REPORT SURVEILLANCE & PRIVACY

Can Laboratories of Democracy Innovate the Way to Privacy Protection?

APRIL 5, 2018 — JOANNE MCNABB

Today more data—our data, data about us—is in more hands, being used for more purposes than ever before. The Internet economy is fueled by personal information, yet it is largely a black box, whose inputs and outputs are not understood by most individuals or even regulators. One thing we do understand is that organizations that collect other people's information—online retailers and apps, banks, credit bureaus and even government agencies—often have a hard time keeping a tight grip on it, as evidenced by a steady stream of data breaches.The TJX breach of the credit card numbers of 94 million customers in 2006, Anthem's breach of the medical information of 79 million in 2015, and the massive Equifax breach reported in 2017 that exposed Social Security numbers, driver's license numbers, and other sensitive information of over 143 million Americans are just a few of the larger data breaches in recent years.[1]

Where is all this data coming from? Companies and other organizations are collecting information not only from our visits to websites and our use of mobile apps, along with our travels through the world using credit cards and passing video cameras, but also from inside our very own homes. Smart appliances, burglar alarms, utility meters, and a burgeoning market of connected consumer devices—even toys in the hands of our children[2]—are collecting data from us and about us: where we are and where we've been, whom we're with or near, what we're doing, waking or sleeping, around the clock, seven days a week. We're becoming nodes in the network of everything, with increasingly less ability to disconnect.

The recent Facebook–Cambridge Analytica incident raises many issues about the use of this very personal data in the marketplace. Reporters are still attempting to untangle the web of players who extracted and used the personal data of more than 87 million, and potentially all, Facebook users.[3] Among the concerns articulated in news reports are the effectiveness of terms of service, whether the incident constitutes a data breach, and the ethics of online political manipulation. More important—and less talked about—the incident reveals a lack in the United States of legal standards for data privacy as a fundamental human right.

Neither the market nor the law is working to protect privacy in our world of Big Data and complex data flows. In fact, the legal framework to protect privacy in the United States is flimsy and has been outpaced and outdated by technological developments. At the same time, the federal government is actually scaling back regulatory and enforcement actions regarding privacy, as on other consumer protection and civil liberties issues.

In the face of this federal retrenchment, states can and should step up their legislative efforts to protect privacy. The advent of a new privacy regulation in the European Union provides an opportunity for states to "harmonize" or modify key state privacy laws to align better with the standards that most companies that do business online will soon have to meet for their European customers.

Big Data and Its Harms

We live in an increasingly connected and data-driven world. Last year, the market intelligence company IDC forecast that by 2025, the global datasphere of all digital data created will grow to 163 zettabytes, a tenfold increase over the 2016 volume.[4] (A zettabyte is 1021 bytes. If everyone in the United States took a digital photo every second of every day for over a month, all of those photos together would amount to about one zettabyte.[5])

It's not just the volume of data collected and stored that makes Big Data big, it's also the capacity to do things with the data—Big Analytics. Big Analytics visionaries believe that the analysis of large volumes of formerly unavailable data holds the promise of providing new insights into and solutions for individual and societal problems, from personalized medicine to improved energy efficiency, detecting the dispersion of infectious diseases and more effective policing.[6]

We are part of the datasphere. Over half the world's population was connected to the Internet in 2017, and estimates for 2025 put the figure at 75 percent.[7] And our digital dossiers are growing. From online searches on a PC or mobile phone, to using a GPS in a car, being recorded by an ATM video camera, and heart rate monitoring by a fitness wearable, the average person is estimated to have experienced 218 data-driven interactions per day in 2016, a number projected to increase to nearly 5,000 transactions per day by 2025.[8]

Dataism

In 2008, Chris Anderson, then-editor of *Wired*, wrote an article articulating a viewpoint that has come to be called Dataism. Anderson asserted that data had supplanted the scientific method:

> *This is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves.*[9]

Do numbers speak for themselves? Is the invisible hand of dataflow a panacea for all individual and societal ills? There is no doubt that data is transforming our lives, but this phenomenon is taking place in an environment of uncertainty and rapid technological change, and so decisions on how our data can be used has implications for our future. We need to ensure that Big Data works *for* us, not just *on* us.

We need to ensure that Big Data works *for* us, not just *on* us.

Behind the Electronic Curtain

The basic Internet business model today is to collect all possible information from and about individual users and monetize that data for use in targeting ads at the individual level. Just how this happens is largely invisible to consumers, who are unaware of evolving browser tools and technologies that enable companies to track an individual's activities across multiple devices such as smartphones, tablets, desktop computers, and other connected devices, and even link that data with offline activities such as purchases in brick-and-mortar stores and information in public records.

One of the touted benefits of data-driven online businesses is that they can deliver personalized content. With the power of Big Analytics, websites and companies can target consumers with content designed to appeal to them, based on their interests as inferred from captured data streams. Of course, the prime objective of this expansive collection of personal information and employment of sophisticated algorithms is profit from targeted advertising. Targeted, data-based advertising is more effective—generates more clicks and sales—than advertising addressed to broad demographic categories of viewers.[10]

Privacy Harms

Consumers vaguely understand that being inundated with advertisements online is the price of "free" access to the Internet's trove of information and services, but most are not happy about this deal. In a nationwide survey of adults conducted online by the National Cyber Security Alliance, respondents ranked concern about not knowing how their personal information is being collected or used higher than becoming a victim of crime or not being able to get health care. The same survey found 65 percent of Americans somewhat or strongly agreed that they are not able to control how their information is used or shared online, and two-thirds would accept less personalized content, including fewer discounts, in order to keep their personal information private.[11]

While some individuals may view advertising "personalized" for them as of more interest or less annoying than non-targeted ads, there are also privacy harms resulting from the use of personal information in this way. Someone who has been followed around the web by an ad for a pair of shoes or Viagra or another product previously clicked on may experience a certain level of discomfort or anxiety from realizing he or she is being surveilled; this is one type of intangible privacy harm.[12] Someone who receives ads based on a medical condition revealed by online searches may feel very uncomfortable indeed.

Such concern is not unjustified. Businesses know about all our online activities, but we remain in the dark about what information they're collecting, what they're inferring from it, and what they're doing with it. The results of this information asymmetry can be tangible as well as subjective. Mathematician Cathy O'Neill, author of *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, warns that companies are using data to direct people to certain goods and services and to offer prices based on how much they think an individual can pay: "Travel sites show fancier hotels to Mac users, auto insurance companies charge more to customers who are less likely to comparison shop, payday lenders focus on people whose search queries show signs of desperation."[13]

O'Neil and other researchers also describe the use of secret algorithms to profile and sort individuals into groups based on weaknesses and vulnerabilities identified by their online activities. These individuals may then be targeted with predatory ads for for-profit colleges or payday loans.[14] In 2016, the California Attorney General won a $1.1 billion judgment against Corinthian Colleges for their predatory and unlawful practices. The complaint included Corinthian's practice of targeting a low-income demographic

> *which it describes in internal company documents as composed of "isolated," "impatient" individuals with "low self-esteem," who have "few people in their lives who care about them" and who are "stuck" and "unable to see and plan well for future," through aggressive and persistent internet and telemarketing campaigns and through television ads on daytime shows like Jerry Springer and Maury Povich.*[15]

Big Data can also be used by websites to steer consumers to particular products or to set prices based on their inferred willingness or ability to pay, in ways that can be unfair or even discriminatory. In 2012, a *Wall Street Journal* investigation found that the Staples website set different prices based on what it inferred to be the user's location.[16] Legal scholar Ryan Calo has written about the power of digital market manipulation, the result of information asymmetry, where companies are able reach out to consumers even before they come to market and use what they know about individuals to take advantage of their vulnerabilities.[17]

Even when we think we are anonymous online—when we haven't registered with a website for example—we likely are not. The sheer volume of data coming in from different sources makes it possible to link individual data to specific people, even when some datasets have been intentionally de-identified by removing key elements such as names or Social Security numbers. One example of the process of re-identification was reported by Professor Latanya Sweeney of Harvard. She purchased de-identified hospital discharge data from the State of Washington and was able to correlate

that dataset with newspaper accounts of accidents in the same time period. She was able to re-identify 43 percent of a sample of 81 accident victims in the hospital discharge data by matching fields common to both sources. Sweeney also noted that predictive analytic companies were big buyers of publicly available health data.[18]

In the service of commerce, the algorithms of Big Analytics are increasingly exposing and monetizing some of the most intimate aspects of our lives—details about our health, who we know, what we think, what we do in the privacy of our homes. In the midst of this assault, how do various privacy laws in the United States and abroad attempt to address these invasive practices?

Privacy Law and Market Failure

The majority of nations protect privacy as a fundamental human right, but the U.S. Constitution does not provide an express guarantee of privacy.[19] Privacy rights in our Constitution are "penumbral"; that is, they are implied by the Bill of Rights rather than explicitly stated. For example, privacy in speech, reading, and association is seen as being protected by the First Amendment, and the privacy of the home against quartering soldiers and unreasonable search and seizure by the Third and Fourth Amendments. Notably, these individual rights are only protected against government action, not against infringing actions of businesses or other organizations.[20]

The United States also differs from other developed countries in Europe, Asia, and the Americas in its statutory law on privacy. Many other countries have comprehensive privacy laws, but the United States does not. Since the 1990s, the federal government has avoided enacting broad privacy laws and instead relied on market mechanisms, notably the failed notice-and-choice regime to regulate the Internet and its related businesses.[21] (As will be discussed later, "notice and choice" is the practice whereby a website or app notifies consumers of its privacy practices with a posted "privacy policy" statement, and consumers then have some degree of choice about the terms offered.)

Federal privacy law, where it does exist, is narrowly sectoral. It is made up of statutes, regulations, and judicial decisions that apply only to certain industries (such as finance, or health care) or certain types of data (such as children's data, drivers' records, video rental data). In the absence of specific privacy laws, the default in the United States is that when it comes to flows of information, the free market prevails, including the market for personal information.

By contrast, the EU considers privacy as a human right essential to the respect for human dignity. In the European Conventions of Human Rights of 1950, privacy is addressed as the "right to respect for private and family life." Similarly, in the EU Charter of Fundamental Rights in 2000, privacy is conceived as respect for private and family life, the home and communications, as well as the protection of personal data. This right is implemented in comprehensive privacy laws

intended to protect the rights of individuals over their own personal data. The default in the EU is that personal data should *not* be processed (that is, collected, stored, used, and so on). Any data processing that does take place must meet standards of transparency, legitimate purpose, and proportionality.[22]

An update of EU privacy law, which will take effect on May 25, 2018, seeks to strengthen and harmonize the law across all member nations. The General Data Protection Regulation (GDPR) creates new individual privacy rights and extends its application to companies that process personal data about EU individuals, even when a company is not located in the EU. The new privacy rights include the "right to be forgotten" (have one's personal data erased in certain situations), data access and rectification (access to or a copy of one's own personal data and correction of inaccuracies) and data portability (transfer one's personal data from one company or platform to another).[23]

While the EU approach has been criticized by some as overly rule-bound, resulting in companies in some countries focusing more on paper compliance than on practical privacy practices,[24] it has often proven more effective in protecting data privacy than the U.S. approach of light-touch regulation and reliance on market forces.

Regulatory Failure: Unnoticeable Notice and Illusory Choice

The foundational principles of data privacy law are actually U.S. in origin, first formulated in 1973 by the U.S. Department of Health, Education, and Welfare in its Fair Information Practice Principles (FIPPs).[25] The FIPPs were then expanded and codified by the Organisation for Economic Co-operation and Development (OECD) in 1980, with the agreement of member countries, including the United States. Intended to support the control of individuals over their own personal data in the hands of organizations, the FIPPs form the basis of many modern international privacy agreements and national laws. The eight FIPPs in the OECD version are Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness or Transparency, Individual Participation, and Accountability.[26]

In most U.S. privacy law, these eight principles have devolved to just two, which have come to be called Notice (Openness or Transparency) and Choice (Use Limitation). A company *notifies* consumers of its policies and practices regarding personal information, and then consumers *choose* whether or not to accept the terms. The failure of this approach is evident, both in the privacy notices that are difficult to notice and understand, and in the choices that are illusory.

In a best practices guide on crafting meaningful privacy policies, the Office of the California Attorney General described their current shortcomings:

> *Dissatisfaction with the effectiveness of privacy policy statements has grown over time. As the use of personal information in commerce has expanded in scope and complexity, comprehensive privacy policy statements have tended to become lengthier and more legalistic in style, yet often fail to address data handling practices of concern to consumers or offer them meaningful choices about the collection and use of their data. The typical policy's ineffectiveness as a consumer communication tool has been borne out by research findings that consumers do not understand, and many do not even read, the privacy policies on the web sites they visit.* [27]

Where they are available, privacy policies usually fail to address critical issues, such as what a company does with the personal information it collects, what entities it shares the information with, what those entities do with it, and how long the information is retained.

The choices offered to consumers regarding the collection and use of their personal information generally boil down to take it or leave it, all or nothing. That is, all too often, the only choice consumers are given is either to accept a company's privacy policy, however unsatisfactory it may be, or decline to use their product. If any specific choice is offered, it tends to be the choice to opt out of allowing the company to share the consumer's personal information with other companies for use in marketing. But the default is to let companies share the data. Since the consumer is unlikely to have read the policy providing this choice and thus likely to fail to opt out, this lack of action is regarded as consent to sharing of the data. Furthermore, some websites and apps start collecting information the moment a user lands on the site or opens the app, before privacy policy notifications have even been given.

Moving Beyond Notice and Choice

One approach to a new privacy framework beyond unnoticeable notice and illusory choice is to offer consumers a full, robust spectrum of privacy settings to choose from, rather than the all-or-nothing approach. Such a framework would be based on three elements: more privacy choices, default to privacy, and a reasonable standard of care for data.

More choices means offering consumers gradations of choice, options between all and nothing. For example, consumers now sometimes have choices about the geolocation information collected by their mobile devices: (1) allowing an app no access to geolocation, (2) allowing access only when the app is being used, or (3) allowing the app to access geolocation data at all times. Rather than simply offering option 3 or nothing, this policy would mean providing additional options as well.

Default to privacy means calibrating default settings to limit the collection of personal information. Even when an online

service provides a privacy policy, it generally comes too late; only after our information has been collected are we able to learn about it. This "grab it first, explain later" approach seems unfair in the growing network of sensors that are collecting information on us as we move through our neighborhoods and even inside our own homes. A better architecture for choice is to set privacy-respectful defaults and give the user the choice to change the setting. This type of architecture not only gives consumers more real control, but also serves as an incentive for companies to provide a privacy notice that is easier to find and easier to understand than we generally see today.

Data security is an essential condition for privacy protection: we can't have privacy without it. The Internet of Things is increasing the volume of data collected and stored, and daily reports of data breaches have made us all aware of the challenges of securing information and of the costs of failing to do so. A clear articulation of a *reasonable standard of care for data*, based on existing laws, jurisprudence, and technical standards, would go a long way to define at least a basic level of security.

Such a framework could inform efforts to update U.S. privacy laws, to move beyond mere notice and choice.

Market Failure: IoT Insecurity

Security guru Bruce Schneier is among many who have called the insecurity of the Internet of Things (IoT) a market failure, with no market solution, because the insecurity is to a large extent an externality, affecting neither buyers nor sellers but other people.[28] Of course, an insecure device can also be turned against the consumer who purchased it, who was focusing on price and features rather than on security.

This is a vitally important matter for privacy (security is a necessary component of privacy) and for cybersecurity. The insecurity of the Internet of Things—made up of smart TVs and toys, electric meters and thermostats, webcams and alarm systems, fitness wearables and smart watches—imperils not just individuals' personal information, but puts their health and safety and that of society as a whole at risk.

The IoT is also one of the sources contributing to the phenomenal growth of the datasphere. The number of Internet-connected devices has been increasing rapidly in recent years. In early 2017, Gartner, the IT research and advisory firm, estimated that the number of devices would surpass global population that year, with 8.4 billion connected devices for 7.6 billion people. Other estimates put the number of devices even higher, forecasting as many as 20 billion of them by 2025.[29]

Connected devices are used in business and industry, on streets and highways and in public buildings. But the biggest component of the IoT is consumer devices, connected things in our homes, our cars, and on—or even in—our bodies.

These billions of things are collecting and transmitting information in a space traditionally regarded as private and protected. The interaction of all these devices with each other and with the companies that sell them and those that carry their data is making our home networks ever more complex. And we may not realize it, but we are in the position of being the chief information officer (and the chief information security officer and chief privacy officer) of our own networks, a responsibility for which few of us are equipped.

The IoT has significant privacy implications. For example, smart meters collect data about gas and electricity consumption at the household level that can reveal information about activities in the home, including when residents are away and whether the home has an alarm system and how often it is activated.

Siemens in Europe has summarized the privacy threat represented by the smart grid: "We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live. From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data."[30]

Medical devices and other connected wearables collect very sensitive information, which raises questions of who is getting this data, and what they are doing with it.[31] Smart toys, digital personal assistants, TVs and other devices that use speech recognition may record and store conversations in our homes, including those with guests who are unlikely to have consented, even if we passively and unknowingly have.

IoT devices have user interface constraints that make it difficult or impossible to provide notice of privacy practices, consumer choices or controls. Imagine trying to find or read a privacy notice on a router or a smart appliance. Furthermore, the companies that make these devices tend to lack experience with privacy and security. In summer 2017, the possibility that the makers of Roomba, the robot vacuum, would share the floor plans the device makes of the homes its device cleans made headlines. The public reaction led the company to speak to privacy issues, ultimately saying that they would not share data with third parties without the informed consent of customers. Exactly how they might advise consumers of the possibility and get their consent was not disclosed.[32]

The privacy concerns related to the IoT are not insubstantial, but it is their insecurity that imperils individuals' health and safety and puts our society as a whole at risk. The *Homeland* episode in which the vice president is killed by a hacker who remotely manipulates his pacemaker is not pure fiction. In recent years, medical device manufacturers have become aware of security bugs in pacemakers, defibrillators, and insulin pumps. In October 2016, Johnson & Johnson warned patients of security vulnerability in one of its insulin pumps that a hacker could exploit to cause patients to receive a dangerous overdose of insulin.[33]

Another danger of insecure IoT devices was demonstrated in 2016 by the spread of the Mirai malware that took down websites and entire networks in fall 2016. The large-scale attack was carried out by a botnet of enslaved consumer devices: insecure security cameras, routers, and DVRs whose owners were unware that their devices were responsible for spreading the malware.[34]

Botnets of insecure IoT devices have the potential to put vast computing power at the disposal of criminals and nation states. The financial services sector, a target because that's where the money is, recognizes IoT as a top vector for cyber-security attacks.[35] The IoT weak link poses a similar threat to other sectors, including the hydroelectric power industry. The vulnerability of the sector to cyberattacks was made public in a March 2016 indictment by U.S. Attorney General Loretta Lynch of Iranian-government-sponsored hackers who were able to penetrate the controls of a small New York dam. The indictment also charges the same Iranian hackers with cyberattacks on major U.S. banks.[36]

As Schneier explains, the manufacturers of IoT devices have neither the expertise nor the financial incentives to make their products more secure. They are designed and built for features and low price, not for security. And unlike other computer hardware, these devices are not configured to receive updates with security patches. We update our phones and computers by installing patches and we replace them every few years. This is not the case with DVRs, or connected TVs, thermostats, or other appliances; we replace them at much longer intervals. The only feasible way to update most IoT devices is to toss them and buy a new model.

We know what the vulnerabilities of IoT devices are and how they can be addressed. A report published by the Broadband Internet Technical Advisory Group (BITAG) in November of 2016, in the wake of the Mirai botnet, outlined the privacy and security improvements needed to prevent the devices from allowing unauthorized users to take them over, mount cyberattacks, conduct surveillance and monitoring, induce device or system failures, leak data, and harass authorized users.[37]

It's not that we don't know what to do; it's that the market isn't letting it happen.

Big Tech and Federal Retrenchment

As discussed above, evidence of the failures of the law and the market to protect privacy abound. The speed of technological evolution outpaces and outdates the law, and the role of the tech industry in resisting efforts to update the law has become significant. In recent years, the tech industry has been active in Washington and increasingly in state legislatures, and has had considerable success in defeating stronger privacy legislation on the grounds that it will stifle innovation.[38] For example, in California last year, the tech industry mounted a vigorous campaign that successfully

stalled, if it did not quite kill, a privacy bill for Internet service providers (ISPs) that would provide for more effective notice and more meaningful choice.[39]

The Electronic Communications Privacy Act (ECPA) is a prime example of a law that has been rendered inconsistent and irrational by technological developments. Enacted in 1986, before the Web, the Cloud, and social media existed, ECPA now gives government very broad access to online communications stored on third-party servers, as opposed to, say, private storage devices in an individual's home. This result is inconsistent with ECPA's original purpose of achieving "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement"; updating the ECPA so that it more closely strikes that balance has been the goal of privacy advocates and tech companies for years.[40] Unfortunately, these efforts have been unsuccessful to date, with opposition coming both from law enforcement and from civil agencies.[41]

Data security, an essential component of privacy protection, is another issue on which industry opposition has long stymied Congressional action. In spite of years of well-publicized data breaches, Congress has not been able to pass legislation setting data security standards for companies that handle personal information. Not only were such proposals opposed by industry, but the Chamber of Commerce resisted even a voluntary program of cybersecurity for critical infrastructure companies developed in response to Executive Order 13636 by President Obama, arguing against any new regulatory regime.[42]

In spite of years of well-publicized data breaches, Congress has not been able to pass legislation setting data security standards for companies that handle personal information.

While Congress has remained gridlocked on addressing the shortcomings in U.S. privacy law, the Trump Administration has been pursuing retrenchment, rolling back existing privacy regulations and reining in enforcement agencies.

The most obvious move to date is the repeal of the broadband privacy rule, which imposed privacy obligations on broadband Internet access service providers (commonly known as ISPs). The rule was adopted by the Federal Communications Commission (FCC) in 2016. Urged by the newly installed FCC chair, Ajit Pai, Congress invoked the Congressional Review Act to hurriedly pass S.J. Res. 34 in March 2017, overturning the broadband privacy rule before it had taken full effect. The repeal also prohibited the FCC from introducing similar rules in the future.

The FCC had adopted the broadband privacy rule after a long battle between cable, telecom, and other technology

companies on the one hand, and consumer privacy and civil liberties advocates on the other. The FCC held public hearings and published a draft version that received public comments for six months. The hasty action to nullify the rule, under cover of Congress's effort to repeal the Affordable Care Act, contrasts strongly with the public deliberation accorded its passage.[43]

This action was a serious blow to privacy protection. The broadband privacy rule recognized the privileged position ISPs hold as gatekeepers to the Internet, a position that provides them with a broad and deep view into every aspect of their customers' online activities. The rule outlined a reasonable privacy regime to give individuals strong data security protections and more control over the use of their personal information by their ISPs. As noted in comments from the California Attorney General,

> *the privacy rule responds to this situation by providing privacy-respectful defaults and more effective user-centric privacy notices, which together enable meaningful customer choices. The schema for customer choice in the proposed rule is based on alignment with customer expectations, with the greatest control granted for uses of customer [personal information] that are not required for the provision of the broadband service and are thus likely to be unexpected by the customer.*[44]

States Can Lead the Way

In the face of inaction and retrenchment at the federal level, can we look to the states to move the ball on privacy? States have been the source of numerous privacy innovations in past years, including laws on identity theft victim rights, data breach notification, limitations on the use of Social Security numbers, cell phone data privacy, cybersecurity, and cyber-exploitation (sometimes known as "revenge porn"). States have served as laboratories in the privacy arena, with legislative innovations that originated in one state often being picked up in other states and sometimes—as in cases of identity theft victim rights, Social Security number restrictions, and data breach notification—in federal laws or regulations.

The new regulatory development occurring in the EU provides an opportunity for states to rebuff the industry critique of state privacy regulation as a patchwork and instead work to harmonize state privacy laws upward. When it takes effect in May 2018, the GDPR will apply not only to any companies based in Europe, but also to many U.S. companies that do business online that results in their collecting, processing, or maintaining information on European residents. With penalties for violation of up to 4 percent of global gross revenues, the GDPR is being taken seriously by U.S. companies.[45] As it turns out, the policies and procedures these companies are implementing to protect their European customers and employees can also benefit Americans as well—provided action is taken.

This report does not propose a comprehensive federal privacy law similar to that in the EU. Nor does it propose a new quasi-self-regulatory approach, such as the "information fiduciaries" concept described by Yale law professor Jack M. Balkin and Harvard law professor Jonathan Zittrain. They propose that companies could choose to be governed by a set of privacy practices based on the FIPPs in exchange for exemption from state privacy laws preempted by the federal government.[46] Either of these approaches would require significant legislative action at the federal level, which is highly unlikely in the present environment.

Rather, this report recommends that states continue to be innovative in privacy law, crafting legislation with an eye to taking advantage of the GDPR's requirements to enact stronger state privacy protections. Such an approach could result in a degree of "harmonization upward," ensuring that proposed legislation provides a level of privacy protection roughly equivalent to that of the GDPR. While this would not constitute a total harmonization—that is, it would not replace tenets of existing U.S. state laws with the rules embodied in the GDPR—it would have the advantage sought in many harmonization efforts of simplifying compliance for any businesses that are subject to EU regulation.

Among the most pressing privacy issues needing to be addressed are broadband privacy, IoT insecurity, and the need for interstate harmonization of data breach notification laws.

Broadband Privacy

Since the repeal of the FCC's broadband privacy rule in late 2017, nearly half the states have introduced legislation to fill the void, according to the National Conference of State Legislatures.[47]

Several of the pending bills are patterned generally after the FCC rule, aiming to provide the same level of protection for the broad swath of personal information available to ISPs.[48] They would require ISPs to get the consent of their customers before disclosing or selling personal information.

States should craft legislation that, rather than seeking the same level of consent for all customer information, should adopt the tiered approach to consent found in the now-repealed FCC rule. Customers should be given greater control over sensitive information, such as precise geolocation, financial and health information, web browsing and app usage history; the use or sharing of this type of information should require the affirmative, opt-in consent of the customer. The use or sharing of non-sensitive personal information, such as email address and type of service, should be allowed, unless the customer says no and opts out. And exceptions should be made for the use of information necessary for providing the contracted service and certain other emergency situations.

While this degree of individual control is not currently provided by most U.S. privacy laws, the central and privileged position of ISPs certainly justifies moving in this direction. In other countries, individuals are afforded more control over their own personal information. The GDPR sets a very high standard for consent to the processing of personal data. An individual's consent must be "freely given, specific, informed and unambiguous" and a clear affirmative action is required.[49] The requirements of the former FCC rule regarding the contents of the notice describing the choices available to customers and for the mechanism by which customers can exercise or revoke their choices went a long way to providing for meaningful consent approaching the GDPR level. State broadband privacy laws should incorporate the consent provisions that had been part of the FCC rule.

This approach is in line with the new privacy framework outlined above, providing consumers with more choices and setting privacy-respectful defaults.

Securing the IoT

Cybersecurity has been a hot topic in Congress for a number of years, with ever-larger data breaches keeping it on the front burner, but numerous efforts to enact broadly applicable cybersecurity legislation have failed. There have also been some congressional hearings and legislative proposals for cybersecurity for the IoT. Even though the attack of the Mirai botnet of consumer devices increased policy makers' awareness of the problem, it remains unlikely that Congress will act anytime soon. And the threat that this insecure attack vector poses continues to grow with the increase in the number of connected devices.

This is an issue on which states might innovate, looking for legislative approaches to correct the market failure by setting minimum security requirements for connected devices. Legislation might narrow the focus to consumer devices, those intended for "personal, family or household purposes," in the language of laws regulating consumer products and services. This would exclude IoT used in business, industry, and government, where organizations have far greater resources and expertise to address the security issues than do consumers on their own. A narrower focus would also somewhat reduce the political burden of passing the legislation.

Legislation might look to the BITAG report discussed above, which outlines the major security vulnerabilities and recommends current best practices for securing IoT devices. The report's recommendations include the following:

- ensure that devices have a mechanism for automated secure software updates, a capability that does not currently exist for most IoT devices;

- use strong authentication by default, to prevent unauthorized parties from accessing devices or changing their code

or configuration;

- test and harden all possible device configurations, not just the default configuration, to ensure that any customization by consumers is secure; and

- protect data with security and cryptography best practices, to protect against data leaks both from the cloud and between devices.[50]

These requirements would constitute privacy defaults and an appropriate standard of care for data, components of the new privacy framework discussed above.

The GDPR might also be consulted on this issue. One of its requirements is data protection by design and default, whereby companies must consider data protection at the outset, when designing systems for processing personal data.[51] The data security requirement in the GDPR would also be relevant. It is risk-based: organizations must implement appropriate technical and administrative measures to ensure a level of security appropriate to the risk.[52]

Harmonizing State Data Breach Notification Laws

One of the most innovative and influential privacy laws originated in a state. In 2003, California enacted the first law requiring organizations to notify individuals of a security breach of personal information. The law made an economic adjustment, shifting most of the burden and cost of data insecurity from individual data subjects to the organizations responsible for it. In addition to alerting individuals that their information is at risk so that they can take defensive action, breach notification requirements have provided an incentive for companies and other organizations to pay attention to and devote resources to data security and privacy.

California's law was followed by similar laws in forty-seven other states, as well as federal regulations and guidelines for health care entities and financial institutions.[53] It has also been taken up by other countries, and will be a requirement of the impending GDPR.[54]

Urged by industry complaints about the compliance burden created by multiple laws, Congress has attempted for over a decade to pass a federal data breach notification law that would preempt state laws. In addition to having an overly broad preemptive scope, some of these federal proposals would have negated not just state data breach laws, but also longstanding consumer protection provisions, and thus would have lowered the level of consumer protection and prevented further improvements. In the current situation, the protections of the strongest state laws—the highest common denominator—are generally afforded to the residents of all states in a multi-state breach.

In the current situation, the protections of the strongest state laws—the highest common denominator—are generally afforded to the residents of all states in a multi-state breach.

State data breach notification laws make a good candidate for harmonization across state jurisdictions, particularly as an alternative to federal preemption,[55] because it would not be that difficult to simplify the pattern in the patchwork of state breach laws.

State breach laws are in fact very similar, following in most respects the original California law.[56] Like California's, the other state laws require organizations to notify individuals when personal information is breached, prefer notification by mail but allow alternative "substitute notice" in some situations, permit a law enforcement delay, and offer an exemption from notification if the breached data is encrypted.

The significant differences between state laws are in three provisions: (1) the notification trigger, (2) notification timing, and (3) the definition of covered information. This is where harmonization efforts should be directed. Such an effort by state policy makers could result in simplifying compliance while preserving consumer protection and other benefits of state regulation. Below is a proposal for approaching the harmonization of state breach laws, with the added benefit of aligning more closely with federal and European breach notification requirements.

Toward a Harmonic Convergence

On the important issue of the *trigger for notification*, the state laws take one of two approaches: over three quarters of the state laws have a harm trigger, requiring notification only if the breached entity judges that the incident poses a risk of harm to individuals; the others have an acquisition trigger, requiring notification if the data was acquired or reasonably believed to have been acquired by an unauthorized person. In a sense, both approaches are based on a risk of harm, with acquisition by an unauthorized person seen as constituting such a risk.

These approaches could be harmonized by using an acquisition trigger and adding a presumption that the breached entity must notify when a breach of personal data has occurred—unless the entity finds through a risk assessment that the incident is very unlikely to result in harm to affected individuals. This would also necessitate reporting incidents to the state Attorney General or other government agency, as is currently required in over half the state laws, which would

have the authority to review decisions not to notify. Setting a breach size threshold to trigger reporting to regulators—but not for notifying individuals—would help reviewing agencies to prioritize the deployment of their limited resources. Currently, over half of state breach laws set such a threshold, ranging from 250 to 500 individuals affected.

This formulation of a notification trigger would also align with the Health Insurance Portability and Accountability Act (HIPAA) and the GDPR. Since 2009, HIPAA has required covered health care entities and their business associates to notify individuals in case of any impermissible use or disclosure of protected health information, *unless* the entity conducts a risk assessment and determines that there is a low probability that the information has been compromised. Similarly, the GDPR requires notification to individuals of a breach of personal data if the incident is determined to pose a high risk of harm to individual rights or freedoms. (The GDPR also requires notifying data protection authorities of breaches when there is any likelihood of harm to the rights or freedoms of individuals, even if the higher threshold for notifying individuals has not been reached.)

The other factor in a harm-based trigger is the definition of harm, which should be left as a general term to allow for different types of harm posed by different types of personal data and by evolving technologies and business practices. While some states limit harm to identity theft or financial harm, the majority of the state laws with a harm trigger employ a broad concept, using the terms "harm" or "misuse of the data." The GDPR also speaks broadly of "physical, material, or non-material damage," including being deprived of control over personal data.[57]

Harmonizing state laws on the *timing of notification* should not be difficult. A harmonized law using a formula such as "in the most expedient time possible, without unreasonable delay" could explicitly allow time for securing the system and determining the scope of the breach and for conducting a risk assessment in order to determine whether notification is required. This would align with the GDPR, which requires notification of individuals "without undue delay" and allows time to assess the level of risk to individuals.

While existing state laws do not provide for a risk assessment, essentially all of them do require notification "in the most expedient time possible" or "without unreasonable delay" and allow for time to secure the system and determine the scope of the breach. Nine states specify an outer limit of 30 to 90 days from discovery of the breach. Similarly, the HIPAA regulation requires notification "without unreasonable delay," allowing up to 60 days. The problem with specifying an outside time limit is that it tends to become the norm. The flexibility of a "without unreasonable delay" standard encourages timely notification of very different incidents. What is considered a reasonable delay in the case of notifying of a breach involving a data owner and one or more contracted service providers and many data subjects

whose contact information is not readily available would likely be considered an unreasonable delay in the case of a breach of a single system involving fewer data subjects. The pressure to notify promptly is felt by organizations, as they are faced with justifying the time they took to the public when the incident is reported in the news.

Harmonizing on the *definition of covered information* for breach notification laws is more challenging. There is diversity among the states on this point. While all state breach notification laws have basic data types in common (name plus Social Security number, driver's license number, or financial account number), after these, the picture becomes more complicated. A third of the state laws also include medical information, a third of the laws include biometric data, nearly a third include online account credentials, and the same number add other data elements (such as passport number, taxpayer ID number, mother's maiden name).

More nimble than Congress, state legislatures have adapted the definition of personal information in breach notification laws to respond to changing circumstances affecting their residents.

More nimble than Congress, state legislatures have adapted the definition of personal information in breach notification laws to respond to changing circumstances affecting their residents. The original California law contemplated financial identity theft as the risk to be addressed by notification, and therefore limited the types of personal information covered to those sought by identity thieves. Five years later, with the burgeoning of medical privacy and medical identity theft, the definition was expanded to include medical and health insurance information. Two years later, the California law was amended again to add online account credentials to the definition of covered information, in response to the targeting of that data by criminal organizations. This evolution is an example of laboratories of innovation at work.

Allowing continuing updating of the law on this issue is important to keeping breach notification effective. Before adding new types of data, however, states would be wise to consider the purpose served by the law: transparency. While the requirement to notify serves as an incentive to organizations to improve their privacy and security practices, that is a secondary effect of the law. (An information security statute that prescribes specific security standards is another matter.) The authors of the original breach notification law stated that its intent was to give consumers early warning that their personal information was at risk of being abused, allowing them to take action to protect themselves.[58] Bearing this purpose in mind, certain types of information might be excluded from or not added to the definition in the state laws, if knowing that it has been breached does not enable individuals to take defensive action.

Certainly differences in state breach laws can complicate compliance for companies that experience a breach affecting

residents of many states. In response, charts and matrices of state breach laws have been developed and are readily available to assist in navigating the terrain.[59] Smaller companies, such as medical and other professional practices and local merchants, often have personal data only on the residents of their state, and thus need comply with only a single law.

Conclusion

While the present political environment at the federal level is unlikely to produce a radical strengthening of data privacy law, there are privacy problems that should not await federal action at some unknown future date. The lack of privacy protections for the ISPs that have access to the broadest swath of our online activities, the insecurity of the IoT devices in our homes, and the possibility of companies gaining legal justification for hiding some breaches that put our data at risk of misuse are issues that state legislatures can address.

States have been responsible for some of the most innovative and effective privacy laws. Today, states have the opportunity to take advantage of a far-reaching European privacy law to enact laws requiring U.S. companies to provide their domestic customers and employees with at least some of the same privacy protections that they accord Europeans. Functioning as the laboratories of democracy that U.S. Supreme Court Justice Louis Brandeis envisioned, states can respond to changing conditions and evolving technologies with new approaches to privacy protection. They can also learn from each other, adopting provisions and laws that prove effective.

Notes

1. Taylor Amerding, "The 17 biggest data breaches of the 21st century," CSO Online, January 26, 2018, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.
2. Lee Matthews, "FBI Warns Parents About the Dangers of Connected Smart Toys,"*Forbes*, July 18, 2017, https://www.forbes.com/sites/leemathews/2017/07/18/fbi-warns-parents-about-the-dangers-of-connected-smart-toys/#33a77d0439e6; James Vlahos, "Barbie Wants to Get to Know Your Child,"*New York Times*, December 17, 2015, https://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html.
3. David Ingram, "Facebook says data leak hits 87 million users, widening scandal," Reuters, April 4, 2018, https://www.reuters.com/article/us-facebook-privacy/facebook-to-revise-terms-of-service-to-include-more-privacy-language-idUSKCN1HB2CM; Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *New York Times*, March 21, 2018,https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.
4. "Data Age 2025: The Evolution of Data to Life-Critical," International Data Corporation (IDC), April 2017,

https://www.seagate.com/our-story/data-age-2025/.

5. “Big Data: Seizing Opportunities, Preserving Values,” Executive Office of the President, May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

6. John Raidt, “7 Great Ways That Data Can Benefit Society,”*U.S. Chamber of Commerce Foundation*, May 23, 2016, https://www.uschamberfoundation.org/blog/post/7-great-ways-data-can-benefit-society-0; Jennifer Bresnick, “How Healthcare Big Data Analytics Helps Build Smart Societies,” *HealthITAnalytics*, Aug. 14, 2017, https://healthitanalytics.com/news/how-healthcare-big-data-analytics-helps-build-smart-societies; Tom Hardy, ”Significant Benefits of Big Data Analytics in Healthcare Industry,” *Built in Los Angeles*, Jan. 12, 2016, https://www.builtinla.com/blog/significant-benefits-big-data-analytics-healthcare-industry.

7. Internet World Stats, World Internet Users and 2017 Population Stats, June 30, 2017, http://www.internetworldstats.com/stats.htm; “Data Age 2025,” 16.

8. “Data Age 2025,” p. 14.

9. Chris Anderson, “The End of Theory: The Data Deluge Makes the Scientific Method Obsolete,” June 23, 2008, https://www.wired.com/2008/06/pb-theory/.

10. Howard Beales, “The Value of Behavioral Targeting,” Network Advertising Initiative, 2010, https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (study sponsored by Network Advertising Initiative found that “behaviorally-targeted advertising secured an average of 2.68 times as much revenue per ad as non-targeted ‘run of network’ advertising”).

11. “Perceptions of Privacy Online and in the Digitally Connected World,” National Cyber Security Alliance, January 2015, https://staysafeonline.org/wp-content/uploads/2017/09/Perceptions-of-Privacy-Online-and-in-the-Digitally-Connected-World.pdf.

12. See Daniel J. Solove, “Conceptualizing Privacy,” *California Law Review* 90, no. 4 (2002): 1087, 1088–93 ; and M. Ryan Calo, “The Boundaries of Privacy Harm,” *Indiana Law Journal* 86, no. 3 (2011): 1131, 1132.

13. Cathy O’Neil, “The Dystopian Future of Privacy Discrimination,”*Bloomberg View*, March 16, 2017, https://www.bloomberg.com/view/articles/2017-03-16/the-dystopian-future-of-price-discrimination.

14. Cathy O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*(New York: Crown Publishers, 2016); “The Scoring of America,” World Privacy Forum, 2014, https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

15. “Attorney General Kamala D. Harris Obtains a $1.1. Billion Judgment against Predatory For-Profit School Operator,” March 23, 2016, https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-obtains-11-billion-judgment-against-predatory; California Attorney General Kamala D. Harris, “Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief,” *People v. Heald College, LLC; Corinthian Colleges, Inc., et al*, October 2013, https://oag.ca.gov/system/files/attachments/press_releases/Complaint%2C%20filed%20stamped_0.pdf.

16. Jennifer Valentino-DeVries, Jeremy Singer-Vine, and Ashkan Soltani, “Websites Vary Prices, Deals Based on Users’ Information,” *Wall Street Journal*, December 24, 2012,

https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

17. Ryan Calo, "Digital Market Manipulation," *George Washington Law Review* 82, no. 4 (2014): 995, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703.

18. "Maximizing Disclosure Risk in HHS Open Data Initiatives, Session 3: What Are the Re-Identification Threats to Releasing Federal Data to the Public?" Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, September 29, 2014, https://aspe.hhs.gov/report/minimizing-disclosure-risk-hhs-open-data-initiatives/session-3-what-are-re-identification-threats-releasing-federal-data-public.

19. Ten U.S. states do have an explicit privacy right in their constitutions. See National Conference of State Legislatures, Privacy Protections in State Constitutions, at www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

20. See, for example, Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, May 2008).

21. "Framework for Global Electronic Commerce," The White House, July 1997, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

22. Directive 95/46, European Data Protection Directive (1995), and its successor, Regulation (EU) 2016/679, the General Data Protection Regulation (2016).

23. Regulation (EU) 2016/679, General Data Protection Regulation, https://gdpr-info.eu/.

24. Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Mass.: MIT Press, 2015).

25. Robert Gellman, "Fair Information Practices: A Basic History," April 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020.

26. *Collection Limitation:* There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. *Data Quality:* Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date. *Purpose Specification:* The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. *Use Limitation:* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law. *Security Safeguards:* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. *Openness:* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. *Individual Participation:* An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily

intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. Accountability: A data controller should be accountable for complying with measures, which give effect to the principles stated above. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Co-operation and Development, 1980, at https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

27. California Attorney General, "Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy," May 2014, 4, https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

28. Bruce Schneier, "Security Economics of the Internet of Things," Schneier on Security, October 10, 2016, https://www.schneier.com/blog/archives/2016/10/security_econom_1.html.

29. "Gartner Says 9.4 Billion Connected 'Things' will be in use in 2017, Up 31 Percent from 2016," Gartner, February 7, 2017, https://www.gartner.com/newsroom/id/3598917; "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," Statista, 2018, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Statistics portal drawing on many sources puts number of devices at 20 billion in 2017, rising to 75.4 billion by 2025).

30. Gerard Wynn, "Privacy concerns challenge smart grid rollout," Reuters, June 25, 2010, https://www.reuters.com/article/us-energy-smart/privacy-concerns-challenge-smart-grid-rollout-idUSTRE65O1RQ20100625.

31. See, for example, Adam Tanner, "Strengthening Protection of Patient Medical Data," The Century Foundation, January 10, 2017, https://tcf.org/content/report/strengthening-protection-patient-medical-data/.

32. Maggie Astor, "Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared," *New York Times*, July 25, 2017, https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

33. Jim Finkle, "J&J warns diabetic patients: Insulin pump vulnerable to hacking," Reuters, October 4, 2016, https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L.

34. Sean Gallagher, "How one rent-a-botnet army of cameras, DVRs caused Internet chaos," *Ars Technica*, October 25, 2016, https://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/.

35. "Today's Cyber Security Threats to the Financial Sector," *Business World*, April 12, 2017, http://businessworld-usa.com/todays-cyber-security-threats-to-the-financial-sector/.

36. Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html; Dustin volz, Jim Finkle, "U.S. indicts Iranians for hacking dozens of banks, New York dam," Reuters, March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

37. "Internet of Things (IoT) Security and Privacy Recommendations: A Technical Working Group Report," Broadband

Internet Technical Advisory Group, November 2016, http://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php.

38. "California Tech sector now an inside political player," *Sacramento Bee*, August 9, 2014, www.sacbee.com/news/politics-government/article2606285.html ("…unlike many sectors that are cutting back on such efforts, Big Tech is expanding its participation in politics, whether that's support for particular candidates or lobbying on issues important to the industry"); "Silicon Valley increasing its lobbying in California's Capitol," *Los Angeles Times*, February 28, 2015, www.latimes.com/local/politics/la-me-pol-tech-sacramento-20150301-story.html (Uber, Lyft, Airbnb fight efforts to regulate them); "Apple, Amazon and Google spent record sums to lobby Trump earlier this summer," *Recode*, July 21, 2017, www.recode.net/2017/7/21/16008504/apple-amazon-google-record-lobby-trump-immigration-science-privacy (Focus of lobbying efforts is on immigration, taxes and privacy).

39. "How lobbyists convinced lawmakers to kill a broadband privacy bill,"*Ars Technica*, October 25, 2017, https://arstechnica.com/tech-policy/2017/10/broadband-privacy-rules-would-help-terrorists-lobbyists-told-lawmakers/ (While the bill would only have applied to ISPs, the broader tech industry and advertising groups joined the opposition, fearing that privacy restrictions would eventually spread to other online companies). AB 375 (Chau) passed the Assembly and was put on inactive file in the Senate. It is eligible for consideration in 2018, the second year of the California Legislature's two-year session. The text of the bill, committee analyses, and additional information are available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375.

40. See Senate Report No. 99-541, to accompany S. 2575, October 17, 1986, at www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf.

41. "The Strange Case against ECPA Reform," Cato Institute, April 11, 2011,https://www.cato.org/blog/strange-case-against-ecpa-reform; "Give Reasons to Reform ECPA Now," Center for Democracy and Technology, September 4, 2013, https://cdt.org/blog/five-reasons-to-reform-ecpa-now/; "Civil Agencies, Law Enforcement Official Threaten Meaningful ECPA Reform," Association of Research Libraries, ARL Policy Notes, May 25, 2016, http://policynotes.arl.org/?p=1372; Reed Smith, "ECPA Reform Legislation on the Horizon (Again)," *Technology Law Dispatch*, August 4, 2017, https://www.technologylawdispatch.com/2017/08/privacy-data-protection/ecpa-reform-legislation-on-the-horizon-again/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

42. Alexei Alexis, "President Obama Signs Executive Order on Cybersecurity, Seeks Voluntary Standards,"*Bloomberg BNA*, February 18, 2013,https://www.bna.com/president-obama-signs-n17179872423/.

43. Kimberly Kindy detailed Congress's action in "How Congress dismantled federal Internet privacy rules,"*Washington Post*, May 30, 2017,www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?utm_term=.d0cf577c6de2.

44. California Attorney General, "Comments on WC Docket No. 16-106: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," July 6, 2016, https://ecfsapi.fcc.gov/file/10707370900670/CA%20AG%20BROADBAND%20PRIVACY%20COMMENTS%207.6.16%20(1).pdf.

45. "Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets,"*PwC*, https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html (Over half of U.S. multinationals

say GDPR is their top data-protection priority; 77% plan to spend $1 million or more on GDPR compliance).

46. Jack M. Balkin and Jonathan Zittrain, "A Grand Bargain to Make Tech Companies Trustworthy,"*Atlantic*, October 3, 2016, https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (Those who handle the money or estates of others have a fiduciary duty to act in a trustworthy manner in the interest of another. Information fiduciaries, such as doctors, attorneys and accountants, have an obligation to handle other people's information only in the interests of those people, including keeping it confidential.)

47. "Privacy Legislation Related to Internet Service Providers," National Conference of State Legislatures, December 29, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx.

48. See, for example, California's AB 375, Oregon's H.B. 4155, and Hawaii's HB 2296.

49. Article 4(11), GDPR, https://gdpr-info.eu/art-4-gdpr/.

50. See note 37.

51. Article 25, GDPR, https://gdpr-info.eu/art-25-gdpr/ and Recital 78, GDPR, at https://gdpr-info.eu/recitals/no-78/.

52.

53. Health Insurance Portability and Access Act (HIPAA), Breach Notification Rule,https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Federal Financial Institutions Examinations Council, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, https://www.fdic.gov/news/news/financial/2005/fil2705a.pdf.

54. General Data Protection Regulation (GDPR),https://gdpr-info.eu/.

55. California Attorney General Kamala Harris recommended harmonization of state data breach laws as an alternative to a preemptive federal statute in the "California Data Breach Report," February 2016, https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

56. Mintz Levin, "State Data Security Breach Laws," September 2017,https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

57. Recital 75, GDPR, https://gdpr-info.eu/recitals/.

58. See legislative committee analyses of SB 1386 (Peace) and AB 700 (Simitian) of 2002,www.leginfo.legislature.ca.gov.

59. For example, see Mintz Levin, "State Data Security Breach Laws," September 2017, www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf and Baker Hostetler, "Data Breach Charts," November 2017, www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf and "State Data Breach Law Summary," November 2017, www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf.

Joanne McNabb, Contributor

Joanne McNabb is a privacy consultant, providing organizations with research and recommendations on privacy issues and practices. McNabb was Director of Privacy Education and Policy in the California Attorney General's Office for five years, prior to retiring from state service in 2017. Ms. McNabb is a Certified Information Privacy Professional, with specializations in Government and Information Technology, a Fellow of the Ponemon Institute, a research center on privacy, data protection and information security policy, and a member of the Consumer Interest Forum of the American National Standards Institute. She attended Occidental College and holds a master's degree in Medieval Literature from the University of California, Davis.