KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

DISAPPEARING PHONE BOOTHS: PRIVACY IN THE DIGITAL AGE

May 2012

CDT Senior Policy Analyst Erica Newland gave a version of this talk to DC Superior Court judges in May 2012. This speech, which draws on past CDT testimony and work, makes the case that in the context of a legal framework that has turned a blind-eye to the foundational benefits of privacy, changes in technology are threatening this civil liberty with obsolescence.

I. Introduction

I want to thank you for asking me to speak today. It's an honor to be invited to talk to such distinguished guests about technology and privacy and I hope my remarks will offer, at the very least, some food for thought.

I'm going to begin with a quick overview of what I will be talking about this afternoon, and then I'll dive right into the meat of it.

First, I'm going to discuss what we are fighting for when we talk about protecting privacy in a digital age: that is, how new technologies are rapidly eroding privacy protections and privacy assurances that we have long taken for granted.

I will then explain why the confluence of at least four circumstances – (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of parties that take part in our daily transactions, (3) the commodification and monetization of data, (4) and woefully out-of-date privacy laws – creates something of a perfect storm, leaving us as a nation poorly equipped, in our present state, to preserve any measure of a right to privacy. That is to say, I will be arguing that technology and policy both play powerful roles in framing what is possible and how we live our lives, and that changes in technology must be accompanied by changes to policy.

Then, I will address the question that I get asked every time I talk about privacy: Why do we care? What's the harm?

And finally, I'll close with a few thoughts about where I think some of the most vexing challenges to privacy will arise over the next decade.

II. How technology is fundamentally challenging our notions of privacy

Any discussion of privacy in the 21st century has to begin with a step back and a look around. When we do that, we can't help but realize that we live in a world where *everything* we do will soon be observable – by some party or another.

That is to say, as a society, there is an incredible amount that we have to gain from innovative new technologies – but, if we go about it wrong, there is also an incredible amount that we have to lose.

What is it that we have to lose?

Let's start with our right to read newspapers unnoticed: the right to throw a quarter into the vending box and grab a copy, to privately choose which articles we want to peruse and which one we don't. This right gradually slips away each time a local paper shutters its presses and halts print distribution, leaving us to read online, where our clicks and page views are tracked and companies are doing everything in their power to associate those clicks and page views with our names, addresses, demographic information, and other personal information.

Now I'm the first to volunteer that I have real soft spot for online newspapers. I'm originally from Auburn, Alabama and I began reading the *New York Times* – the paper copy – probably as a nine- or ten-year-old. Then, sometime around 8th grade, the *Times* stopped making home deliveries in my town. But by going online I was able to get a daily fix of news about the world, news that wasn't filtered through the small, local paper. I strongly believe I would have led a very different life had I not had that access to the *Times*, or a similar news outlet, online.

But, that doesn't change the fact that by consuming my news online, I am opening myself up to those who are trying to create a dossier of everything I read.

What else do we have to lose?

- The right to read a book unnoticed, especially as some titles are now published only as e-books.

- The right to drive unnoticed – whether it's because we have GPS built into our cars or because our phones, which are basically homing devices, are sitting with us in our cars.

- The right to use the restroom unnoticed. My colleague recently shared the following haiku with a few of us at the office:

  From the bathroom stall
  an unmistakable sound
  an iPhone typing.

  Indeed, 75% of people have taken their mobile devices into the bathroom with them, and apps on these devices are able to turn on our microphones and our cameras without our permission or without really notifying us. I have a friend who calls his iPad his "thousand-dollar bathroom entertainment system," but it's not inconceivable that he's sharing another type of entertainment with prying eyes.

What else do we have to lose?

- The right to make purchases unnoticed, to sit in our living rooms and watch TV unnoticed, and to get milk out of the refrigerator unnoticed.

- We also lose the right to send letters unnoticed. One of the conversations we have not been having as the US Postal Service faces death's door is the conversation about how much privacy protection postal mail receives compared to electronic mail. Given the state of our laws, the decline of postal mail is also the decline of mail privacy.

- Even our right to walk down the street unnoticed is being eroded. In some cases, this is because we are beaming our location information to our smartphones and their apps – telling them exactly where we are and, often, what we are doing at any moment in time. In other cases, we lose the right to walk down the street unnoticed because of rapidly improving facial recognition technology that is paired with closed-circuit televisions or drones – like the types that will be deployed for surveillance during the London Olympics this summer.

- And how about the right to have our hearts beat in our chests unnoticed? We may soon have phones that not only turn on our cameras and microphones, but that can monitor our heart rates and blood sugar levels. There are some really exciting healthcare applications of technology like this, but this is also data that never before has been so regularly transmitted to a third party.

This list could stretch on for pages. Needless to say, the privacy of the most mundane, and sensitive, of our activities is rapidly eroding as these activities move into the networked world.

III. The perfect storm

This laundry list probably prompts a number of questions. Among them:

- Can't I just purchase a paperback with cash and call it a day?
- Are these really rights anyway?
- To whom have we lost our privacy?
- And what's the harm?

To answer questions like these, I need to talk about four really crucial and interrelated circumstances that amplify the consequences of the data collection that we subject ourselves to on a daily basis.

A. 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.

B. 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.

C. 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.

D. 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.

1. Privacy vis-à-vis companies

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

We do not have a baseline privacy law 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 called 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 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 and have done some really great work in this regard, Congress has not really given them the enforcement 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.

2. *Privacy vis-à-vis government*

Ok, 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.

a. 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.

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.

b. 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, 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 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*, 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, 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.

E. 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, is 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.

IV. What's the harm?

Now if you haven't noticed, I've kind of been dancing around the million dollar question here (I wish I could do a pirouette on stage to demonstrate, but sadly I'm not that talented). Why should we care about privacy? Or as some would put it, what's the harm? Why am I up here sounding worried that some corporate conglomerate may know what I did or where I went last night? Who really cares?

There are a number of different types of harms that CDT often thinks about. Here, I want to focus on four of them.

A. Data breach

One harm, and this is a harm that often catches Congressional attention, is the increased risk of security breaches and with those, identity theft, that data collection and storage creates. Sony, in April 2011, experienced a massive security breach, one in which approximately 100 million records were leaked. Many of these records consisted of credit card data from 2007 that the company no longer used and no longer needed. This begged an important question: why was Sony even keeping such data in the first place? Sony would have been in far less trouble had it practiced data minimization – had it only kept the data it actually needed. But in a world in which many believe that more data may some day mean more dollars, few companies seem keen on the whole data minimization idea.

B. Innovation

There is some irony in this, because one of the other privacy harms we often talk about is the real risk to innovation. While few consumers fully grasp the extent of this large and growing data trade, numerous independent studies have shown that practices such as deep packet inspection, online behavioral advertising, and the merger of online and offline consumer data into user profiles all undermine consumer trust. I saw one study recently that found that adoption of mobile shopping is slower than would have been anticipated, largely because of consumer concerns about the privacy and security of their information.

Trust is the difference between innovation that delights us and innovation that deeply discomforts us.

In short, trust underpins and fuels innovation. If consumers are unable to trust this increasingly complex network of innovative services, innovation suffers. *Privacy is about securing user rights.* But it is also about building trust in the marketplace in hopes of protecting and accelerating the innovation we see today.

Innovation and privacy are not necessarily incompatible paths – they can be intertwined paths as well.

C. Government access

Still other times, when we talk about harms, we talk about access to information by the government. As I discussed earlier, data stored by third parties is data the government can dip its fingers into pretty easily: the hotels at which we stay, the websites we browse, the emails we send, the places we shop. As Justice Sotomayor said in her concurrence in *US v Jones*:

> "The government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring - by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government in its unfettered discretion, chooses to track - may 'alter the relationship between citizen and government in a way that inimical to democratic society.'"

It's a warning that I think is relevant far beyond the limited case of GPS tracking.

D. Privacy allows us enjoy our rights to liberty

And this brings me to a point about liberty. And here, I want to read from President Obama's forward to the White House privacy report:

> "Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers. At the same time, we set up a postal system to enable citizens all over the new nation to engage in commerce and political discourse. Soon after, Congress made it a crime to invade the privacy of the mails."

He continues: "Citizens who feel protected from misuse of their personal information feel free to engage in commerce, to participate in the political process, or to seek needed health care."

"This," Obama adds, "is why the Supreme Court has protected anonymous political speech, the same right exercised by the pamphleteers of the early Republic and today's bloggers."

Privacy enables us to exercise liberty and to enjoy our rights to liberty. It empowers us to feel that we can speak freely, associate freely, and access information freely. And to me, the threat to that liberty is the most disconcerting harm of all.

V. Concluding thoughts

So where does all of this leave us?

In that lodestar privacy case, *Katz v United States*, Justice Stewart wrote:

> "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll 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 communications."

Mr. Katz closed the door to a phone booth, demonstrating that he expected the contents of his conversation would stay private. And, as Justice Harlan wrote in his now famous concurrence, that desire for privacy was one that society was prepared to recognize.

Today our phone booths are disappearing.

Yes, I mean that literally. Phone booths are hard to find these days.

But I also mean that figuratively. A key challenge for Congress and for our Courts over the next decade will be one of finding those metaphorical phone booths, those safe spaces or times or situations in which we may, to paraphrase Justice Stewart, be "entitled to assume that the words" we utter and the things we do "will not be broadcast to the world."

As I talked about above, we now live in a world in which technology has weakened the constitutional protections against government intrusion into that sturdiest of phone booths, the home.

And as I've discussed at greater length, we also live in a world in which digital third parties, typically companies, involve themselves in the huge majority of our actions and our communications, of our searches for information, of our speech, of our efforts to associate. If we want to communicate with friends, search for jobs, read the news, watch TV, seek out health information, or organize political protests, we have little choice but to so-called "volunteer" this information not only to third parties, but to third parties that have the technical capacity, have reserved the rights, and may regularly exercise those rights, to monitor or use that information.

Where these third parties have free reign to collect and use this data however they so desire, and where our laws and jurisprudence similarly do little to limit government access to the data they hold, those metaphorical phone booths will become increasingly difficult, even impossible, to find.

I'm not one to believe that technology has to kill privacy. But it will if we let it.