Disappearing Phone Booths, Part II: A Perfect Storm for Privacy

May 23, 2012

I recently gave a speech entitled "Disappearing Phone Booths" – this is the second in a four-part series recapping the speech. Part I addressed the threat to privacy posed by new innovations *[1]. Part III will discuss* the harms caused by the loss of privacy *[2]. Part IV will explain* what's at stake if privacy continues down its collision course with obsolescence *[3]. A full version of the speech can be found* here *[4].*

There are four interrelated circumstances that amplify the consequences of the data collection that we subject ourselves to on a daily basis.

1. Digital ubiquity

These first of these four circumstances is digital ubiquity.

The digital technologies that collect data about us are unavoidable – they are ubiquitous. To disconnect from all of the services and technologies that collect personal, sensitive data about us would be to disconnect from society. The on-the-ground reality is that to “opt out” of the data collection, correlation, and/or use that takes place when we go about the activities described above would be analogous to “opting out” of electricity a mere thirty years ago. For most Americans, within the next two decades, just about every activity of daily life will be monitored to some degree or another. And while we could perhaps come up with some academic scenario in which this won’t be the case, the truth is, you’d have to be a hermit’s hermit to avoid it.

2. The increasing number of parties that take part in our daily transactions

This brings me to the second of our four circumstances. That today, third parties are involved in each of our transactions – our purchases, our visits to websites, our communications. They are involved in the most mundane, and the most sensitive, activities of our daily lives.

For example, when you visit a typical news site, your ISP as well as Twitter, Facebook, analytics providers, and dozens of ad networks all may know exactly which articles you have read. Your email provider technically has access to your email and your phone carrier knows everywhere you go and everywhere you’ve been. Credit card carriers know about your purchases and if you use a cloud-based service to write or share documents, then some company knows everything you write.

3. The commodification and monetization of data

And what about all of that data that these third party companies – the ones that facilitate, or maybe just latch on to, all of your activities – are seeing and collecting? Well, this brings us to our third circumstance: Data is a hot commodity and storing massive quantities of it is becoming cheaper with each passing day. Not only do companies facilitate many of our daily actions, they are *strongly* incentivized to monetize the information they obtain in doing so. They may sell this data, they may use this data for their own purposes, and they may hand this data over to our government – either as part of intelligence gathering or criminal investigations. Multinational companies may hand this data over to other governments as well.

Data is a hot commodity for companies *and* governments alike.

4. Woefully out-of-date privacy laws

And we now arrive at our fourth circumstance, and this is one I want to spend a bit more time talking about.

Our privacy laws, with regards to privacy vis-à-vis companies and privacy vis-à-vis our government, are woefully lacking.

A. Privacy vis-à-vis companies

Let's start with privacy vis-a-vis companies.

We do not have a baseline privacy law [5] in this country. We do have sectoral privacy laws – the Health Information Portability and Accountability Act, the Video Privacy Protection Act – but the next new phone, or the next new tablet, or the next new facial recognition device, or the next new drone – well, when these come into market, there's no evergreen law that provides a floor of protection for users, that governs the type of data companies can collect, the type of transparency or choice they have to offer consumers or, alternatively, how these companies can or cannot use the highly sensitive information they may end up storing. The White House has repeatedly [6] called [7] for such a baseline privacy law, and CDT has long argued that we need one sooner, not later.

But while we don't have a baseline consumer privacy law, we do have the Federal Trade Commission (FTC), which has the power to enforce against unfair and deceptive trade practices, including those relating to privacy. With respect to privacy, the FTC has largely focused their enforcement actions on what are called deceptive trade practices: that is, they'll bring a case against a company that violates one of its promises to users.

But it doesn't take the world's best general counsel to know that if your company is going to be held liable for promising something, then your best bet may be not to promise anything at all. So what we end up with are companies that write privacy polices that are simultaneously extraordinarily vague *and* extraordinarily long and legalistic. Many of them use a lot of words to say nothing.

In fact, some great researchers at Carnegie Mellon a few years ago conducted a study [8] to predict the cost, in terms of time and money, if the average American were to actually read every single privacy policy of every single web service that she used in a year. The numbers they calculated were just astounding. The average user would have to spend between *181 and 304 hours* each year reading privacy policies. Nationally, that sums to between *39 billion and 67 billion* hours a year. And if you translate that into economic terms, that is between *559 billion and 1.1 trillion dollars* of productivity that would be lost if we were all to read privacy policies like we are "supposed" to in order to make an informed choice about the sites and services we use. (Of course, it's not like reading vague and legalistic privacy policies actually gives most people that much usable information about what companies do with their data anyway!)

Now, while the FTC has been pretty clear that privacy policies are insufficient, while they have expended tremendous effort putting forth new model privacy frameworks [9] and have done some really great work in this regard, Congress has not really given them the power they need to enforce these new frameworks. So for the time being, we largely seem to be stuck in an old privacy policy paradigm.

This means that consumers today simply aren't provided with enough insight to make informed choices about how the data they share with third parties is being collected and used, even when such choices are available. On the web alone, only the savviest consumer will be able to successfully complete the obstacle course that is preventing online tracking. When it comes to protecting our privacy on our mobile devices, in our cars, on our streets, and yes, even in our homes – think about your phone tracking you from room to room or monitoring your heart rate as you sit and watch TV, we have little control, little power.

B. Privacy vis-à-vis government

Okay, so I've now talked about commercial privacy. What about privacy from our government?

The sad state of affairs is that when it comes to privacy, neither statutes nor case law offers great protection.

Statutes

Let's start with statutes. The primary statute governing government access to electronic information, both real-time interceptions and stored communications, is the Electronic Communications Privacy Act, or ECPA [10].

ECPA was passed in mid-October 1986 – when I was *three weeks old*.

I'll put that another way: I'm the same age as ECPA.

Needless to say, I like to think that I have aged more gracefully than ECPA has.

That's because ECPA, a strong law when it was passed 25 years ago, was created for a time when there was no such thing as a World Wide Web.

Let me offer one example of ECPA's less than graceful aging. When drafting ECPA, Congress wasn't sure how to treat email that was in storage with an email service provider. At the time, electronic storage was expensive, and email service providers routinely deleted email after 30 or 90 days. So Congress assumed that, if someone wanted to keep a copy of an email, they would download it onto their own computer or print it out; Congress felt that after a certain period of time, email left on the server would be the analog of abandoned property, in which the recipient had no privacy interest. And so Congress decided that after 180 days, email would no longer be protected by the warrant standard and instead would be available to the government with just a subpoena.

But today, most of us now save our emails indefinitely and we store them not on our hard drives but in the cloud, on the servers of our email providers. Of course we also store our calendars, photos, and a wealth of other sensitive, private data in the cloud. Any of this data stored on our laptops or in the confines of our homes requires a warrant for the government to seize it. Yet the same data, sitting in our private, password protected account with a service provider, is available to the government without a warrant under ECPA.

Other examples abound of how ECPA has not kept up with modern technology. The laws on the books, it turns out, offer us cold comfort when it comes to privacy from intrusion by our government.

Courts

So what about case law? Where our laws fail us, does the 4th Amendment not offer a sturdy floor of protection?

In an age, where, as I discussed earlier, third parties increasingly involve themselves in some of the most intimate aspects of our daily lives, the third-party doctrine (which states that when you convey information to a third party, you lose your expectation of privacy in that information) stands as a pretty impressive barrier to Fourth Amendment privacy protections for our private and sensitive information.

It's a situation exacerbated by the flimsy privacy policies that companies offer their users. Some courts have held that a company's Terms of Service agreements, by reserving all types of rights for the company to play around with user data, can destroy a user's reasonable expectation of privacy in her online activity; even the 6th Circuit Court, in its *Warshak* decision [11], a decision that was a big win for email privacy, held that "a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account."

In other words, when a company fails to offer users strong assurances that it takes steps to reduce the data it collects, accesses and/or uses, it not only obliterates users' privacy vis-à-vis itself, the company, it also may obliterate users' protections against government intrusions on their privacy. But, for the reasons discussed above, because of the incentive structures in place today, there's little reason to believe those privacy policies are going to improve on their own accord.

Fortunately, some are starting to question the wisdom of holding on too tightly to the third-party doctrine, recognizing that in today's age, it renders the Fourth Amendment not a floor built out of hearty oaks but one made of rotting pines, one that threatens to collapse on any who dare tread too heavily.

Indeed, in her concurrence [12] in *US V. Jones*, the recent GPS tracking case, Justice Sotomayor wrote that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

I would be remiss if I did not also at least briefly acknowledge the Supreme Court's 2001 decision in *Kyllo* [13], in which it suggested that police surveillance of the home using technologies "in general public use" does not violate a reasonable expectation of privacy and therefore would not require a warrant. The Court in *Kyllo* held that thermal imaging devices, the type of technology at issue in the case, were *not* "in general public use" and therefore their use by law enforcement did in fact necessitate a warrant. But eleven years later, such devices are available to you and to me for about $1,000 on Amazon [14], leaving open the question of whether or not police today need a warrant to use them.

Scalia wrote in *Kyllo* that in the home, "all details are intimate details, because the entire area is held safe from prying government eyes." But as technologies that are increasingly capable of discerning what we are doing in our own homes enter "general public use," Kyllo's own reasoning calls this assertion into question, setting the privacy protections we have long enjoyed in our own homes on a collision course with obsolescence.

So back to our four circumstances

Put these four circumstances together — (1) digital ubiquity, (2) the increasing number of parties that take part in our daily transactions, (3) the commodification and monetization of data, (4) and woefully out-of-date privacy law – and we have something of a perfect storm.

Yet the loss of privacy is not an inevitable cost of technological innovation. Instead, it has been the natural outgrowth of a policy framework, contextualized by business incentives that are not well aligned with protecting privacy, that has turned a blind eye to the foundational benefits that privacy offers us as citizens of a democracy and as consumers in a strong capitalist society.

Cutting off all data collection is not viable, but finding middle-ground legislative compromises that forestall persistent monitoring, and that prevent collection from morphing into surveillance, is absolutely necessary.

Links:
[1] https://www.cdt.org/blogs/erica-newland/2205disappearing-phone-booths-part-i-privacy-and-new-technologies
[2] https://www.cdt.org/blogs/erica-newland/2405disappearing-phone-booths-part-iii-privacy-harms
[3] https://www.cdt.org/blogs/erica-newland/2505disappearing-phone-booths-part-iv-what-if-privacy-becomes-obsolete
[4] https://www.cdt.org/files/pdfs/Privacy-In-Digital-Age.pdf
[5] https://www.cdt.org/issue/baseline-privacy-legislation
[6] https://www.cdt.org/blogs/aaron-brauer-rieke/momentum-builds-obama-administration-urges-congress-enact-privacy-legislati
[7] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[8] http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf
[9] http://www.ftc.gov/opa/2012/03/privacyframework.shtm
[10] https://www.cdt.org/issue/wiretap-ecpa
[11] http://caselaw.findlaw.com/us-6th-circuit/1548071.html
[12] http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf
[13] http://www.law.cornell.edu/supct/html/99-8508.ZS.html
[14] http://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=thermal+imaging