DATA (/DATA)

Rethinking Privacy: Though Technology has Outpaced Policy, That's No Reason to Give Up

Privacy is almost universally valued by humanity, but technology is advancing so quickly that people haven't had time to settle on a useful definition for the word -- let alone a solution that everyone can live with.

BY COLIN WOOD (HTTP://WWW.GOVTECH.COM/AUTHORS/COLIN-WOOD.HTML) / JUNE 2, 2014

Rebecca Jeschke, a digital rights analyst for the Electronic Frontier Foundation, says that privacy isn't dead; that's a cop-out. "Privacy is really important and it's deeply contextual, and I think anyone who says that privacy is dead has an agenda, and it's only dead if we say it is." JESSICA MULHOLLAND/E.REPUBLIC (HTTP://EREPUBLIC.SMUGMUG.COM)

Privacy isn't dead, it's just going through an identity crisis. As policymakers struggle to define a meaningful role for themselves in one of the most contentious areas of American politics, the advancement of digital technologies only makes the issue loom larger. Each convenient new feature developed by Apple, Google or Facebook fuels a public conversation about the border between cutting-edge and creepy. Privacy is almost universally valued by humanity, but technology is advancing so quickly that people haven't even had time to settle on a useful definition for the word, let alone a solution that everyone can live with.

The state of free speech in America at any point in modern history can be fairly accurately sampled by looking at what live performance artists, particularly stand-up comedians, are allowed to do and say. From 1961 until his death in 1966, Lenny Bruce was repeatedly arrested for the obscenities he used on stage, including one arrest directly following his use of the Yiddish word "schmuck." The Lenny Bruce era demonstrated a nation's lofty but fading sense of propriety, yet it also demonstrated the relatively high level of privacy Americans enjoyed. Pretty much the only way to have one's privacy invaded in those days was to get arrested for something, a truth made evident when you consider that the president was rumored to have had a secret affair with the nation's most iconic sexpot. Today, the president can't even sneak a Marlboro without making the front page.

From 1966 until 2005, which is, incidentally, the same period that spanned Richard Pryor's legendary career, America experienced a golden age of privacy. The puritanical and somewhat naïve outlook of the 1950s was quickly fading in the late 1960s, and consequently, people no longer cared as much about what others did or said. And even better for privacy, today's digital technologies hadn't yet arrived en masse. It wasn't until sometime after the year 2000 that everyone began carrying their own personal "gotcha" devices.

And people did start getting got. In 2006, cellphone video captured actor Michael Richards, of Seinfeld fame, in a racist, profanity-laced outburst aimed at a black audience member during a set in West Hollywood, Calif. Video of the incident posted to YouTube turned what would have been a single bizarre occurrence into an ongoing national discussion as the scene was viewed over and over again. Had that same incident happened 10 or even five years earlier, before most people had smartphones, it probably would have become urban legend or perhaps even gone completely ignored by the public. The Richards incident was the start of a new phenomenon in the comedy world and the world in general.

Suddenly what was once considered a quasi-private setting was compromised by the power and omnipresence of the smartphone. But it's not just celebrities who get busted now, and it's not just comedy clubs where the busting happens — it can happen to anyone, anywhere.

The concept of privacy simply covers a lot of territory, and that's part of the problem, said Paul Schwartz, professor and co-director at the Berkeley Center for Law and Technology. "It can mean everything and it can mean nothing," he explained. "That can have some dangerous consequences."

For instance, privacy can involve the right to make intimate decisions, or maintaining control of sensitive information, or deciding when and how to share data. What's more, the environment is getting more complex. As digital sensors and cameras become cheaper, an emerging Internet of Things is transforming an issue that continues to derive context from a bygone era.

The tools for controlling privacy in years past were eyes, ears and lips, but the dynamic has since changed radically. "We lived in neighborhoods and you knew certain things about people in your neighborhood, and it was a relatively static world in that regard," Schwartz said. "Your parents would tell you to draw the blinds, or you would gossip about people and share information about neighbors."

Now Internet-enabled smartphones are to the privacy discussion what shoulder-fired rocket launchers are to the Second Amendment debate. But when it comes to privacy, public mindset and government policy haven't caught up to reality.

One reason policymakers are struggling so much with emerging privacy issues is that the issues themselves are simply unprecedented. "It's a huge challenge, because it becomes what lawyers call 'a normative issue,'" Schwartz said. Researchers can poll people about new technologies or devices, or developers can make guesses about how people will react to the introduction of new products, but there's no way to establish a reliable plan for technologies that have never been used before.

"A term that you frequently hear is that people feel something is 'creepy,'" he added. "People in industry will talk about avoiding 'creeping out' your customers or you get the privacy backlash." Even the most competent technology companies don't know where

REDEFINING NORMAL

California Lt. Gov. Gavin Newsom is of the mind that yes, privacy as we've known it is dead in today's more transparent world.

"We're going to have to reconcile that the two things need to go together: privacy and transparency," he told Government Technology late last year.

Mindlessly downloading an app onto a smartphone, like so many of us do, is a de facto forfeit of vast amounts of personal information. Newsom blames a lack of transparency about what we're giving away for the phenomenon.

"We have to have more hyper-transparency in a world where privacy is being challenged by these tools of technology," he said.

He went on to predict that expectations of privacy will continue to evolve, and things that might have previously been perceived as shocking will soon be accepted as normal.

to draw the line sometimes, because they're doing something new. Now that everyone has spying tools, everyone is trying to figure out, together, how they should be used.

For practical purposes, Schwartz said, it is not wise to act as though privacy is dead, because the stakes are high. Vigilance is needed, he said, because the victim of ineffective privacy legislation is the public.

The National Do Not Call Registry is an example of privacy legislation done right, Schwartz said. "That is one of the most successful privacy laws of the last 15 years," he said. "It's viewed as a privacy issue, but what you can really view it as is a 'don't bug me when I'm eating dinner' law. You don't care that you're known as a person who might contribute to a certain charity. What you really don't want is to be interrupted. It's kind of a tax on your time. So privacy, we find out, is sometimes just having control of your time or limiting access to yourself in certain contexts."

But other times legislation doesn't work as intended or becomes out of date. The Song-Beverly Credit Card Act of 1971 protects people's privacy by limiting the amount of data that can be collected about them when they buy something. Essentially, the act prohibits the

collection and storage of a customer's personally identifiable information as a condition of sale.

In 2011, the California Supreme Court ruled that the act prohibited merchants from collecting customers' ZIP codes at checkout. The problem, Schwartz said, is that the ruling closed the door on the security benefits of asking for a ZIP code in certain settings where it makes sense to do that, like at a gas station or online. The law was eventually adjusted because those instances were determined to be exceptions outside the spirit of the act, but "there was an amazing amount of litigation," Schwartz said, "to figure out all the various instances in which additional information should or should not be permitted."

For the most part, policymakers don't understand modern technology very well, Schwartz contends, and they're not anticipating technological disruptions in society. There should be groups dedicated to imagining all the various scenarios that could arrive, he said, as is done in the intelligence community, because there will be disruptions and privacy is worth safeguarding.

Fred Cate, professor at the Maurer School of Law at Indiana University, isn't surprised that legislators and other policymakers don't have a good grasp on the tech industry's latest and greatest. "I mean, who really does have a grip on emerging technologies and the issues they present?" he said.

And he agreed that the lack of a good single definition for privacy is holding back progress. "[Legislators] say, 'Privacy is a very personal concept, and it's really up to how the individual sees it,'" said Cate, who researches privacy, cybersecurity and health information. "You can't regulate anything if you say the thing that we're regulating is up to how the individual sees it."

The lack of clear objectives on privacy leads to ineffective policy, Cate said. He points to examples like the Children's Online Privacy Protection Act, which requires websites with adult content to make users enter birthdates before proceeding. Rather than protecting children online, the law does little more than punt privacy responsibility to the consumer — a common theme of tech-driven privacy legislation.

"Another good example is security breach notification laws," Cate said. "We don't have any idea what to do in response to breached information. So what do we do? We say, 'Let's just tell everybody about it. They're not going to know what to do either, but we'll all be worried and ignorant together.'"

One of the worst punts, Cate said, are terms of service agreements. "Every time you update your iPhone there are 65 screens of policy to read," he said. "But the average consumer isn't a privacy expert, nor does he have the legal background to soundly evaluate if the agreement is fair."

If privacy means controlling data, then privacy is indeed dead, Cate said. But it should be possible to protect citizens from the harmful misuse of their data. He argues that companies need to make service agreements clear to consumers, and those companies should be held accountable when harmful misuse of data occurs.

Another problem is that data-oriented wrongdoing doesn't have its own definition of harm — it just piggybacks on existing laws, Cate said. Someone who stalks another person using their data is subject to prosecution under stalking laws. Someone who defrauds another person using their data is subject to punishment under fraud laws. Data privacy law itself doesn't really exist in any comprehensive sense.

"I don't think our aspirations have caught up to where our technologies are now," he said. "To be honest, most of the so-called privacy legislation we've seen in recent years I think shows a lack of ambition."

Don't tell Rebecca Jeschke that privacy is dead. Jeschke is a digital rights analyst for the Electronic Frontier Foundation, a civil rights nonprofit focusing on the digital world. That's a cop-out, she said.

"There are studies about how kids, who supposedly don't care about privacy, code their Facebook messages to make sure no one they don't want to see what they're doing sees what they're doing," Jeschke said. "Privacy is really important and it's deeply contextual, and I think anyone who says that privacy is dead has an agenda, and it's only dead if we say it is."

She said the current environment often forces consumers to give up personal data to get something they want. "I don't enjoy Facebook, and yet I can't really not be on it, or I'm not going to see pictures of my nieces and nephews," she said. "Do I really want this app or not? I really don't want to read this 25-page terms of service, but I want that functionality."

Similarly, when Jeschke scans her transit card to board various forms of public transit in the San Francisco Bay Area, she's giving up a little privacy because she's trackable, and in exchange she gets the conveniences and discounts the technology brings. "One of the things that infuriates me is that I have to make that choice between convenience and privacy, when you could use encryption on that card and give me both," she said.

Rarely do consumers understand the ramifications of the privacy trade-offs they're making, Jeschke added. "Transparency is only one level of it. Then you need to make sure people know what that means."

As consumers become more sensitive to privacy threats, she said there's a great opportunity in the market for technology companies that consider privacy from the beginning. "We're trying to encourage developers to think about what they would want as a customer instead of what makes it easier for them as a software creator."

Peter Swire was President Clinton's chief counselor on privacy, he's worked under President Obama on privacy issues, and when the NSA domestic surveillance scandal hit, he was one of five privacy experts who wrote The NSA Report: Liberty and Security in a Changing World. He said policymakers can't throw in the towel on privacy.

"In every decade, people have written that privacy is dying," Swire said. "In most ways, though, privacy is a bigger issue today than it's ever been."

Swire pointed out that the number of privacy and security rules has skyrocketed in recent years to keep up with the explosion of data generation and collection. In May 2013, IBM reported that 90 percent of all data in existence had been generated in the previous two years, and the marketplace reflects that.

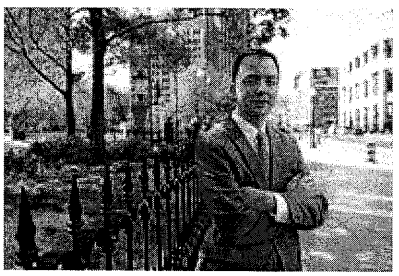
There's still data that needs sound national standards of control, just as the Health Insurance Portability and Accountability Act created national standards for medical data, he said.

"The people who think privacy is dead tend to think that privacy is a lost cause," Swire said. "My response is that we still need to govern the data carefully or else identity fraud will flourish."

Colin Wood (http://www.govtech.com/authors/Colin-Wood.html) | Staff Writer

Colin has been writing for *Government Technology* since 2010. He lives in Seattle with his wife and their dog. He can be reached at cwood@govtech.com and on Google+ (https://plus.google.com/u/0/117086278388898679660/?rel=author).

RELATED STORIES



(http://www.govtech.com/state/Rise-of-the-Chief-Privacy-

Rise of the Chief Privacy Officer (http://www.govtech.com/state/Rise-of-the-Chief-Privacy-Officer.html)

(/subscribe?promo_code=Story)

Free subscription to Government Technology

(/subscribe?promo_code=Story)

ADVERTISEMENT