64 STAN. L. REV. ONLINE 117
April 12, 2012

SYMPOSIUM KEYNOTE[†]

THE DEAD PAST

Alex Kozinski*

I must start out with a confession: When it comes to technology, I'm what you might call a troglodyte. I don't own a Kindle or an iPad or an iPhone or a Blackberry. I don't have an avatar or even voicemail. I don't text.

I don't reject technology altogether: I do have a typewriter—an electric one, with a ball. But I do think that technology can be a dangerous thing because it changes the way we do things and the way we think about things; and sometimes it changes our own perception of who we are and what we're about. And by the time we realize it, we find we're living in a different world with different assumptions about such fundamental things as property and privacy and dignity. And by then, it's too late to turn back the clock.

When I think of new frontiers on the internet I'm reminded of a science fiction story I read in college by my favorite SciFi author, Isaac Asimov. It's called "The Dead Past," and it goes something like this: Scientists have invented a machine called a chronoscope that can be used to view any time in the past, anywhere in the world, but this technology is strictly regulated by the government. Historians try to get licenses to view ancient Carthage or Rome, but government bureaucrats churlishly deny most requests based on mundane considerations of cost and convenience. So a frustrated historian teams up with a frustrated physicist and a frustrated journalist and together they reverse-engineer the chronoscope. They are eventually apprehended, but by that time the journalist had sent the plans to half a dozen of his news outlets; the secret is out and can never be retrieved.

And there, in the closing pages of the story, Asimov explains why the government had been so secretive about this invention:

> When people think of the past, they think of it as dead, far away and gone, long ago. . . . [But] when did [the past] begin? A year ago? Five minutes ago? One second ago? Isn't it obvious that the past begins an instant ago? The dead past is just another name for the living present. What if you focus the chrono-

† 2012 Symposium: *The Privacy Paradox: Privacy and Its Conflicting Values*. Keynote delivered at Stanford Law School on February 3, 2012.

* Chief Judge, United States Court of Appeals for the Ninth Circuit.

> scope in the past of one-hundredth of a second ago? Aren't you watching the present? . . . . There will be no such thing as privacy. Every man, his own peeping Tom and there'll be no getting away from the watcher.

The story ends with the line that I've remembered ever since I first read it, maybe forty years ago: "You have created a new world among the three of you. I congratulate you. Happy goldfish bowl to you, to me, to everyone . . . ."

I have worried a good deal about that fish bowl over the years, and it seems pretty clear that it's getting smaller, and its walls are getting more transparent. To give just one example, the other day one of my sons sent me a link to a satellite picture of my house from Google Maps. You could not only see the house in pretty clear detail, but you could see who was home, from the two cars in the yard—my son's blue Subaru and my brother-in-law's gray Avalanche. I was very happy that I hadn't been taking one of my famous nude sun-baths on my patio.

I flew here today from Los Angeles. I drove to LAX, landed at San Jose Airport and a student drove me to Palo Alto. Who knows this? Big Brother knows. Why? Because I carried my cell phone, and who doesn't carry a cell phone nowadays? The cell phone logs in every few minutes to a nearby cell tower, so if you obtain the telephone company's records, it's pretty easy to piece together exactly where I've been all day. And, if you have the student's cell phone number, you'd also know how long we spent together and where we went.

Does the government obtain such records to check people's alibis in case they are suspected of crimes? You bet they do. In fact, if you left your phone at home that day, so there's no cookie-crumb trail to show you were somewhere else, prosecutors will argue that you not only committed the crime, but premeditated it as well—by leaving your cell phone at home so your steps couldn't be traced. China has taken this to another level: Earlier this year, Beijing officials announced that they intend to use cell phones to monitor the movements of twenty million residents—"to ease traffic and subway congestion."

But who needs cell phones? That's old technology. Someday soon they'll decide it's easier to watch all of us, all the time. If you think it won't happen, just look at Mexico: Last year, the city of Leon partnered with a biometrics firm to install iris scanners in public places from airports and police stations to stores and restaurants. The scanners will identify up to fifty people per minute, and will be used for both law enforcement and commercial purposes.

Speaking of phone data, remember the revelation in 2006 that the federal government persuaded phone companies to turn over the telephone records of millions of people who made or received calls from abroad? Whether it is a good thing or a bad thing that the government asked, and that the phone companies cooperated, is a matter about which people differ, and I will not express a view on it today. But I do want to point out that, as a matter of technology, such a request could not have been complied with twenty-five years earlier. Nor would it have done the government much good to receive such massive

data in what would have been, essentially, printed form. Where would the government have gotten the manpower to mine the data for any useful pattern? But with computers doing the heavy lifting, it's easy to sort and cross-check millions of records to see who's talking to whom and when.

As software has gotten more sophisticated, it has become not only quite feasible for phone companies to provide such information, but quite lucrative. In 2008 alone, Sprint "pinged" the real-time location of its cell phone subscribers over eight million times at the request of law enforcement. In fact, Sprint created a self-service website where police can check on the movements of any customer—for a fee. This practice was publicly disclosed—Congress had a hearing about it—and no one batted an eyelash. The idea that law enforcement can now ping your cell phone and find out exactly where you are at any time, with no probable cause and no judicial supervision, is greeted with a big collective yawn. In a Twitter world where people clamor for attention, having the police know your whereabouts just increases your fan base.

There is a subtler, and more important, point here than a mere lament about the dangers of technology: Twenty-five years earlier, it's highly unlikely that the government would have asked for such records and, had it done so, it's likely the telephone companies would've said no. Why? Because twenty-five years earlier both the government and the phone companies would probably have considered this information private and therefore beyond the reach of the government—at least without a warrant.

And this brings into focus a key issue in the law pertaining to privacy: Not everything an individual wishes to keep private is legally protected as such. The law, and particularly the Fourth Amendment, only protects those items as to which an individual has a legitimate expectation of privacy.

For example, if you have a conversation with someone behind closed doors, it's considered private; the government can't listen in without first obtaining a warrant and making a showing of probable cause. But if you have a conversation in a public place where it can be overheard by others, it's not protected. Similarly, if you keep your money at home in your mattress, the government can't break in to count it without making a proper showing. But, if you keep your money in a bank account, you disclose your financial information to the bank and can no longer claim it's private. The government will be able to obtain that information on a much lesser showing than probable cause, or perhaps no showing at all. What this means is that the degree of protection individuals have in their privacy depends a great deal on the degree of protection they themselves expect and preserve. To the degree that we ourselves act in ways that give up our privacy, the law will follow and give us less protection from government intrusion.

Let's take as an example the case of *Katz v. United States*, decided by the Supreme Court in 1967. Katz used a public phone in a phone booth to transact some illegal business; the conversation, or at least Katz's half of it, was captured by law enforcement officials who had placed a microphone and tape re-

corder on top of the booth. The Supreme Court held that this was a seizure of Katz's conversation and suppressed the evidence. The Supreme Court's reasoning was fairly straightforward: When two people speak face to face, and take precautions not to be overheard, their conversation is private. Why? Because they have a legitimate expectation of privacy. The situation is no different, the Court reasoned, when the two individuals are in different locations, connected by a telephone line. In such circumstances, individuals can reasonably expect that no one will tap the phone line, so if they take reasonable precautions to keep people from overhearing them while speaking on the phone, they can expect the law to keep their conversation private. Here, Katz was in a phone booth, a space that could be made private by closing the door, and thus he had taken reasonable precautions to keep his information private. The government could not invade that privacy.

Note that in reaching this conclusion, the Court was saying something about Katz's own conduct and expectations, but even more about the nature of telephone communications. It was generally understood in 1967 that a phone conversation is a private communication; the Court's judgment reflected a commonly accepted standard in our society. I wonder how the *Katz* case would have come out if it had been decided in 2011 rather than 1967.

To begin with, phone booths are a distant memory. If you can even find a public phone today, it's generally one of a block of phones all squeezed next to each other, and it's very difficult to keep others from overhearing. No one seems much bothered by this, which is why phone companies no longer invest in phone booths. Far worse, of course, is the ubiquitous use of cell phones. It's very difficult these days to visit a public place, such as an airport or supermarket, and *not* overhear somebody's cell phone conversation. People seem to lack the least compunction about discussing the most intimate subjects within full earshot of other people, often shouting so loudly that the phone seems superfluous.

It is still possible, of course, to keep phone conversations private, by using a cell phone in a protected location, or waiting to get home before making a call. But Fourth Amendment protections don't turn entirely on the conduct of any one individual; to a large extent they depend on whether we, as a society, treat something as private. If judges and justices, who are known to travel through airports and frequent supermarkets, determine that we, as a society, do not consider telephone conversations private, they may well conclude that individuals do not have *legitimate* expectations of privacy in such communications.

I'm not really worried that the Supreme Court is about to overrule *Katz v. United States*, in large part because our long-standing perception that telephone communications are private seems so far to have survived these recent developments. But this is a result of the fact that telephones came into common use at a time when we took privacy much more seriously than we do today. It's not at all clear that the same protective attitude will prevail as to new technologies.

I have some personal experience with this. About eleven years ago, right before 9/11, some of my colleagues and I discovered that the Administrative Office of the United States Courts—in other words, the bureaucrats in Washington who administer the federal judiciary—had installed monitors at our internet gateways, and these monitors were set to detect various types of communications: specifically when someone within the judiciary accessed internet porn and gambling sites. The monitoring had been implemented without approval of the judiciary's governing body, which is made up entirely of judges (as you would expect). The monitoring was discovered when the AO, as the Administrative Office is known, started sending out letters to various chief judges, attaching long print-outs of salacious web traffic and suggesting that the responsible employees be disciplined.

When this program was discovered, many of my colleagues—myself among them—were quite perturbed. As we saw it, the computer today had in many ways displaced the telephone as a means for people to conduct their personal business. You used to call the bank to check on your balance; now you do it online. You used to call home to see if your children were OK; now you use iHound to keep them on a short, digital leash. And so on. To be sure, the phone on your desk, just like your computer, is owned by your employer. But no one would even remotely consider listening in on the phone conversations of employees when they call home or the doctor's office. Surely, exactly the same logic applied to the office computer.

Many of my colleagues agreed and eventually the monitoring was stopped. But it didn't come without a big fight, and what I found surprising is how many judges took the position that employees had no legitimate expectation of privacy in communications conducted by means of government-owned computers. When I suggested to them that they couldn't listen in on employees' telephone conversations, the answer was that phones are different. Why are they different? Because our expectations of privacy about phones were shaped in a world where people used landlines and phone booths. And it was not just the judges. As part of my campaign to stop the monitoring, I wrote an opinion piece in the *Wall Street Journal*, disclosing the monitoring and suggesting it was an unjustified invasion of privacy. I received some 300 e-mails in response to that article. While most supported my view, a large number took the position that whoever owns the computer is entitled to limit its use, and also to monitor how it's being used.

A great deal of our loss of privacy is entirely consensual—we seem to revel in making public what was once considered private. I seldom watch television, but a while back I happened to be in the room when my sons were watching a show—I believe it was *Jerry Springer*. A man was telling Springer about how he had cheated on his wife with the wife's own sister. After he told his story, who should walk onto the set, but the man's wife. They proceeded to shout some unpleasant things at each other—she calling him names for being a cheat, he complaining that she was insufficiently attentive to his male libido.

Then who else should walk onstage? You guessed it, the perfidious sister. The three of them then started shouting unkind things to each other as Springer egged them on. The two women threw down. The studio audience ate it up, and presumably the audience at home did too because the show is still on the air.

There was a time, still within living memory, when people would be embarrassed to find themselves in the situation of the three people on the *Springer* show. Cheating has always been considered at least a foible, but doing it with your wife's sister was considered in truly bad taste. Moreover, the fallout from having such conduct discovered—the pain, the disappointment, the hurt feelings, the sense of betrayal, the rip in the social and family fabric—were sad and private things. Sometimes it became necessary to tell others, such as when the parties sought a divorce, but it would have been unthinkable to disclose such misconduct to one's friends and neighbors, much less to millions of viewers across the country. I felt a deep sense of shame to be a witness to it, not because I'm naive and don't know that such things do happen, but because I had been forced to witness something that should have been private. In an odd way, I felt my own privacy invaded.

Television at least has some inherent limits; presumably not everybody with a sordid personal story can get on *Jerry Springer*. But now even that weak restraint is gone. We live in the age of the blog, so anyone with a computer can present whatever thoughts he may have—no matter how trivial or distasteful—to the entire world. And people do, lots of them, so the internet is chock-full of personal diaries presenting the deep personal insights, philosophical ruminations, homilies, and sordid stories of an ever-growing number of people.

A while back, for example, the United States District Court for the District of Columbia saw the filing of a lawsuit titled *Steinbuch v. Cutler*. Steinbuch (a man) and Cutler (a woman) had been staffers for U.S. Senator Michael DeWine. They met after hours, had a few drinks and then went to her home and engaged in the type of activities that used to be considered private. The following day Cutler posted the following gem: "To answer The Question, no, RS and I did not fuck. (It is my 'week off,' if you recall.)" This, in my humble judgment, is already too much information. But the posting doesn't stop there—oh, no, it's just getting started. We learn, for example, that RS "[h]as a great ass," that he had two ejaculations, and that he likes spanking.

During the course of the succeeding two weeks, Cutler continued to see quite a bit of Steinbuch, both figuratively and literally. And she assiduously reported their activities to the world, along with those involving other men with whom she was having sexual relations, including some for money.

This puerile and narcissistic account was picked up by another, better-known Washington blog and, for reasons I have difficulty understanding, soon *tout-le-civilized-monde* was reading about Steinbuch and Cutler's sexual escapades. The upshot of all this was that Cutler lost her job with Sen. DeWine, but had no time to regret it because she soon got a six-figure book deal and a photo spread on Playboy.com. Meanwhile, Steinbuch brought his lawsuit, complain-

ing of—you guessed it—invasion of privacy and infliction of emotional distress. He cut and pasted every word of Cutler's blog into his complaint, which is where I read it.

There may only be a handful of people like Cutler and the people I saw on *Jerry Springer*—though it seems there is actually an endless supply of them. But we can all try to find comfort in thinking that these people are not like us—that they really are an aberration, representing a view of privacy and decorum that is quite different from that of ourselves and our friends and neighbors. But this is an illusion, because for every Jessica Cutler among us, there are the thousands or millions who are prepared to read their exhibitionistic writing and to watch the TV shows where they air their dirty laundry. By providing them an audience, we encourage others to engage in similar conduct, and we acquiesce in the erosion of privacy for all of us.

Blogs, incidentally, can be terrible offenders. To begin with, bloggers are the kind of people who start every morning thinking that the world is breathlessly waiting for their thoughts, so they must get on that computer and fill the screen with whatever pops into their heads—full-baked, half-baked, or (very frequently) unbaked. Take my office number for example: I wondered how it came to show up online, since our court takes some elaborate measures to hide information about the judges and their personal staff. For example, if you get a call from my office, you won't see my office number on caller ID. So how *did* my phone number get picked up by Google?

It turns out that in late September 2003, one of my former law clerks, and four of his law professor buddies, ran a blog with the tantalizing name *A Taxing Blog*. For what must have been three glorious weeks starting September 23, 2003, the blog was heavily populated with posts about Grover Norquist, Rush Limbaugh, Gov. Schwarzenegger, and other fascinating people and issues of tax policy. Then, suddenly, on October 16, a short message announced a hiatus while one of the bloggers works on what he calls "'tenurable activity' (i.e. traditional scholarship)," and no one has ever posted to that blog again.

But there the three-week tax-policy blog lives in hyperspace, where all the bots and crawlers can run across it. And if you look closely, you will see a link to the bio of one of the bloggers, and if you click on it, it opens a Word document with said bio, and deep within it, near the end, is a list of references, which includes their phone numbers, and of course, I'm on that list. And that's how my telephone number is now posted on the internet, and can never be taken back.

Finally, the internet is a cruel place. Who here doesn't remember when Lauren Caitlin Upton, better known as Miss Teen South Carolina, flubbed the answer to a question about why one-fifth of Americans can't locate the U.S. on a world map? We've all had bad days like that and, of course, she was an 18-year-old in a pressure-cooker situation. In an earlier era, her answer, such as it was, would have been heard and forgotten by the audience. But this is the era of YouTube, and so a fifty-second clip of her making a fool of herself has got-

ten over forty-nine million views—and that doesn't begin to count all the parodies of her that immediately sprung up, making her look even more foolish than she was.

Of course, that is one of the great dangers of the internet and particularly of Web 2.0: No matter how private, dangerous, hurtful, sensitive, or secret a piece of information may be, any fool with a computer and an internet connection—which means just about everybody—can post it online, never again to be private or secret. They say that removing something from the internet is about as easy as removing urine from a swimming pool, and that's pretty much the story. As soon as somebody posts an item, someone else picks it up and e-mails it to his friends, and friends of friends, and then bots and crawlers pick it up and the Wayback Machine makes sure the genie is never, ever to be stuffed back into the bottle.

Judges, legislators and law enforcement officials live in the real world. The opinions they write, the legislation they pass, the intrusions they dare engage in—all of these reflect an explicit or implicit judgment about the degree of privacy we can reasonably expect by living in our society. In a world where employers monitor the computer communications of their employees, law enforcement officers find it easy to demand that internet service providers give up information on the web-browsing habits of their subscribers. In a world where people post up-to-the-minute location information through Facebook Places or Foursquare, the police may feel justified in attaching a GPS to your car. In a world where people tweet about their sexual experiences and eager thousands read about them the morning after, it may well be reasonable for law enforcement, in pursuit of terrorists and criminals, to spy with high-powered binoculars through people's bedroom windows or put concealed cameras in public restrooms. In a world where you can listen to people shouting lurid descriptions of their gall-bladder operations into their cell phones, it may well be reasonable to ask telephone companies or even doctors for access to their customer records. If we the people don't consider our own privacy terribly valuable, we cannot count on government—with its many legitimate worries about lawbreaking and security—to guard it for us.

Which is to say that the concerns that have been raised about the erosion of our right to privacy are, indeed, legitimate, but misdirected. The danger here is not Big Brother; the government, and especially Congress, have been commendably restrained, all things considered. The danger comes from a different source altogether. In the immortal words of Pogo: "We have met the enemy and he is us."