BROOKINGS

Report

Why protecting privacy is a losing game today—and how to change the game

Cameron F. Kerry Thursday, July 12, 2018

Summary

Recent congressional hearings and data breaches have prompted more legislators and business leaders to say the time for broad federal privacy legislation has come. Cameron Kerry presents the case for adoption of a baseline framework to protect consumer privacy in the U.S.

Kerry explores a growing gap between existing laws and an information Big Bang that is eroding trust. He suggests that recent privacy bills have not been ambitious enough, and points to the Obama administration's Consumer Privacy Bill of Rights as a blueprint for future legislation. Kerry considers ways to improve that proposal, including an overarching "golden rule of privacy" to ensure people can trust that data about them is handled in ways consistent with their interests and the circumstances in which it was collected.

Table of Contents

Introduction: Game change?

There is a classic episode of the show "I Love Lucy" in which Lucy goes to work wrapping candies on an assembly line. The line keeps speeding up with the candies coming closer together and, as they keep getting farther and farther behind, Lucy and her sidekick Ethel scramble harder and harder to keep up. "I think we're fighting a losing game," Lucy says.

This is where we are with data privacy in America today. More and more data about each of us is being generated faster and faster from more and more devices, and we can't keep up. It's a losing game both for individuals and for our legal system. If we don't change the rules of the game soon, it will turn into a losing game for our economy and society.

More and more data about each of us is being generated faster and faster from more and more devices, and we can't keep up. It's a losing game both for individuals and for our legal system.

The Cambridge Analytica drama has been the latest in a series of eruptions that have caught peoples' attention in ways that a steady stream of data breaches and misuses of data have not.

The first of these shocks was the Snowden revelations in 2013. These made for long-running and headline-grabbing stories that shined light on the amount of information about us that can end up in unexpected places. The disclosures also raised awareness of how much can be learned from such data ("we kill people based on metadata," former NSA and CIA Director Michael Hayden said).

The aftershocks were felt not only by the government, but also by American companies, especially those whose names and logos showed up in Snowden news stories. They faced suspicion from customers at home and market resistance from customers overseas. To rebuild trust, they pushed to disclose more about the volume of surveillance demands and for changes in surveillance laws. Apple, Microsoft, and Yahoo all engaged in public legal battles with the U.S. government.

Then came last year's Equifax breach that compromised identity information of almost 146 million Americans. It was not bigger than some of the lengthy roster of data breaches that preceded it, but it hit harder because it rippled through the financial system and affected individual consumers who never did business with Equifax directly but nevertheless had to deal with the impact of its credit scores on economic life. For these people, the breach was another demonstration of how much important data about them moves around without their control, but with an impact on their lives.

Now the Cambridge Analytica stories have unleashed even more intense public attention, complete with live network TV cut-ins to Mark Zuckerberg's congressional testimony. Not only were many of the people whose data was collected surprised that a company they never heard of got so much personal information, but the Cambridge Analytica story touches on all the controversies roiling around the role of social media in the cataclysm of the 2016 presidential election. Facebook estimates that Cambridge Analytica was able to leverage its "academic" research into data on some 87 million Americans (while before the 2016 election Cambridge Analytica's CEO Alexander Nix boasted of having profiles with 5,000 data points on 220 million Americans). With over two billion Facebook users worldwide, a lot of people have a stake in this issue and, like the Snowden stories, it is getting intense attention around the globe, as demonstrated by Mark Zuckerberg taking his legislative testimony on the road to the European Parliament.

The Snowden stories forced substantive changes to surveillance with enactment of U.S. legislation curtailing telephone metadata collection and increased transparency and safeguards in intelligence collection. Will all the hearings and public attention on Equifax and Cambridge Analytica bring analogous changes to the commercial sector in America?

I certainly hope so. I led the Obama administration task force that developed the "Consumer Privacy Bill of Rights" issued by the White House in 2012 with support from both businesses and privacy advocates, and then drafted legislation to put this bill of rights into law. The legislative proposal issued after I left the government did not get much traction, so this initiative remains unfinished business.

The Cambridge Analytica stories have spawned fresh calls for some federal privacy legislation from members of Congress in both parties, editorial boards, and commentators. With their marquee Zuckerberg hearings behind them, senators and congressmen are moving on to think about what do next. Some have already introduced bills and others are thinking about what privacy proposals might look like. The op-eds and Twitter threads on what to do have flowed. Various groups in Washington have been convening to develop proposals for legislation.

This time, proposals may land on more fertile ground. The chair of the Senate Commerce Committee, John Thune (R-SD) said "many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing." A number of companies have been increasingly open to a discussion of a basic federal privacy law. Most notably, Zuckerberg told CNN "I'm not sure we shouldn't be regulated," and Apple's Tim Cook expressed his emphatic belief that self-regulation is no longer viable.

For a while now, events have been changing the way that business interests view the prospect of federal privacy legislation.

This is not just about damage control or accommodation to "techlash" and consumer frustration. For a while now, events have been changing the way that business interests view the prospect of federal privacy legislation. An increasing spread of state legislation on net neutrality, drones, educational technology, license plate readers, and other subjects and, especially broad new legislation in California pre-empting a ballot initiative, have made the possibility of a single set of federal rules across all 50 states look attractive. For multinational companies that have spent two years gearing up for compliance with the new data protection law that has now taken effect in the EU, dealing with a comprehensive U.S. law no longer looks as daunting. And more companies are seeing value in a common baseline that can provide people with reassurance about how their data is handled and protected against outliers and outlaws.

This change in the corporate sector opens the possibility that these interests can converge with those of privacy advocates in comprehensive federal legislation that provides effective protections for consumers. Trade-offs to get consistent federal rules that preempt some strong state laws and remedies will be difficult, but with a strong enough federal baseline, action can be achievable.

how current law is falling behind

Snowden, Equifax, and Cambridge Analytica provide three conspicuous reasons to take action. There are really quintillions of reasons. That's how fast IBM estimates we are generating digital information, *quintillions* of bytes of data every day—a number followed by 30 zeros. This explosion is generated by the doubling of computer processing power every 18-24 months that has driven growth in information technology throughout the computer age, now compounded by the billions of devices that collect and transmit data, storage devices and data centers that make it cheaper and easier to keep the data from these devices, greater bandwidth to move that data faster, and more powerful and sophisticated software to extract information from this mass of data. All this is both enabled and magnified by the singularity of network effects—the value that is added by being connected to others in a network—in ways we are still learning.

This information Big Bang is doubling the volume of digital information in the world every two years. The data explosion that has put privacy and security in the spotlight will accelerate. Futurists and business forecasters debate just how many tens of billions of devices will be connected in the coming decades, but the order of magnitude is unmistakable—and staggering in its impact on the quantity and speed of bits of information moving around the globe. The pace of change is dizzying, and it will get even faster—far more dizzying than Lucy's assembly line.

Most recent proposals for privacy legislation aim at slices of the issues this explosion presents. The Equifax breach produced legislation aimed at data brokers. Responses to the role of Facebook and Twitter in public debate have focused on political ad disclosure, what to do about bots, or limits to online tracking for ads. Most state legislation has targeted specific topics like use of data from ed-tech products, access to social media accounts by employers, and privacy protections from drones and license-plate readers. Facebook's simplification and expansion of its privacy controls and recent federal privacy bills in reaction to events focus on increasing transparency and consumer choice. So does the newly enacted California Privacy Act.

This information Big Bang is doubling the volume of digital information in the world every two years. The data explosion that has put privacy and security in the spotlight will accelerate. Most recent proposals for privacy legislation aim at slices of the issues this explosion presents.

Measures like these double down on the existing American privacy regime. The trouble is, this system cannot keep pace with the explosion of digital information, and the pervasiveness of this information has undermined key premises of these laws in ways that are increasingly glaring. Our current laws were designed to address collection and storage of structured data by government, business, and other organizations and are busting at the seams in a world where we are all connected and constantly sharing. It is time for a more comprehensive and ambitious approach. We need to think bigger, or we will continue to play a losing game.

Our existing laws developed as a series of responses to specific concerns, a checkerboard of federal and state laws, common law jurisprudence, and public and private enforcement that has built up over more than a century. It began with the famous Harvard Law Review article by (later) Justice Louis Brandeis and his law partner Samuel Warren in 1890 that provided a foundation for case law and state statutes for much of the 20th Century, much of which addressed the impact of mass media on individuals who wanted, as Warren and Brandeis put it, "to be let alone." The advent of mainframe computers saw the first data privacy laws adopted in 1974 to address the power of information in the hands of big institutions like banks and government: the federal Fair Credit Reporting Act that gives us access to information on credit reports and the Privacy Act that governs federal agencies. Today, our checkerboard of privacy and data security laws covers data that concerns people the most. These include health data, genetic information, student records and information pertaining to children in general, financial information, and electronic communications (with differing rules for telecommunications carriers, cable providers, and emails).

Outside of these specific sectors is not a completely lawless zone. With Alabama adopting a law last April, all 50 states now have laws requiring notification of data breaches (with variations in who has to be notified, how quickly, and in what circumstances). By making organizations focus on personal data and how they protect it, reinforced by exposure to public and private enforcement litigation, these laws have had a significant impact on privacy and security practices. In addition, since 2003, the Federal Trade Commission—under both Republican and Democratic majorities—has used its enforcement authority to regulate unfair and deceptive commercial practices and to police unreasonable privacy and information security practices. This enforcement, mirrored by many state attorneys general, has relied primarily on deceptiveness, based on failures to live up to privacy policies and other privacy promises.

These levers of enforcement in specific cases, as well as public exposure, can be powerful tools to protect privacy. But, in a world of technology that operates on a massive scale moving fast and doing things because one can, reacting to particular abuses after-the-fact does not provide enough guardrails.

As the data universe keeps expanding, more and more of it falls outside the various specific laws on the books. This includes most of the data we generate through such widespread uses as web searches, social media, e-commerce, and smartphone apps. The changes come faster than legislation or regulatory rules can adapt, and they erase the sectoral boundaries that have defined our privacy laws. Take my smart watch, for one example: data it generates about my heart rate and activity is covered by the Health Insurance Portability and Accountability Act (HIPAA) if it is shared with my doctor, but not when it goes to fitness apps like Strava (where I can compare my performance with my peers). Either way, it is the same data, just as sensitive to me and just as much of a risk in the wrong hands.

As the data universe keeps expanding, more and more of it falls outside the various specific laws on the books.

It makes little sense that protection of data should depend entirely on who happens to hold it. This arbitrariness will spread as more and more connected devices are embedded in everything from clothing to cars to home appliances to street furniture. Add to that striking changes in patterns of business integration and innovation—traditional telephone providers like Verizon and AT&T are entering entertainment, while startups launch into the provinces of financial institutions like currency trading and credit and all kinds of enterprises compete for space in the autonomous vehicle ecosystem—and the sectoral boundaries that have defined U.S. privacy protection cease to make any sense.

Putting so much data into so many hands also is changing the nature of information that is protected as private. To most people, "personal information" means information like social security numbers, account numbers, and other information that is unique to them. U.S. privacy laws reflect this conception by aiming at "personally identifiable information," but data scientists have repeatedly demonstrated that this focus can be too narrow. The aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them. The result is that today, a widening range of data has the potential to be personal information, i.e. to identify us uniquely. Few laws or regulations address this new reality.

Nowadays, almost every aspect of our lives is in the hands of some third party somewhere. This challenges judgments about "expectations of privacy" that have been a major premise for defining the scope of privacy protection. These judgments present binary choices: if private information is somehow public or in the hands of a third party, people often are deemed to have no expectation of privacy. This is particularly true when it comes to government access to information—emails, for example, are nominally less protected under our laws once they have been stored 180 days or more, and articles and activities in plain sight are considered categorically available to government authorities. But the concept also gets applied to commercial data in terms and conditions of service and to scraping of information on public websites, for two examples.

As more devices and sensors are deployed in the environments we pass through as we carry on our days, privacy will become impossible if we are deemed to have surrendered our privacy simply by going about the world or sharing it with any other person. Plenty of people have said privacy is dead, starting most famously with Sun Microsystems' Scott McNealy back in the 20th century ("you have zero privacy … get over it") and echoed by a chorus of despairing writers since then. Without normative rules to provide a more constant anchor than shifting expectations, true privacy actually could be dead or dying. The Supreme Court may have something to say on the subject in we will need a broader set of norms to protect privacy in settings that have been considered public. Privacy can endure, but it needs a more enduring foundation.

The Supreme Court in its recent *Carpenter* decision recognized how constant streams of data about us change the ways that privacy should be protected. In holding that enforcement acquisition of cell phone location records requires a warrant, the Court considered the "detailed, encyclopedic, and effortlessly compiled" information available from cell service location records and "the seismic shifts in digital technology" that made these records available, and concluded that people do not necessarily surrender privacy interests to collect data they generate or by engaging in behavior that can be observed publicly. While there was disagreement among Justices as to the sources of privacy norms, two of the dissenters, Justice Alito and Gorsuch, pointed to "expectations of privacy" as vulnerable because they can erode or be defined away.

How this landmark privacy decision affects a wide variety of digital evidence will play out in criminal cases and not in the commercial sector. Nonetheless, the opinions in the case point to a need for a broader set of norms to protect privacy in settings that have been thought to make information public. Privacy can endure, but it needs a more enduring foundation.

Our existing laws also rely heavily on notice and consent—the privacy notices and privacy policies that we encounter online or receive from credit card companies and medical providers, and the boxes we check or forms we sign. These declarations are what provide the basis for the FTC to find deceptive practices and acts when companies fail to do what they said. This system follows the model of informed consent in medical care and human

subject research, where consent is often asked for in person, and was imported into internet privacy in the 1990s. The notion of U.S. policy then was to foster growth of the internet by avoiding regulation and promoting a "market resolution" in which individuals would be informed about what data is collected and how it would be processed, and could make choices on this basis.

Maybe informed consent was practical two decades ago, but it is a fantasy today. In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't.

It is not simply that any particular privacy policies "suck," as Senator John Kennedy (R-LA) put it in the Facebook hearings. Zeynep Tufecki is right that these disclosures are obscure and complex. Some forms of notice are necessary and attention to user experience can help, but the problem will persist no matter how well designed disclosures are. I can attest that writing a simple privacy policy is challenging, because these documents are legally enforceable and need to explain a variety of data uses; you can be simple and say too little or you can be complete but too complex. These notices have some useful function as a statement of policy against which regulators, journalists, privacy advocates, and even companies themselves can measure performance, but they are functionally useless for most people, and we rely on them to do too much.

Maybe informed consent was practical two decades ago, but it is a fantasy today. In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't.

At the end of the day, it is simply too much to read through even the plainest English privacy notice, and being familiar with the terms and conditions or privacy settings for all the services we use is out of the question. The recent flood of emails about privacy policies and consent forms we have gotten with the coming of the EU General Data Protection Regulation have offered new controls over what data is collected or information communicated, but how much have they really added to people's understanding? Wall Street Journal reporter Joanna Stern attempted to analyze all the ones she received (enough paper printed out to stretch more than the length of a football field), but resorted to scanning for a few specific issues. In today's world of constant connections, solutions that focus on increasing transparency and consumer choice are an incomplete response to current privacy challenges.

Moreover, individual choice becomes utterly meaningless as increasingly automated data collection leaves no opportunity for any real notice, much less individual consent. We don't get asked for consent to the terms of surveillance cameras on the streets or "beacons" in stores that pick up cell phone identifiers, and house guests aren't generally asked if they agree to homeowners' smart speakers picking up their speech. At best, a sign may be posted somewhere announcing that these devices are in place. As devices and sensors increasingly are deployed throughout the environments we pass through, some after-the-fact access and control can play a role, but old-fashioned notice and choice become impossible.

Ultimately, the familiar approaches ask too much of individual consumers. As the President's Council of Advisers on Science and Technology Policy found in a 2014 report on big data, "the conceptual problem with notice and choice is that it fundamentally places the burden of privacy protection on the individual," resulting in an unequal bargain, "a kind of market failure."

This is an impossible burden that creates an enormous disparity of information between the individual and the companies they deal with. As Frank Pasquale ardently dissects in his "Black Box Society," we know very little about how the businesses that collect our data operate. There is no practical way even a reasonably sophisticated person can get arms around the data that they generate and what that data says about them. After all, making

sense of the expanding data universe is what data scientists do. Post-docs and Ph.D.s at MIT (where I am a visiting scholar at the Media Lab) as well as tens of thousands of data researchers like them in academia and business are constantly discovering new information that can be learned from data about people and new ways that businesses can —or do—use that information. How can the rest of us who are far from being data scientists hope to keep up?

As a result, the businesses that use the data know far more than we do about what our data consists of and what their algorithms say about us. Add this vast gulf in knowledge and power to the absence of any real give-and-take in our constant exchanges of information, and you have businesses able by and large to set the terms on which they collect and share this data.

Businesses are able by and large to set the terms on which they collect and share this data. This is not a "market resolution" that works.

This is not a "market resolution" that works. The Pew Research Center has tracked online trust and attitudes toward the internet and companies online. When Pew probed with surveys and focus groups in 2016, it found that "while many Americans are willing to share personal information in exchange for tangible benefits, they are often cautious about disclosing their information and frequently unhappy about that happens to that information once companies have collected it." Many people are "uncertain, resigned, and annoyed." There is a growing body of survey research in the same vein. Uncertainty, resignation, and annoyance hardly make a recipe for a healthy and sustainable marketplace, for trusted brands, or for consent of the governed.

Consider the example of the journalist Julia Angwin. She spent a year trying to live without leaving digital traces, which she described in her book "Dragnet Nation." Among other things, she avoided paying by credit card and established a fake identity to get a card

for when she couldn't avoid using one; searched hard to find encrypted cloud services for most email; adopted burner phones that she turned off when not in use and used very little; and opted for paid subscription services in place of ad-supported ones. More than a practical guide to protecting one's data privacy, her year of living anonymously was an extended piece of performance art demonstrating how much digital surveillance reveals about our lives and how hard it is to avoid. The average person should not have to go to such obsessive lengths to ensure that their identities or other information they want to keep private stays private. We need a fair game.

Shaping laws capable of keeping up

As policymakers consider how the rules might change, the Consumer Privacy Bill of Rights we developed in the Obama administration has taken on new life as a model. The Los Angeles Times, The Economist, and The New York Times all pointed to this bill of rights in urging Congress to act on comprehensive privacy legislation, and the latter said "there is no need to start from scratch …" Our 2012 proposal needs adapting to changes in technology and politics, but it provides a starting point for today's policy discussion because of the wide input it got and the widely accepted principles it drew on.

The bill of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission: individual control, transparency, respect for the context in which the data was obtained, access and accuracy, focused collection, security, and accountability. These broad principles are rooted in longstanding and globally-accepted "fair information practices principles." To reflect today's world of billions of devices interconnected through networks everywhere, though, they are intended to move away from static privacy notices and consent forms to a more dynamic framework, less focused on collection and process and more on how people are protected in the ways their data is handled. Not a checklist, but a toolbox. This principles-based approach was meant to be interpreted and fleshed out through codes of conduct and case-by-case FTC enforcement—iterative evolution, much the way both common law and information technology developed.

As policymakers consider how the rules might change, the Consumer Privacy Bill of Rights developed in the Obama administration has taken on new life as a model. The bill of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission.

The other comprehensive model that is getting attention is the EU's newly effective General Data Protection Regulation. For those in the privacy world, this has been the dominant issue ever since it was approved two years ago, but even so, it was striking to hear "the GDPR" tossed around as a running topic of congressional questions for Mark Zuckerberg. The imminence of this law, its application to Facebook and many other American multinational companies, and its contrast with U.S. law made GDPR a hot topic. It has many people wondering why the U.S. does not have a similar law, and some saying the U.S. should follow the EU model.

I dealt with the EU law since it was in draft form while I led U.S. government engagement with the EU on privacy issues alongside developing our own proposal. Its interaction with U.S. law and commerce has been part of my life as an official, a writer and speaker on privacy issues, and a lawyer ever since. There's a lot of good in it, but it is not the right model for America.

There's a lot of good in the GDPR, but it is not the right model for America.

What is good about the EU law? First of all, it is a law—one set of rules that applies to all personal data across the EU. Its focus on individual data rights in theory puts human beings at the center of privacy practices, and the process of complying with its detailed requirements has forced companies to take a close look at what data they are collecting, what they use it for, and how they keep it and share it—which has proved to be no small task. Although the EU regulation is rigid in numerous respects, it can be more subtle than is apparent at first glance. Most notably, its requirement that consent be explicit and freely given is often presented in summary reports as prohibiting collecting any personal data without consent; in fact, the regulation allows other grounds for collecting data and one effect of the strict definition of consent is to put more emphasis on these other grounds. How some of these subtleties play out will depend on how 40 different regulators across the EU apply the law, though. European advocacy groups were already pursuing claims against "*les GAFAM*" (Google, Amazon, Facebook, Apple, Microsoft) as the regulation went into effect.

The EU law has its origins in the same fair information practice principles as the Consumer Privacy Bill of Rights. But the EU law takes a much more prescriptive and process-oriented approach, spelling out how companies must manage privacy and keep records and including a "right to be forgotten" and other requirements hard to square with our First Amendment. Perhaps more significantly, it may not prove adaptable to artificial intelligence and new technologies like autonomous vehicles that need to aggregate masses of data for machine learning and smart infrastructure. Strict limits on the purposes of data use and retention may inhibit analytical leaps and beneficial new uses of information. A rule requiring human explanation of significant algorithmic decisions will shed light on algorithms and help prevent unfair discrimination but also may curb development of artificial intelligence. These provisions reflect a distrust of technology that is not universal in Europe but is a strong undercurrent of its political culture.

We need an American answer—a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy. The Consumer Privacy Bill of Rights offers a blueprint for such an approach.

Sure, it needs work, but that's what the give-and-take of legislating is about. Its language on transparency came out sounding too much like notice-and-consent, for example. Its proposal for fleshing out the application of the bill of rights had a mixed record of consensus results in trial efforts led by the Commerce Department.

It also got some important things right. In particular, the "respect for context" principle is an important conceptual leap. It says that a people "have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." This breaks from the formalities of privacy notices, consent boxes, and structured data and focuses instead on respect for the individual. Its emphasis on the interactions between an individual and a company and circumstances of the data collection and use derives from the insight of information technology thinker Helen Nissenbaum. To assess privacy interests, "it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."

We need an American answer—a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy.

Context is complicated—our draft legislation listed 11 different non-exclusive factors to assess context. But that is in practice the way we share information and form expectations about how that information will be handled and about our trust in the handler. We bare our souls and our bodies to complete strangers to get medical care, with the understanding that this information will be handled with great care and shared with strangers only to the extent needed to provide care. We share location information with ride-sharing and navigation apps with the understanding that it enables them to function,

but Waze ran into resistance when that functionality required a location setting of "always on." Danny Weitzner, co-architect of the Privacy Bill of Rights, recently discussed how the respect for context principle "would have prohibited [Cambridge Analytica] from unilaterally repurposing research data for political purposes" because it establishes a right "not to be surprised by how one's personal data issued." The Supreme Court's *Carpenter* decision opens up expectations of privacy in information held by third parties to variations based on the context.

The Consumer Privacy Bill of Rights does not provide any detailed prescription as to how the context principle and other principles should apply in particular circumstances. Instead, the proposal left such application to case-by-case adjudication by the FTC and development of best practices, standards, and codes of conduct by organizations outside of government, with incentives to vet these with the FTC or to use internal review boards similar to those used for human subject research in academic and medical settings. This approach was based on the belief that the pace of technological change and the enormous variety of circumstances involved need more adaptive decisionmaking than current approaches to legislation and government regulations allow. It may be that baseline legislation will need more robust mandates for standards than the Consumer Privacy Bill of Rights contemplated, but any such mandates should be consistent with the deeply embedded preference for voluntary, collaboratively developed, and consensus-based standards that has been a hallmark of U.S. standards development.

In hindsight, the proposal could use a lodestar to guide the application of its principles—a simple golden rule for privacy: that companies should put the interests of the people whom data is about ahead of their own. In some measure, such a general rule would bring privacy protection back to first principles: some of the sources of law that Louis Brandeis and Samuel Warren referred to in their famous law review article were cases in which the receipt of confidential information or trade secrets led to judicial imposition of a trust or duty of confidentiality. Acting as a trustee carries the obligation to act in the interests of the beneficiaries and to avoid self-dealing.

A Golden Rule of Privacy that incorporates a similar obligation for one entrusted with personal information draws on several similar strands of the privacy debate. Privacy policies often express companies' intention to be "good stewards of data;" the good steward also is supposed to act in the interests of the principal and avoid self-dealing. A more contemporary law review parallel is Yale law professor Jack Balkin's concept of "information fiduciaries," which got some attention during the Zuckerberg hearing when Senator Brian Schatz (D-HI) asked Zuckerberg to comment on it. The Golden Rule of Privacy would import the essential duty without importing fiduciary law wholesale. It also resonates with principles of "respect for the individual," "beneficence," and "justice" in ethical standards for human subject research that influence emerging ethical frameworks for privacy and data use. Another thread came in Justice Gorsuch's *Carpenter* dissent defending property law as a basis for privacy interests: he suggested that entrusting someone with digital information may be a modern equivalent of a "bailment" under classic property law, which imposes duties on the bailee. And it bears some resemblance to the GDPR concept of "legitimate interest," which permits the processing of personal data based on a legitimate interest of the processor, provided that this interest is not outweighed by the rights and interests of the subject of the data.

The fundamental need for baseline privacy legislation in America is to ensure that individuals can trust that data about them will be used, stored, and shared in ways that are consistent with their interests and the circumstances in which it was collected. This should hold regardless of how the data is collected, who receives it, or the uses it is put to. If it is personal data, it should have enduring protection.

The fundamental need for baseline privacy legislation in America is to ensure that individuals can trust that data about them will be used, stored, and shared in ways that are consistent with their interests and the circumstances in which it was collected.

Such trust is an essential building block of a sustainable digital world. It is what enables the sharing of data for socially or economically beneficial uses without putting human beings at risk. By now, it should be clear that trust is betrayed too often, whether by intentional actors like Cambridge Analytica or Russian "Fancy Bears," or by bros in cubes inculcated with an imperative to "deploy or die."

Trust needs a stronger foundation that provides people with consistent assurance that data about them will be handled fairly and consistently with their interests. Baseline principles would provide a guide to all businesses and guard against overreach, outliers, and outlaws. They would also tell the world that American companies are bound by a widely-accepted set of privacy principles and build a foundation for privacy and security practices that evolve with technology.

Resigned but discontented consumers are saying to each other, "I think we're playing a losing game." If the rules don't change, they may quit playing.
