).

[39] See Smith v. Maryland, 442 U.S. 735, 744 (1979).

[40] 385 U.S. 293 (1966).

[41] *Id.* at 303 (quoting Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting)).

nothing will be private, and the *Katz* standard will become as unworkable as the *Olmstead* trespass standard before it.

Fortunately, it's not too late to turn back the clock on the privacy implications of most of modern technology. The Supreme Court expressed a willingness to listen in the *Quon* case from the 2009–2010 Term. Justice Anthony Kennedy's opinion cautioned that ''[t]he 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.''[42] And the Supreme Court's recent decision to affirm the U.S. Court of Appeals for the D.C. Circuit in *United States v. Jones*—especially with the concurring opinions of Justices Samuel Alito and Sonia Sotomayor—keeps hope alive.[43]

But we must do our share, by becoming aware of the privacy implications of many of the things we do and by starting to impose a measure of discipline on ourselves and those around us to ensure that the idea of a reasonable expectation of privacy retains some real meaning.

[42] City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

[43] See 132 S. Ct. 945, 948 (2012) (majority opinion); *id.* at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring in the judgment).