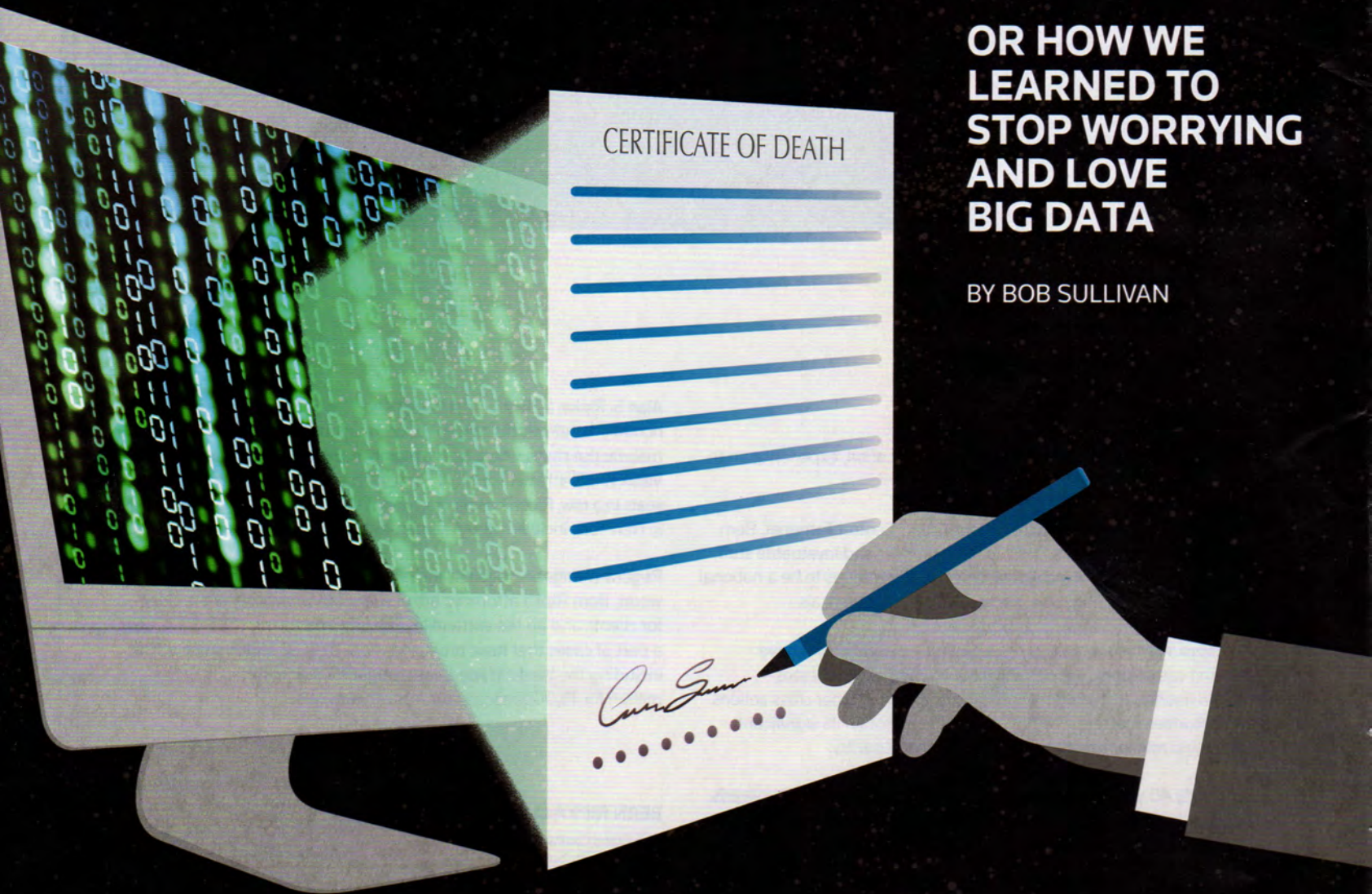
IS PRIVACY DEAD?

OR HOW WE LEARNED TO STOP WORRYING AND LOVE BIG DATA

BY BOB SULLIVAN



LET'S PLAY A GAME. YOU'RE A CORONER, and your job is to sign the death certificate for privacy. What year do you write on the form?

Maybe it's 2015, when the following who's who list of government and private organizations confirmed they'd been hacked or dealt with the repercussions of recent hacks: the Ashley Madison website, Premera Blue Cross, Anthem, the U.S. Office of Personnel Management, the State Department, the Pentagon and the White House.

How about the Sony hack of 2014 or the Target hack of 2013? Or that same year, when Edward Snowden told the world that the U.S. government was collecting data on virtually every phone call and Internet click?

There's 2007, when Apple's iPhone started the smartphone revolution, leading to the placement of easily tracked devices in almost everyone's pocket or purse. Or perhaps you'd reach back further, to 2004, when Facebook opened its doors and invited everyone to do the same. Or back to 1995 when Internet-tracking cookies were first deployed.

Or maybe, just maybe, you'd crumple up the form and declare, Mark Twain-style, that reports of privacy's demise have been greatly exaggerated.

"Privacy is not dead, but it will be conceived of differently," says Lisa Sotto, a cybersecurity and privacy lawyer at Hunton & Williams. "Being in a state of constant observation will be the new normal. Everyone will come to expect it whether at work or at play."

Most of the electronic blips that make people pop up on the grid are well known: drive through a toll booth, send an e-mail, make a credit card purchase. Some are less well known: turn down the thermostat (the Smart Grid knows), pass by a retail store with your cellphone (it's being tracked), walk near a protest at a park (it's being filmed by low-flying aircraft).

"I don't think there's any doubt that more information is being gathered on ordinary people than ever before both through commercial entities and by governments," says Catherine Crump, a Berkeley assistant clinical law professor and former ACLU lawyer, who has repeatedly sued the U.S. government over surveillance issues. "No one has figured out how to stop it."

Most consumers find all of the attention a little spooky. A recent Pew survey reveals that nine out of 10 people feel that privacy is important, but fewer than one in 10 feels that either the government or corporations are in a position to preserve that privacy. As a result, Pew says, a "cloud of data insecurity" looms over Americans' daily lives.

"People feel helpless," says Dan Solove, a privacy law professor at George Washington University. "We have a world where people lack the ability to manage the information that is collected about them ... and how it is used."

In a world where everything from toasters to thermostats snitch on your personal habits, it turns out that both George Orwell and George Jetson were right. We've got plenty of futuristic gadgets, but they're all watching us.

Jane, stop this crazy thing.

ONLY A FEW YEARS AGO, THE NOTION THAT every phone line could be tapped was the stuff of paranoid fantasy. Who would have time to listen to all those chats, let alone the ability to store all the files? Today, storage costs are trivial and computers do the listening. The NSA's Utah Data Center and its estimated 10,000 racks of servers, which can each hold a petabyte of data (a million gigs), may very well be able to store the audio from every phone call ever made—if *Forbes*' estimates on the center are to be believed. And thanks to constantly improving media-processing software, no one needs to listen to all those conversations, or watch all the recorded video from all those closed-circuit TV cameras around the planet. Faces and words can be plucked out of the mass of data.

After Snowden went public, in fact, the U.S. government responded with its version of the if-a-tree-falls-in-the-forest story. If a computer sees you do something and collects data about it, but no human ever looks at that data, were you really observed? Similarly, if large corporations maintain huge amounts of information on you, but anonymizes the data, were you really tracked?

"My viewpoint is that collection is going to happen," says Chris Wolf, a privacy and data security lawyer with Hogan Lovells in Washington, D.C. "The far more important issue is: How is data used? What rules do the stewards have to follow? Ultimately, that is what will affect individuals. There's going to have to be many more stewards of the data to make sure it's used properly."

Twenty years ago, stewards would have included the credit bureaus, the department of motor vehicles, the Internal Revenue Service, and maybe your employer. Today everyone from your favorite restaurant to the local dollar store can be a data steward capable of losing or abusing your personally identifiable information.

Unfortunately, outside of a few sector-specific areas, such as health and credit data, U.S. privacy laws are helplessly old. How old? The Electronic Communications Privacy Act was passed in 1986.

"It's extremely frustrating that the electronic privacy law in this country doesn't even reference cellphones," Crump says.

So what's the solution? "Right now, and for the last 10 years or so, we have been moving toward more and more laws that deal with pieces of the puzzle: industry-specific or practice-specific," says Kirk J. Nahra, a health care attorney with Wiley Rein in Washington, D.C.

Such rules would respect context: Data collected by health care providers could be liberally used while delivering health care, but other rules would kick in when a firm wants to use that data for marketing.

"It is a more reasonable and practical approach, focusing on use and harms as opposed to trying to boil the ocean and regulate everything," says Wolf, who is also a founder of the thinktank Future of Privacy Forum.

Whenever the privacy discussion turns to use, it also pivots to the issue of consumer choice. Some companies take a position that they can use whatever data they have however they wish as long as they obtain consumers' consent. Consumers, however, are notoriously bad at protecting themselves. Who reads the fine print of online agreements? Some consumers are already agreeing to let health and life insurance companies measure, through various gadgets, the number of steps they take each day, all for the promise of a discount. When economic pressure is applied to privacy decisions, is it really a choice?

"There are lots of people who generally think consent in most situations is kind of pointless," Nahra says. "That leads me to think we should have more laws and rules that tell companies what they can and can't do, independent of any consent."

Besides, says Crump, the battle between privacy advocates and data collectors is hardly a fair fight, since most of the data collection is done in secret. When Crump filed a Freedom of Information Act request through the ACLU about the Department of Justice's use of cellphone location records, federal law dictated she get a response within 20 days. It took seven years and a lawsuit to get answers.

"By its very nature, surveillance is covert, so it's very difficult to see the uses, let alone abuses, of data," she says.

THEN THERE ARE THE CRIMINALS.

All the rules in the world don't matter to hackers. Once all the data is collected, even if honest companies and well-meaning governments behave, the potential for criminals to exploit it is immense. The FBI says that in one recent 12-month span, criminals stole 500 million financial records.

"When it comes to cybersecurity, we are not in a good place," Sotto says. "We need new thinking on cyberthreats. We are no longer thinking in terms of keeping intruders out; we are thinking about identifying them once they are in. We now know it's nearly impossible to keep them out."

More, consumers whose personal information is hacked and exploited because of their relationship with a company must prove they suffered a loss in order to get any kind of restitution. Inconvenience doesn't cut it.

That was the hurdle Vincent Esades had to jump. An antitrust and consumer attorney with Heins Mills & Olson in Minneapolis, Esades led a class action lawsuit against Target after it was hacked in 2013. Esades managed to defeat a motion to dismiss the case by piling up anecdotes showing that Target victims suffered real damage. One woman said the debit card she uses to receive child-support payments was drained of $3,600 and then frozen, leaving her with no way to support her son. Another was locked out of her debit card for nearly a month while her bank investigated fraudulent charges, leaving her unable to pay bills, which led to a pile of late fees. A third said his Target card was drained of value and then a series of fraudulent inquiries were made against his credit, lowering his credit score.

"These were really impactful stories. It resonated with the judge," Esades says. He and Target settled the case for $10 million.

But that's the exception. Proving harm in privacy-related cases is notoriously difficult, particularly when the harm might come many years into the future—as can be the case with a leaked Social Security number. Alessandro Acquisti, a privacy economics expert at Carnegie Mellon University, talks about the challenge of making good cost-benefit decisions in privacy transactions. When you give a supermarket your phone number for a loyalty card, the benefit is obvious—maybe 50 cents off a gallon of ice cream. But what is the cost? Is it junk mail? Spam? Being hacked and drained of $3,600 from your debit card?

There is one sliver of good news. In the Internet's early days, companies routinely lost data on consumers in complete secrecy. Then in 2002, California passed its data-breach notification rule, which led directly to revelations that data broker ChoicePoint had been hacked and lost dossiers on about 150,000 Americans. ChoicePoint became viewed as the digital age's first privacy villain. An avalanche of news about hacking followed. The Snowden revelations had the same effect on government data collection.

Before ChoicePoint, Wolf says, his firm had only a few privacy expert lawyers. Now it has 27.

PRIVACY CONCERNS WILL ONLY GET BIGGER, while big data concerns will only get more complex. In part because of the Snowden fallout, nation-states are racing to recapture control over such data. In 2014, Russia passed a "data localization" law that will require all information gathered about its citizens to be stored on servers only within Russia—a regulation that will make it hard for companies like Google to operate there.

"It's an absolute nightmare dealing with cross-border transfer restrictions," says Sotto. "It takes the 'world' out of the World Wide Web. ... But data is increasingly viewed as currency, and we need to figure out how to put rules around the data that won't conflict with local expectations but will cater to global needs."

Experts caution that legal solutions to privacy issues will not arrive for years or decades. In the future, data may be considered the toxic chemical of the digital age, with experts only now beginning to figure out how to safely use, store and dispose of it.

"It's a little like the discussion about environmental law. In the 1960s people were talking about clean air and water. Now people are talking about privacy solutions," Wolf says. "This will be a lengthy process. We might be talking about the Privacy Act of 2020 as a new baseline."

Or we might not be talking at all. For fear of who's listening. SL