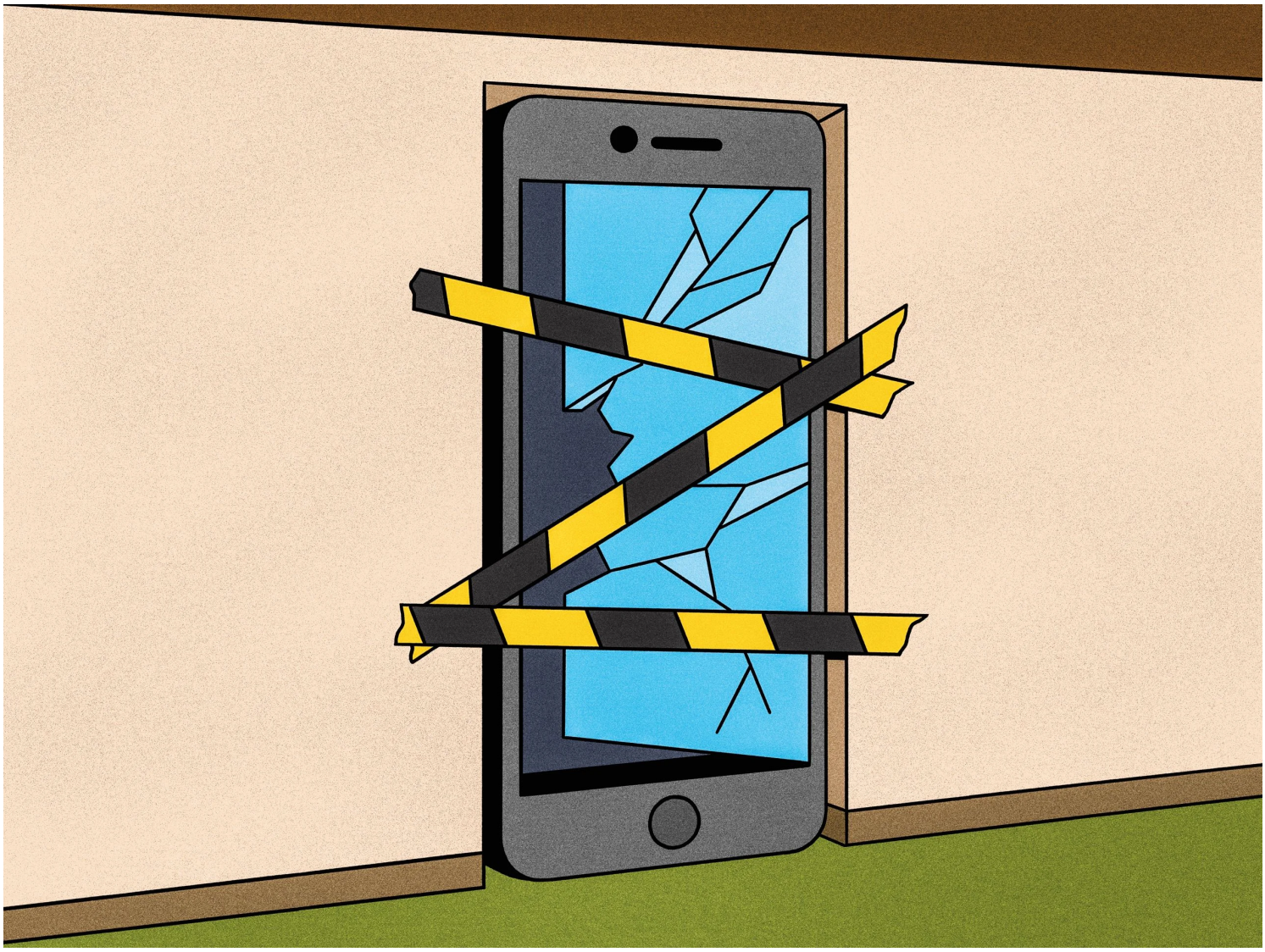
THE DIGITAL AGE JUNE 18, 2018 ISSUE

WHY DO WE CARE SO MUCH ABOUT PRIVACY?

Big Tech wants to exploit our personal data, and the government wants to keep tabs on us. But "privacy" isn't what's really at stake.

By Louis Menand

June 11, 2018



Amid ever-evolving technologies, the law is always playing catch-up. **Illustration by Seb Agresti**

0:00 / 31:07

Audio: Listen to this article.

The reason you've been receiving a steady stream of privacy-policy updates from online services, some of which you may have forgotten you ever subscribed to, is that the European Union just enacted the General Data Protection Regulation, which gives users greater control over the information that online companies collect about them. Since the Internet is a global medium, many companies now need to adhere to the E.U. regulation.

How many of us are going to take the time to scroll through the new policies and change our data settings, though? We sign up to get the service, but we don't give much thought to who might be storing our clicks or what they're doing with our personal information. It is weird, at first, when our devices seem to "know" where we live or how old we are or what books we like or which brand of toothpaste we use. Then we grow to expect this familiarity, and even to like it. It makes the online world seem customized for us, and it cuts down on the time we need to map the route home or order something new to read. The machine anticipates what we want.

But, as it has become apparent in the past year, we don't really know who is seeing our data or how they're using it. Even the people whose business it is to know don't know. When it came out that the consulting firm Cambridge Analytica had harvested the personal information of more than fifty million Facebook users and offered it to clients, including the Trump campaign, the *Times*' lead consumer-technology writer published a column titled "I Downloaded the Information That Facebook Has on Me. Yikes." He was astonished at how much of his personal data Facebook had stored and the long list of companies it had been sold to. Somehow, he had never thought to look into this before. How did he think Facebook became a five-hundred-and-sixty-billion-dollar company? It did so by devising the most successful system ever for compiling and purveying consumer data.

And data security wasn't even an issue: Cambridge Analytica didn't hack anyone. An academic researcher posted an online survey and invited people to participate by downloading an app. The app gave the researcher access not just to personal information in the participants' Facebook accounts (which Facebook allows) but to the personal information of all their "friends" (which Facebook allowed at the time). Cambridge Analytica, which hired the researcher, was thus able to collect the personal data of Facebook users who had never downloaded the app. Facebook at first refused to characterize this as a security breach—all the information was legally accessed, although it was not supposed to be sold—and continues to insist that it has no plans to provide recompense.

Cambridge Analytica isn't the only threat to digital privacy. The Supreme Court is set to decide the fate of Timothy Carpenter, who, in 2014, was convicted of participating in a series of armed robberies on the basis, in part, of records obtained by the police from his cell-phone company. These showed the location of the cell-phone towers his calls were routed through, and that information placed him near the scenes of the crimes. Carpenter was sentenced to a hundred and sixteen years in prison. The Court is being asked to rule on whether the collection of the cell-phone company's records violated his constitutional rights.

The government's position (argued before the Court last fall by Michael Dreeben, a Deputy Solicitor General, who is currently assisting the Mueller investigation) relies on what is known as the third-party doctrine. Police cannot listen in on your phone conversations without a warrant. But since Carpenter knowingly revealed his location to a third party, his cell-phone service provider, that information—called metadata—is not protected. It can be obtained with a court order, equivalent to a subpoena, which is served on the provider, not the customer. The third-party doctrine dates from a 1979 case, Smith v. Maryland, and it has been used to obtain, for example, suspects' bank records.

The third-party doctrine is what made legal the use of a pen register, a device that records all outgoing and incoming calls, on the phones of Donald Trump's lawyer Michael Cohen. Rather more consequentially, it was the legal justification for the National Security Agency's collection of metadata for all the incoming and outgoing calls of every person in the United States between 2001 and 2015. You "gave" that information to your phone service, just as you gave your credit-card company information about where and when you bought your last iced latte and how much you paid for it. The government can obtain that information with minimal judicial oversight.

Meanwhile, of course, Alexa is listening. Last month, an Oregon couple's domestic conversation (about hardwood floors, they said) was recorded by Echo, Amazon's "smart speaker" for the home, which sent it as an audio file to one of the husband's employees. Amazon called the event "an extremely rare occurrence"—that is, not a systemic security issue.

The good that is said to sit at the nexus of these developments in technology, commerce, and the law is privacy. "It's *private!* " kids are always yelling at their parents and siblings, which suggests that there is something primal about the need for privacy, for secrecy, for hiding places and personal space. These are things we seem to want. But do we have a right to them?

In 1948, the District of Columbia, in an arrangement with Muzak, the company that sells background music for stores and hotel lobbies, began piping radio broadcasts into the city's trolleys and buses. The broadcasts were mostly music, with some commercials and announcements, and were not loud enough to prevent riders from talking to one another. On the other hand, riders could not not hear them. Complaints were received, and a survey was duly commissioned. The survey found that ninety-two per cent of bus and trolley riders did not have a problem with the broadcasts. So they continued.

Two customers, however, chose to take a stand. They were Franklin Pollak and Guy Martin, and they happened to be lawyers. These gentlemen sued the city. Being compelled to listen to a radio program not of their choosing on a public bus, they maintained, represented an unlawful deprivation of liberty under the Constitution. The case made it all the way to the United States Supreme Court.

The Court handed down its decision in 1952. A bus, it said, is not like a home. It is a public space, and in a public space the public interest prevails. As long as the city government has the comfort, safety, and convenience of its riders at heart, it can run its transportation system any way it wants. Pollak and Martin had no more right to demand quiet on the bus than they had to tell the driver where to stop.

The vote was 7–1. One Justice, Felix Frankfurter, recused himself. Frankfurter explained that his own aversion to Muzak was so visceral—"my feelings are so strongly engaged as a victim," he wrote—that he was incapable of attaining the degree of disinterestedness necessary to render a judgment. (This posture is pretty much Felix Frankfurter in a nutshell.)

The lone dissenter was William O. Douglas. Douglas was a judicial renegade, with little concern for precedent. “We write,” he began his dissent, “on a clean slate.” Finding no rule, he provided one. Freedom was the issue, he explained, and “the beginning of all freedom” is “the right to be let alone”—that is, the right to privacy. To Douglas, more was at stake than annoying background music. Forcing people to listen to the radio, he said, is a step on the road to totalitarianism. If you can tell people what to listen to, you can tell people what to think. “The right of privacy,” Douglas concluded, “is a powerful deterrent to any one who would control men’s minds.”

Douglas did not coin the phrase “the right to be let alone.” It appears in one of the most famous law-review articles ever written, “The Right to Privacy,” by Samuel Warren and Louis Brandeis, published in the *Harvard Law Review* in 1890. (Warren and Brandeis took it from an 1879 treatise on tort law.) And “The Right to Privacy” is where Sarah Igo begins “The Known Citizen” (Harvard), her mighty effort to tell the story of modern America as a story of anxieties about privacy.

Igo’s first book, “The Averaged American,” was a well-received study of how twentieth-century social researchers created the idea of a “mass public.” Her new effort has to be mighty because, as she admits at the start, privacy is a protean concept—“elastic” is the term she uses—and, once you start looking for it, it pops up almost everywhere. Every new technological, legal, and cultural development seems to have prompted someone to worry about the imminent death of privacy. In the nineteenth century, people were shocked by the introduction of postcards, which invited strangers to read your mail. Mail was supposed to be private.

The Muzak case is not in Igo’s book, but plenty else is. She takes on telegraphy, telephony, instantaneous photography (snapshots), dactyloscopy (fingerprinting), Social Security numbers, suburbanization, the Minnesota Multiphasic Personality Inventory, Fourth Amendment jurisprudence, abortion rights, gay liberation, human-subject research, the Family Educational Rights and Privacy Act, “60 Minutes,” Betty Ford, the 1973 PBS documentary “An American Family,” the Starr Report, the memoir craze, blogging, and social media. Igo is an intelligent interpreter of the facts, and her intelligence frequently leads her to the conclusion that “privacy” lacks any stable significance. Privacy is associated with liberty, but it is also associated with privilege (private roads and private sales), with confidentiality (private conversations), with nonconformity and dissent, with shame and embarrassment, with the deviant and the taboo (Igo does not go there), and with subterfuge and concealment.

Sometimes, as in Douglas's dissent, privacy functions as a kind of default right when an injury has been inflicted and no other right seems to suit the case. Douglas got a second crack at applying his theory of privacy as a constitutional right in 1965, in the case of Griswold v. Connecticut. At issue was a Connecticut law that made the use of contraception a crime. "Specific guarantees in the Bill of Rights," Douglas wrote for the Court, "have penumbras, formed by emanations from those guarantees that help give them life and substance." The right to privacy was formed out of such emanations.

What places contraception beyond the state's police powers—its right to pass laws to protect the health and welfare of its citizens? The answer, Douglas said, is something that predates the Constitution: the institution of marriage. "Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred," he wrote. It is beyond politics and even beyond law. (Douglas, incidentally, was married four times.) Eight years later, Griswold was a key precedent in another case about reproductive rights, Roe v. Wade. "The right to privacy," the Court said in that case, "is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."

Igo notes that often privacy is simply a weapon that comes to hand in social combat. People invoke their right to privacy when it serves their interests. This is obviously true of "fruit of the poisonous tree" arguments, as when defendants ask the court to throw out evidence obtained in an unauthorized search. But it's also true when celebrities complain that their privacy is being invaded by photographers and gossip columnists. Reporters intrude on privacy in the name of the public's "right to know," and are outraged when asked to reveal their sources.

People are inconsistent about the kind of exposure they'll tolerate. We don't like to be fingerprinted by government agencies, a practice we associate with mug shots and state surveillance, but we happily hand our thumbprints over to Apple, which does God knows what with them. A requirement that every citizen carry an I.D. card seems un-American, but we all memorize our Social Security numbers and recite the last four digits pretty much any time we're asked.

A lot of people considered reports about which videos Clarence Thomas rented to be relevant to the question of whether he was qualified to sit on the Supreme Court, and a lot of people hoped that someone would leak Donald Trump's income-tax returns. But many of the same people were

indignant about the publication of the Starr Report, on the Oval Office sexcapades of Bill Clinton. Sex is supposed to be private.

Privacy has value, in other words, and, as Igo points out, sometimes the value is realized by hoarding it and sometimes it's realized by cashing it out. Once, it was thought that gay people were better off keeping their sexuality secret. Then it was decided that they were better off making their sexuality public, and, almost overnight, privacy became a sign of hypocrisy.

In the nineteen-seventies and eighties, people began making themselves famous, and sometimes wealthy, by exposing their and other people's lives on television and in books. Some of these glimpses into private life were stage-managed, like the TV show "Lifestyles of the Rich and Famous." Some were exposés, like many of the books and programs about the Kennedys. And some, like "An American Family," the PBS documentary about the Loud family, were both revealing and self-promoting. But reality shows and confessional memoirs did not mark the death of privacy. On the contrary, they confirmed how valuable a commodity privacy is.

Privacy is especially valuable to criminals. The same Fourth Amendment rights that prohibit the government from entering your home and listening to your conversations without a warrant also protect people engaged in illegal activities. Figuring out when law enforcement is crossing the line in getting the goods on criminal suspects has been an unending job for the courts.

The job is unending because technology is always changing. The government now has many methods besides tapping into your phone wire—you probably don't even have a phone wire—for finding out what you're up to. How far the constitutional right to privacy can be made to stretch is the subject of Cyrus Farivar's lively history of recent Fourth Amendment jurisprudence, "Habeas Data: Privacy vs. the Rise of Surveillance Tech" (Melville House).

Warren and Brandeis's article on privacy, back in 1890, said nothing about the Constitution. It argued that a right to privacy is inherent in the common law, and generated various "privacy torts," such as the disclosure of private facts or the unauthorized use of someone's name or likeness. Igo is a bit dismissive of "The Right to Privacy." She calls it "a strategy for reestablishing proper social boundaries and regulating public morality"—an attempt by the privileged to keep unwanted photographs and salacious gossip out of the newspapers by threatening legal action. And it is true

that privacy, like many civil rights, can serve as a protection for property owners and the status quo generally. But inside "The Right to Privacy" was a time bomb, and, almost forty years later, it went off.

Roy Olmstead was a big-time Seattle bootlegger who was convicted of conspiracy to violate the Prohibition Act, in part on the basis of evidence gathered through government wiretaps. In Olmstead v. United States, decided in 1928, the Supreme Court affirmed the conviction. But Louis Brandeis was now an Associate Justice on the Court, and he filed a dissent. Brandeis argued that because the government had broken the law—wiretapping was a crime in the state of Washington—the evidence gained from the wiretap should have been excluded at Olmstead's trial. His rights had been violated. "The right to be let alone," Brandeis wrote, is "the most comprehensive of rights, and the right most valued by civilized men." Those are, of course, the sentiments that William O. Douglas echoed twenty-four years later in the Muzak case.

Brandeis's opinion in Olmstead is one of those dissents which outlive the decision. And, in 1967, in Katz v. United States, the Supreme Court overturned Olmstead. Charles Katz lived in an apartment house on Sunset Boulevard, in Los Angeles. Almost every day, he walked down the street to a bank of three telephone booths, entered one of them, and made a long-distance call. Katz was a handicapper; he was calling his bookie, in Massachusetts. He had been making his living this way for thirty years.

To catch him, the F.B.I. placed microphones on top of two of the phone booths and put an "Out of Order" sign on the third. After recording Katz for six days, agents arrested him and obtained a warrant to search his apartment, where they found ample evidence of gambling. The question before the Supreme Court was whether the use of microphones on the phone booths violated Katz's Fourth Amendment rights.

The Fourth Amendment had always been understood in terms of trespass. It prohibits the government from violating the sanctity of private property—a home or an office—without a warrant. But Katz was not in a home or an office. He was in a public space. It may have seemed wrong for the F.B.I. to listen in on his conversations without a warrant, but it was hard, under existing jurisprudence, to explain why it was unconstitutional.

The Court found a fix. Persuaded by Katz's attorney, Harvey Schneider, and by a young lawyer clerking for Justice Potter Stewart, Laurence Tribe (now a well-known Harvard law professor), it changed its interpretation of the Fourth Amendment. The right to privacy does not attach to property, the Court now said; it attaches to persons. Charles Katz carried that right with him, and whatever he did "with a reasonable expectation of privacy" the government was barred from eavesdropping on.

Katz became a key precedent in Fourth Amendment cases. Intuitively, the reasoning appears sound. If it is unconstitutional to tap a telephone without a warrant, it seems obvious that using a microphone to record a phone conversation (in Katz's case, half of a conversation) should also be unconstitutional. But there are two problems at the heart of Katz. The first is the distinction between a microphone and an ear. If Katz had spoken loudly enough to be overheard by agents standing outside the phone booth, his words could have been used as evidence against him in a court of law. In effect, the microphone was just a prosthetic device, an extension of the agents' ears. It was not hearing differently; it was only hearing better.

As Farivar shows us, technology continually poses problems of this kind. Take the case of Jones v. United States, in which police attached a G.P.S. tracking device to the Jeep of Antoine Jones, who was suspected of being a drug dealer, and followed his movements for four weeks. The Supreme Court found that the use of the device violated Jones's right to privacy. Theoretically, the police could have trailed Jones's Jeep in a car or a helicopter, or posted officers along every road in the area, and the evidence they gathered would have been admissible. The tracking device only improved law-enforcement efficiency. Why did it trigger the Fourth Amendment? In the majority opinion, by Antonin Scalia, the Court reverted to the trespass theory: it was the physical trespass onto Jones's property, his Jeep, that required a warrant.

In another case, Kyllo v. United States, police used a thermal-imaging device to monitor the apartment of one Danny Lee Kyllo. The device recorded an unusual amount of heat radiating from the walls and the roof. Police used this information to obtain a search warrant, and discovered that Kyllo was operating a marijuana farm in his apartment. The Supreme Court ruled that evidence gained from a thermal device cannot be used to get a warrant—even though an officer on the sidewalk who noticed the heat could have used his observations to obtain one, and the thermal device simply allowed detectives to "feel" the heat at a distance.

The other problem in Katz is the "reasonable expectation of privacy" standard. Again, the rule seems sensible. People assume that when they are talking inside a phone booth they are not being monitored. But who gets to claim an expectation of privacy and where is not self-evident. Can a person driving a rented car whose name is not on the agreement with the rental company? Last month, the Supreme Court, in a unanimous decision, said yes. And as Anthony Amsterdam, a law professor who argued, and won, the famous death-penalty case Furman v. Georgia, in 1972, has pointed out, people's reasonable expectations are easily altered.

If people are told by the government or by a service provider that their behavior is being monitored, the expectation of privacy instantly becomes unreasonable. Twenty years ago, for example, citizens could assume that they were not being photographed when they walked down the street. Today, there are thirty thousand closed-circuit surveillance cameras on the streets of Chicago alone. A cop can theoretically match up a face on the street with a mug shot; with facial-recognition technology, the CCTV system does it automatically.

Police now have license-plate readers, which are mounted on squad cars and use optical-character-recognition technology to record license-plate numbers. Farivar says that the city of Oakland collects forty-eight thousand license-plate numbers a day. What concerns him is not that license plates are being read but that they are being read and recorded by a machine. We don't object when a cop checks a license-plate number against a list in a notebook. We consider that good police work, a way to identify traffic-ticket scofflaws and to find stolen cars. The fact that the cop has been replaced by a robot can summon up images of "1984." But you could argue that the robot is just way more efficient.

Farivar, in short, is correct that among the many things the tech industry has disrupted is Fourth Amendment jurisprudence. The law is constantly playing catch-up. In the digital age, almost all transactions are recorded somewhere, and almost any information worth keeping private involves a third party. Most of us store more in the cloud than in lockboxes. It does not make sense to constrain the technological capacities of law enforcement just because the technology allows it to work more efficiently, but those capacities can also lead to a society whose citizens have nowhere to hide.

And, even if its applications are brought up to date, the Fourth Amendment is good only against the government. Restricting a corporation's use of personal data requires a legislative act, and Congress is a barely functioning body. As for the Trump Administration, it seems indifferent to any rights except

those which are enumerated in the Second Amendment or which might protect the President and his henchmen. There is also the extraordinary economic power of the tech industry, a major engine of growth whose enormous cash reserves make legal settlements low-impact capital events.

Igo does what historians do: she shows us that although we may feel that the threat to privacy today is unprecedented, every generation has felt that way since the introduction of the postcard. The government is doing what it has always done, which is to conduct surveillance of individuals and groups it suspects of presenting a danger to society. And commercial media are doing what they have always done, which is to use consumer information to sell advertising. Of course Facebook does this. So do CBS and *People*.

What makes us feel powerless today is the scale. Fifty years ago, the government could not have collected the metadata for every phone call in a fourteen-year period. The technology did not exist (or would have been prohibitively expensive). Radio and television enabled advertisers to come right into your living room, but the reach of online industries is vaster by many orders of magnitude. Last month, the season finale of CBS's most popular show, "The Big Bang Theory," had roughly fifteen million viewers, and *People* reaches an estimated forty-one million readers a week. Those are tiny numbers. Facebook has 2.2 billion active monthly users. Google processes 3.5 billion searches every day.

"The twin imperatives of corporate profit and national security," Igo says, militate against greater privacy protections. A classic contest between them played out in the wake of the San Bernardino massacre. In 2015, Syed Rizwan Farook and Tashfeen Malik, a married couple, killed fourteen people and wounded twenty-two in that terrorist attack. Farook and Malik died in a shoot-out with police, who retrieved an iPhone carried by Farook. When the National Security Agency was unable to unlock the device, the F.B.I. asked Apple to do it.

Apple refused, on the ground that its business would suffer if customers knew that third parties could hack into their phones. The government accused Apple of marketing to criminals, and sued. The case was in the courts when the F.B.I. found someone to sell it a tool that unlocked the phone, and the lawsuit was dropped. Three media companies subsequently sued under the Freedom of Information Act to compel the government to reveal the identity of the person or the firm that sold the F.B.I. the unlocking tool, but last fall a federal judge ruled that the information was classified as a matter of

national security. How a public agency got something a private corporation was trying to keep a secret is a secret. This is the world we are living in.

The question about national security and personal convenience is always: At what price? What do we have to give up? On the criminal-justice side, law enforcement is in an arms race with lawbreakers. Timothy Carpenter was allegedly able to orchestrate an armed-robbery gang in two states because he had a cell phone; the law makes it difficult for police to learn how he used it. Thanks to lobbying by the National Rifle Association, federal law prohibits the National Tracing Center from using a searchable database to identify the owners of guns seized at crime scenes. Whose privacy is being protected there?

Most citizens feel glad for privacy protections like the one in Griswold, but are less invested in protections like the one in Katz. In "Habeas Data," Farivar analyzes ten Fourth Amendment cases; all ten of the plaintiffs were criminals. We want their rights to be observed, but we also want them locked up.

On the commercial side, are the trade-offs equivalent? The market-theory expectation is that if there is demand for greater privacy then competition will arise to offer it. Services like Signal and WhatsApp already do this. Consumers will, of course, have to balance privacy with convenience. The question is: Can they really? The General Data Protection Regulation went into effect on May 25th, and privacy-advocacy groups in Europe are already filing lawsuits claiming that the policy updates circulated by companies like Facebook and Google are not in compliance. How can you ever be sure who is eating your cookies?

Possibly the discussion is using the wrong vocabulary. "Privacy" is an odd name for the good that is being threatened by commercial exploitation and state surveillance. Privacy implies "It's nobody's business," and that is not really what Roe v. Wade is about, or what the E.U. regulations are about, or even what Katz and Carpenter are about. The real issue is the one that Pollak and Martin, in their suit against the District of Columbia in the Muzak case, said it was: liberty. This means the freedom to choose what to do with your body, or who can see your personal information, or who can monitor your movements and record your calls—who gets to surveil your life and on what grounds.

As we are learning, the danger of data collection by online companies is not that they will use it to try to sell you stuff. The danger is that that information can so easily fall into the hands of parties whose motives are much less benign. A government, for example. A typical reaction to worries about the police listening to your phone conversations is the one Gary Hart had when it was suggested that reporters might tail him to see if he was having affairs: "You'd be bored." They were not, as it turned out. We all may underestimate our susceptibility to persecution. "We were just talking about hardwood floors!" we say. But authorities who feel emboldened by the promise of a Presidential pardon or by a Justice Department that looks the other way may feel less inhibited about invading the spaces of people who belong to groups that the government has singled out as unpatriotic or undesirable. And we now have a government that does that. ♦

Published in the print edition of the June 18, 2018, issue, with the headline "Nowhere to Hide."

Louis Menand has been a staff writer at The New Yorker since 2001. He teaches at Harvard University.

More: Privacy "The Known Citizen" Sarah Igo "Habeas Data: Privacy vs. the Rise of Surveillance Tech" Cyrus Farivar Books