Consensus and Controversy in the Debate Over Federal Data Privacy Legislation in the United States

Müge Fazlioglu, CIPP/E, CIPP/US, Senior Westin Fellow

iapp

A lot of blood, sweat and tears have been spilled this year over privacy regulation in the United States. Indeed, at the beginning of 2019, legislative developments related to privacy and data protection at all levels of government showed no signs of slowing down. At the center of these developments has been the California Consumer Privacy Act. Since it was signed into law in June 2018, the CCPA has ignited heated discussions within privacy circles regarding its scope, provisions and exceptions and has forced privacy professionals to re-examine their organizations' practices and compliance efforts. According to Chad Marlow of the American Civil Liberties Union, the increasing number of state-level efforts to pass privacy laws indicates that states have reached a tipping point where, "if Congress is not willing or able to enact strong privacy laws, their legislatures will no longer sit on their hands."

In response to these developments, discussions within the U.S. Congress about passing a federal U.S. privacy and data protection law have intensified over the past few months. At the end of September 2018, the IAPP's Jedidiah Bracy, CIPP, covered the details of a Senate hearing about privacy legislation, sharing the initial reactions of key actors in the process. In another IAPP piece, Bracy wrote about the privacy advocacy groups that voiced their dissatisfaction with not being included in the hearings, which mostly involved representatives from industry.

As these tensions swelled in the first quarter of 2019, numerous lawmakers and organizations offered proposals or recommendations regarding a new federal U.S. data privacy law. To shine more light on the specific provisions that are being debated, we look here at a set of the most recent bills that have been introduced in Congress, including the Consumer Data Protection Act introduced by Sen. Ron Wyden, D-Ore., the Data Breach Prevention and Compensation Act of 2018 introduced by Sen. Elizabeth Warren, D-Mass., the Data Care Act of 2018 proposed by Sen. Schatz, D-Hawaii, in early December 2018, the Privacy Bill of Rights Act introduced by Sen. Edward Markey, D-Mass, the Algorithmic Accountability Act of 2019 introduced by Sens. Cory Booker, D-N.J., and Ron Wyden, D-Ore., and Rep. Yvette Clarke, D-N.Y., the Do Not Track Act introduced by Sen. Joshua Hawley, D-Mo., the Designing Accounting Safeguards to Help Broaden Oversight and Regulation on Data introduced by Sens. Mark Warner, D-Va., and Josh Hawley, D-Mo., and the Information Transparency and Personal Data Control Act introduced by Rep. Suzan DelBene, D-Wash.

Further, we also examine a selection of recommendations made in comments submitted to the National Telecommunications and Information Administration from across government, industry and advocacy organizations in response to a set of desired privacy outcomes. These broad outcomes include transparency, control, reasonable minimization, security, access and correction, risk management and accountability.

Lastly, we identify several areas of broad agreement, as well as pointed disagreement regarding the nature, shape and scope of a potential federal U.S. data privacy law.

Proposals from Lawmakers

Internet Bill of Rights

In October 2018, Rep. Ro Khanna, D-Calif., released the Internet Bill of Rights Principles, which was endorsed by the founder of the World Wide Web, Tim Berners-Lee. Khanna's Internet Bill of Rights incorporates EU General Data Protection Regulation–like provisions, such as data portability, the right to access and the right to be forgotten, in addition to provisions regarding anti-discrimination, net neutrality and accountability.

These principles built upon President Barack Obama's 2012 proposal for the Consumer Privacy Bill of Rights and were developed with input from former Federal Communications Commissioner Mignon Clyburn and former U.S. Chief Technology Officer and Technology Advisor for President Obama Todd Park, as well as representatives from Uber, Twitter, Amazon, Facebook, Microsoft and the Electronic Frontier Foundation.

The 10 principles of the Internet Bill of Rights are:

- The right of access to and knowledge of companies' personal data collection and use.
- Opt-in consent for personal data collection and its sharing with third parties.
- In certain contexts, the right to "obtain, correct, or delete personal data controlled by any company and to have those requests honored by third parties."
- Ensuring the security of personal data and providing data breach notifications.
- Data portability, or the right to "[m]ove all personal data from one network to the next."
- The right to network neutrality, or "[t]o access and use the internet without internet service providers blocking, throttling, engaging in paid prioritization, or otherwise unfairly favoring content, applications, services, or devices."
- The right "[t]o internet service without the collection of data that is unnecessary for providing the requested service absent opt-in consent."
- The right to access "multiple viable, affordable internet platforms, services, and providers with clear and transparent pricing."
- Prohibiting exploitation and unfair discrimination based on personal data.
- Ensuring "reasonable business practices" and accountability.

The Consumer Data Protection Act of 2018

On Nov. 1, 2018, Sen. Ron Wyden, D-Ore., released a discussion draft of the Consumer Data Protection Act, along with a section-by-section analysis and one-page summary

of it. In addition to expanding consumers' privacy rights, this bill would give the Federal Trade Commission more authority and additional regulatory commitments.

Above all, the CDPA would recognize non-economic injury in privacy protection through an amendment to the FTC Act that would encompass business practices that create a "significant risk of unjustified exposure of personal information" when considering "harmful" business practices. Moreover, the CDPA would establish a national Do Not Track system for consumers to opt out of their data being shared with third parties. For companies that offer their products or services on the condition that a consumer shares their personal data with them, they can offer a paid version of those products and services. The bill also requires that the charge for this paid version cannot be more than what the entity would earn through the sale of the personal data.

Regarding sanctions, the CDPA would authorize the FTC to impose civil penalties of up to $50,000 per violation and 4% of an organization's annual revenue. It would also require senior executives — namely, the "Chief Executive Officer, Chief Privacy Officer and Chief Information Security Officer" — of companies with more than $1 billion per year of revenue or data on more than 50 million consumers to file annual reports to the FTC on their privacy and security compliance measures. If an executive approves a false statement in one of these annual reports, the law imposes personal liability and criminal penalties of up to 20 years in prison.

Further expanding the FTC's authority, the law would also authorize the FTC to create regulations to "establish and implement minimum privacy and security standards" and provide people the opportunity to review the information companies have about them, to know which third parties are receiving their data, "challenge inaccuracies," and require companies to conduct impact assessments for their "high-risk automated decision systems and high-risk information systems." It would also increase the number of FTC staff by establishing a Bureau of Technology within the FTC to be staffed by 50 new technical experts. In addition, it would authorize the FTC to appoint 100 additional staff members for the Division of Privacy and Identity Protection of the Bureau of Consumer Protection and 25 additional staff in the Bureau's Enforcement Division. The FTC would also be given the authority to establish resolution mechanisms for consumers' complaints regarding the CDPA — with the FTC acting as a bridge by communicating complaints to the companies and their responses back to consumers — as well as to establish minimum cybersecurity standards and require companies to conduct impact assessments regarding their "high-risk automated decision systems."

Social Media Privacy and Consumer Rights Act of 2018

The Social Media Privacy and Consumer Rights Act of 2018, which aims to provide privacy protection for social media and online platform users, was introduced by Sen. Amy Klobuchar, D-Minn. The SMPCRA defines terms such as "covered online platform," "geolocation information" and "personal data." It also creates rules on transparency, such as the forms of providing the terms and conditions of the online platforms' operations, the privacy and security program that the platform needs to establish, and the rules on changing them, and it provides users with

rights, such as the opportunity to easily withdraw their consent, the right to access their information and the right to see a list of the third parties that have received personal data from the platform through "sale or other means."

Data Breach Prevention and Compensation Act of 2018

Introduced by Sen. Elizabeth Warren, D-Mass., in January 2018, the Data Breach Prevention and Compensation Act would create an Office of Cybersecurity within the FTC, which would be tasked with implementing and overseeing the law. The provisions of the law address system and network security, network management and monitoring, application management and data security. While targeted at credit-reporting agencies, in reality, "any collected database of typical consumer data that is used for almost any purpose and is communicated to another party" would fall within the regulatory scope of the law.

Under the DBPCA, businesses would have to inform the FTC's Office of Cybersecurity about their cybersecurity measures, demonstrate that they follow reasonable data security practices and notify it of data breaches no later than 10 days following the breach. Penalties would amount to $100 for each consumer whose first and last name (or first initial, last name and at least one other piece of personally identifying information) were disclosed, as well as an additional $50 for each additional piece of personally identifying information of each consumer compromised in the breach. Fines would be limited, however, to 50% of the business's annual revenue from the previous year or 75% if they failed to notify the FTC of the breach in a timely manner or violated another regulation.

Innovative and Ethical Data Use Act of 2018

Intel Corporation also laid out its own full proposal for a federal privacy law, the Innovative and Ethical Data Use Act of 2018. The law focuses on the principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The proposal also envisions more enforcement authority and resources for the FTC, including "[t]he ability to enforce meaningful but fair sanctions."

More specifically, the law would encourage organizations to allow users to provide "meaningful consent" for data use and to create mechanisms whereby they can make "informed choices." Under this law, organizations would need to "narrowly and specifically" describe their purpose for data collection, while making room for individuals to object to the continued holding of incorrect data or to data whose use may "disproportionately cause harm." It would also require organizations to adopt "reasonable" security measures to protect personal data, as well as implement "robust" privacy programs to reduce the risk of data misuse and breaches.

Data Care Act of 2018

The Data Care Act of 2018 was introduced in the Senate by Sen. Brian Schatz, D-Hawaii, Dec. 12, 2018. The bill defines key terms such as "individual identifying data" and "sensitive information" and contains sections on the duties of online service providers and enforcement by the FTC. Namely, the bill would require online service providers to "fulfill the duties of care, loyalty, and confidentiality" to end users. To fulfill the duty of care, companies would have to "reasonably secure individual identifying data from

unauthorized access" and promptly inform them of any data breaches. Adhering to the duty of loyalty would mean a company could not use individual identifying data in a way that would "benefit the online service provider to the detriment of an end user," "result in reasonably foreseeable and material physical or financial harm to an end user" or "be unexpected and highly offensive to a reasonable end user." Lastly, the bill's duty of confidentiality would impose restrictions on the disclosure and sale of individual identifying information to third parties.

Privacy Bill of Rights Act

This bill contains a definition of "personal information" that is substantially similar to the one contained in the CCPA. Like other bills, it would enhance the authority of the FTC to enact regulations granting individuals the right to be notified about various aspects of data processing by covered entities, be able to condition entities' collection and use of data on their opt-in consent, access their information in a "portable electronic table," correct inaccurate personal information and request deletion. The act would also require the FTC to prohibit certain practices, such as linking deidentified data back to a specific individual or device or using "take-it-or-leave-it-offers," whereby an entity refuses to serve individuals who do not consent to the processing of their personal information. It would also enable the FTC to prohibit entities from offering a financial incentive "that relates the price of a product or service to the privacy protections afforded the individual." Finally, as the act states that a violation of one of its provisions would amount to "an injury in fact" to the individual, it would grant a private right of action to individuals to sue entities for privacy-related injuries.

Algorithmic Accountability Act of 2019

Relatively narrower in scope, this bill would require the FTC to promulgate regulations that require covered entities to conduct "automated decision system impact assessments," as well as data protection impact assessment of existing and any new "high-risk" automated decision systems that they employ. Covered entities would be required to conduct these "as frequently as the Commission determines is necessary" and "if reasonably possible, in consultation with external third parties," such as independent auditors and technology experts. Covered entities would then be required to "reasonably address" the results of these impact assessments "in a timely manner."

Do Not Track Act

The Do Not Track Act, introduced by Sen. Joshua Hawley, R-Mo., would require the FTC to establish and enforce a Do Not Track system "to protect consumers from unwanted online data harvesting and targeted advertising." To do so, the bill gives the commission the authority to create a program that individuals can download that would send DNT signals to websites, online services and applications of an individual's choice. Covered entities would also be required to search for the DNT signal of devices that connect to their websites, services and applications. The bill would then prevent covered entities from collecting data — "other than such data as is necessary" for the operation of its website, service or application — using that data for a secondary purpose, such as targeted advertising, or sharing the data with third parties unless the user "expressly consents." Third-party operators that receive DNT signals would also be prohibited from collecting data from users, apart from "data collected for the purpose of analyzing how or whether the user engaged" with the

website, service or application. This type of data, however, may only be collected in a deidentified manner and may not be used to create a profile of the user from whom it was collected. Covered entities would also be prohibited from denying access to services or providing different levels of access or service to users who employ the DNT signal.

Covered entities would also have to notify users who are not using the DNT that it is available from the public website of the FTC. Entities would also have to notify users not sending the DNT signal about their collection of any data "beyond what is necessary" for it to operate the website, service or application. Critically, the act considers data that is collected "for the purpose of displaying targeted advertisements" to fall under this definition of "more data than is necessary."

In terms of penalties, those for actions that constitute a "negligent violation" would not be in excess of $50 per affected user, while penalties for actions that constitute a "will or reckless violation" cannot be less than $100,000 but would also not exceed $1,000 per affected user.

Designing Accounting Safeguards to Help Broaden Oversight and Regulation on Data

Another bill introduced by Sens. Mark Warner, D-Va., and Josh Hawley, R-Mo., is aimed at forcing social media companies to disclose how they monetize user data. The DASHBOARD Act, a bipartisan piece of legislation, would require services with more than 100 million monthly active users to disclose the types of data they collect, as well as to assess the value of that data. Covered commercial data operators would also be required to file annual reports on the "aggregate value" of the user data they collect and any contracts they have entered into with third parties that involve data collection. Moreover, the bill would give users the right to request the deletion of all or individual fields of data that commercial data operators have collected about them.

Information Transparency and Personal Data Control Act

Introduced by Rep. Suzan DelBene, D-Wash., the Information Transparency & Personal Data Control Act is intended to give consumers more control over their data by implementing an opt-in model of collection and "plain English" privacy policies. Like other proposals, it would enhance the authority of the FTC, giving it greater power to fine companies while also increasing the number of full-time FTC staff by 50 (15 of whom must be "technical experts") and its budget by $35 million. The bill would also require companies to acquire "privacy audits" by "a neutral third party" and submit those results every other year to the FTC.

Of note, the bill considers "sensitive personal information" to encompass genetic data, geolocation data and information about religious beliefs and sexual orientation.

Other Draft Bills

Several other bills are reportedly in the works, although drafts of them have not been yet introduced or made publicly available. In the Senate, Commerce, Science and Transportation Committee Chairman Sen. Roger Wicker, R-Miss., along with fellow members Sens. Jerry Moran, R-Kan., Richard Blumenthal, D-Conn., and Brian Schatz, D-Hawaii, has been working for several months on a bill that would, according to Senate aides, enhance the FTC's powers and preempt state privacy laws.

Recently, Sens. John Thune, R-S.D., and Maria Cantwell, D-Wash., were reported to have joined this effort or been independently working on separate bills. A framework for a separate bill developed by Cantwell would include "a private right of action, new restrictions for online advertising, and expanded rulemaking and fining authority for the FTC." While Blumenthal has supported a private right of action, Wicker has said, "We're not going to have a private right of action. It's totally a non-starter." In addition, Blumenthal and Moran are reportedly working on another bill that would preempt state laws and give both state attorneys general and the FTC more enforcement authority. One aide reported that some members of Congress believe that the inclusion of "pre-emption language to override state laws would be necessary to pass a bill in this Congress."

In the House of Representatives, meanwhile, Reps. Anna Eshoo and Zoe Lofgren, both Democrats from California, have reportedly circulated a draft proposal that would include a private right of action and also establish a new data protection authority. Most recently, an effort has been led by Rep. Jan Schakowsky, D-Ill., in the House Energy and Commerce Committee to introduce a bill toward the end of September or early October, as well as hold one or two hearings on data privacy over the next few months.

Analysis of Federal Privacy Law Proposals

Taken together, these bills serve as useful indicators of where federal U.S. privacy legislation is currently headed. To parse out what a potential federal privacy law would look like, we further analyzed each bill for the presence of several key privacy rights and data protection mechanisms: the right of access, correction, deletion and portability of personal information; requirements for opt-in consent; private right of action; and requirements for data breach notifications and risk assessments.

Most Common Provisions:

- Right of access.
- Right to correct inaccurate information.
- Right to delete personal data.
- Opt-in consent.
- Data breach notifications.

Least Common Provisions:

- Right to data portability.
- Private right of action.

The most common provisions were the right of access, the rights to correct and delete personal information, some form of opt-in consent, and data breach notifications, which were each present in five of the 11 bills analyzed in this section. Provisions requiring some sort of privacy or data protection risk assessments were the next most common, being present in four of 11 bills. The least common provisions were the right to data portability and the private right of action, each of which were only present in 2 of the 11 bills.

See Table 1, "Presence of Provisions in Federal Data Privacy Bills," page 14.

Comments Submitted to the NTIA

The results of the Request for Comments "on ways to advanced consumer privacy while protecting prosperity and innovation," released by the National Telecommunications and Information Administration in September 2018 are voluminous. By mid-November of last year, more than 200 individuals, government entities, and companies — from Amazon to Zebra Technologies — had submitted recommendations to the NTIA regarding what it should and should not do with

respect to consumer privacy, addressing the NTIA's list of desired outcomes, including transparency, control, data minimization, security, access and correction, risk management and accountability.

It is helpful, therefore, to summarize the recommendations provided in comments submitted by individuals, advocacy groups, companies and government entities. In particular, we unify these comments around several core themes where broad consensus seems to exist, while also identify key areas of disagreement.

Most parties seemed to agree on the benefits of harmonizing the fragmented legal landscape in U.S. privacy and data protection, the cross-sector or "technology-neutral" application of such a law, the central role of the FTC in enforcing its provisions, and the prudence of pursuing a risk-based approach.

Opposing recommendations were made concerning whether the law should resemble the EU General Data Protection Regulation, as well as whether it should preempt privacy protections afforded by state laws.

Points of Consensus

On the whole, the individuals and groups that submitted comments to NTIA expressed support for its espoused outcomes as general guiding principles for any federal privacy law.

Most of the comments submitted elaborated on why a particular outcome was important, how their own work and initiatives served to promote that outcome and what more could be done at a practical level to advance that outcome. They also often explained why legislation that intends to support that outcome should or should not include certain provisions.

Harmonization

Nearly all the organizations that submitted comments voiced support for the goal of reducing fragmentation in U.S. privacy and data protections laws and bringing greater harmony to the regulatory landscape. As Amazon put it, this should be done to "avoid a patchwork of obligations that will burden organizations and confuse users." Speaking to the increase in economic efficiency that a federal privacy law could bring about, the Network Advertising Initiative noted that the "patchwork" of state privacy laws in the United States "inevitably raise compliance costs for businesses."

Access Now, which clearly expressed its support for state privacy laws, even conceded that the statement from NTIA that this kind of fragmentation "naturally disincentivizes innovation" was "superficially true." Google also noted that, although "meaningful and effective privacy protections" already exist in domestic law, including at the state level, "we can improve upon the current framework with a comprehensive baseline privacy law" that would codify longstanding privacy principles and bring unity to the U.S. approach.

Technology-Neutral Application

Many organizations also voiced support for the idea that a federal privacy law should apply across all sectors of the economy, rather than being limited to a particular type of company. For example, AT&T argued that the law should "appl[y] comprehensively on a technology-neutral basis." Google wrote that "organizations are increasingly competing across sectors, and a regulatory regime should apply in a manner neutral to industry, technology, and business model." Similarly, Amazon commented that "any action addressing consumer privacy should be applied

comprehensively across private sector organizations that use personal data." In its comments, the European Commission also suggested that NTIA's goal of harmonizing the regulatory landscape would be served "through a set of overarching principles that would apply to all business activities previously not covered by sectoral laws."

Authority of the Federal Trade Commission

Most organizations envisioned the FTC playing the lead role in the enforcement of any new privacy and data protection regulations. Intel, for example, proposed that the FTC's authority be expanded, while others, such as Charter Communications, suggested the idea of expanding the power of the FTC is at least worth considering. The American Civil Liberties Union pointedly argued that "the FTC should be given authority to levy civil penalties in consumer protection actions," while Columbia University Professor Steven Bellovin similarly recommended that the FTC's authority to take action against security and privacy breaches "should be enhanced by statute." The Association of Research Libraries also argued that the FTC should have greater enforcement powers, "including the ability to impose meaningful fines from companies who fail to comply with privacy standards."

On this point, those from within industry also tended to agree. The Network Advertising Initiative, for example, not only suggested that "the FTC is well suited to leverage its longstanding experience and expertise to remain the primary administrator of consumer privacy and data protection laws," but also noted that consumers would benefit from increased resources going to FTC enforcement. Numerous proposals also pointed out that the FTC's privacy division is currently understaffed, with Brave noting that the FTC has only 60 staff working on privacy enforcement versus the 180 staff of the Irish Data Protection Commissioner.

While acknowledging the pre-eminent role of the FTC as the U.S.'s privacy enforcer, some entities also used the opportunity to call for greater clarity about which privacy and data protection practices are reasonable and unreasonable. For example, a coalition of advertising associations, led by the Association of National Advertisers, proposed that a federal U.S. privacy law define "per se 'unreasonable'" data practices, or, more specifically, actions that violate the FTC Act, and "per se 'reasonable'" data practices, or those that "create little to no risk of consumer harm" and would thus be permissible.

Risk-Based Approach

The NTIA refers to "risk-based flexibility" as the "heart" of its approach, and numerous entities endorsed its proposal's incorporation of a risk-based approach. Explaining a hallmark feature of risk-based regulation, Google stated in its comments that "[e]nforcement and remedies should be proportional to the potential harms involved in the violation." It further suggested that "[b]aseline precautions should apply to any collection of personal information, and additional measures should account for the sensitivity of the underlying information and be proportionate to the risk of harm."

Some of the commenters, however, found the NTIA's reference to a risk-based approach to lack necessary specificity. The Center for Digital Democracy, which was one of the harshest critics of the NTIA's approach, noted that the NTIA's proposal "fails to elaborate on the approach of a 'risk-management' regime." Moreover,

CDD cautioned it against focusing on risks to business and economic risk at the expense of privacy risks and harms, recommending instead that it define risks broadly. In this vein, it also urged NTIA to develop methodologies "to assess the human rights, social, economic and ethical impacts of the use of algorithms in modern data processing." Similarly, the Center for Democracy & Technology advised NTIA to explicitly adopt the privacy risks compiled by the National Institute for Standards & Technology, which go beyond economic loss to include things like "diminished capacity for autonomy and self-determination, discrimination (legal or otherwise), and a generalized loss of trust."

Indeed, comments emphasized that a general mandate for organizations to conduct risk assessments may do little to nothing to enhance the rights of data subjects. As CDT explained, without firm legislative rules, calling for "risk management" would still allow businesses to have "considerable discretion to determine what risks individuals may assume." Access Now pointed out "there are many entities to which risk can be assessed — risk to the data processor, risk to the general public, or risk to the individual person, to name only a few." Thus, to avoid a situation in which entities collecting data solely focus on the risks to themselves, it advised the NTIA to ensure that the risk management elements in their approach refer "specifically and clearly to the risk of the person to whom the data pertains."

Points of Divergence

Resemblance to the GDPR

A major area of disagreement among the proposals involved whether a comprehensive federal U.S. privacy law should resemble the GDPR. For example, the proposal from Brave, an open-source web browser launched in 2016, recommended that the federal law adopt the features of or build upon the standards of the GDPR, including its approach to purpose specification and the concepts of data controller and data processor. Brave's proposal further claimed that the burden the GDPR imposes on small- and medium-sized companies has been "overstated," arguing rather that the GDPR's "robust" approach to purpose specification will "help restrain large tech platforms from leveraging their dominant positions in one line of business by cross-using data accumulated in that line of business to dominate other lines of business too." The Future of Privacy Forum suggested that a U.S. privacy law "should also consider notable privacy provisions" of the GDPR "and address issues of interoperability where feasible." Google expressed its support for the GDPR's notion of legitimate interests, which it described as "a meaningful way to permit standard or typical data uses that are consistent with individuals' interest while reserving express consent to those situations where individuals need to pause and consider their choice."

In its comments, BSA | The Software Alliance also urged that the administration incorporate the GDPR-based distinction between data controller and data processor into its privacy approach, imposing different levels of responsibility upon each. Similarly, Brave wrote that the NTIA's desired outcome of accountability "requires the concepts of 'data controller' and 'data processor' … to be established in law." On this point, Google also noted "the need to clarify obligations based on an organization's ability to meet" certain obligations. It further elaborated upon the distinction between processors and controllers as an example of where separate responsibilities and accountability regimes should be in place.

The Association of National Advertisers, by contrast, voiced its disapproval with recent privacy legislation, including the GDPR and the California Consumer Privacy Act, referring to these as "misguided approaches." In plain terms, the Network Advertising Initiative stated that it "does not believe the GDPR is an appropriate model for U.S. privacy regulation." More specifically, it contended that "the GDPR and the CCPA have adopted an overly broad definition of sensitive information, and this is one of the areas where a national privacy framework could benefit from a more thoughtful, flexible approach." Likewise, TechFreedom argued it would be "a profound mistake" for the U.S. to model its privacy legislation upon the GDPR.

Preemption of State Law

U.S.-based companies may want a preemptive federal U.S. privacy law because they expect it "to be less restrictive on the gathering and use of personal data than, for example, CCPA." Indeed, statements in favor of preemption were mostly made by private companies or industry groups. The National Retail Federation, for example, argued that "without effective preemption of state law, Congress would simply add another data privacy regulation to what may eventually become a 50-state regulatory regime, where the U.S. laws fall within a larger, unworkable global regulatory gauntlet for businesses as state, national and multi-national laws all potentially conflict." Similarly, the Network Advertising Initiative argued that it "supports the adoption of a new federal privacy law that reduces the complexity of compliance through preemption of state privacy laws, which inevitably will become conflicting." The Future of Privacy Forum also recommended that a federal privacy law take exiting legal frameworks into consideration "by preempting certain state laws where they create conflicting or inconsistent requirements."

On the other end of the spectrum, organizations that are critical of a preemptive federal U.S. privacy law worry that it would "invalidate a host of existing protections for sensitive information like Social Security Numbers, student data, and more." For example, in its comments to NTIA, Access Now argued that federal preemption of state data privacy laws will "undermine the protection of data." Moreover, privacy advocacy groups, as well as other organizations that oppose federal preemption, have insisted that state governments are nimbler than the federal government and thus "more adept at responding to new challenges." The ACLU also noted that state laws that overlap with federal regulations in other areas have "historically allowed state[s] to fill gaps that federal regulators simply do not have the resources or expertise to address."

Such groups have therefore advised the NTIA to keep preemption out of the proposal or to strictly limit its scope. Noting the decline in consumers' trust in online commercial services, Brave explicitly called for "a federal law of an equal or higher standard than state laws." Similarly, the ACLU argued that "federal privacy standards should be a floor — not a ceiling — for consumer protections." The Electronic Privacy Information Center urged for federal legislation to act as a "baseline" that "ensures minimal protections while still preserving state and local innovation in response to new developments." A group of privacy law scholars also noted their opposition to "wholesale pre-emption of state privacy laws and enforcement," instead recommending that NTIA "consider a cooperative federal-state approach that better recognizes the reality of strong state regulatory capacities in this space."

As an example of what preemption could look like, Intel's privacy bill preempts the civil provisions of state laws that are focused on privacy, personal data, collection and processing. It does not, however, preempt state constitutions or laws regarding trespass, contract or data breach notifications, tort laws, laws related to fraud, laws that extend the protections offered by federal privacy laws, such as the Health Insurance Portability and Accountability Act, or private contracts based on state law that provide additional privacy or security protections to individuals.

(For more on preemption, see Alston Bird's Peter Swire's analysis of preemption in the privacy sphere, published in two parts by the IAPP.)

Analysis of Support for Provisions in a Sub-Sample of Public Comments to NTIA

As with the proposed bills, we also measured the prevalence of certain rights and mechanisms within the recommendations submitted to NTIA. These included the right to access, correct and request deletion of personal information; the right to data portability; a requirement to obtain opt-in consent for the collection and processing of personal data; a private right of action or redress mechanism; data breach notifications; and risk assessments.

Among these, the most commonly mentioned provision was the right of access. Approximately 61% of organizations in the sub-sample expressed support for a federal U.S. data privacy law that would grant users the right to access or know about the data companies had collected from them. Almost half of them (48%) also supported a provision that would give users the right to correct or delete information they had provided to a company.

The next most-popular provisions were data breach notifications and risk assessments. Slightly more than 4 out of every 10 entities that submitted comments to NTIA expressed support for a provision that would require companies to notify users in the event of a data breach. Roughly the same percentage also suggested that a requirement to perform risk assessments should be incorporated into the law. The least-popular provisions were the right to private action (32% recommended this), the requirement to obtain opt-in consent (27% recommended this) and, lastly, the right to data portability (23% recommended this).

See Table 2, "Support for Provisions within a Sub-Sample of Comments Submitted to NTIA," page 16.

Conclusion

By analyzing the proposals that have been put forth for a federal U.S. privacy law, as well as recommendations from across government, industry, and advocacy organizations, we have identified several areas of consensus and controversy.

Notably, a consensus seems to have emerged regarding the value, efficiency, and reduction of confusion that would be brought about by harmonizing the fragmented landscape of state privacy and data protection protections in the U.S. through the passage of a federal law. Moreover, given that companies in virtually every sector of the economy process personal data to some degree, there seems to be broad agreement that such a law should apply across the entire spectrum of private, as well as public, entities that process personal data. Most

organizations also continue to see the FTC playing the primary role and even expanding its powers to enforce a federal privacy law. Lastly, the risk-based and outcome-based approach outlined by the NTIA was endorsed by most of the entities that commented on it.

As this analysis of legal proposals and recommendations demonstrates, law and policymaking in privacy and data protection is anything but straightforward. Crafting a piece of legislation that carves out reasonable exceptions, responds to constantly evolving technology and can be effectively operationalized is obviously a massive undertaking. The rapid pace of legislative developments and the diversity of voices involved in the discussions further add to the complexity of the process. Stakeholders from across industry, government and the public sphere are playing critical roles in shaping the federal U.S. data privacy law of the future. Whether or not the move toward federal legislation in privacy and data protection produces a new law "on the books" in the U.S. anytime soon, a long-awaited and much-needed national debate about such a law has begun.

Published 10/10/2019

Table 1. Presence of Provisions in Federal Data Privacy Bills

Bill	Sponsors	Right of access	Right to correct or delete PI	Right to data portability	Opt-in consent	Private right of action	Data breach notifications	Risk assessments
Consumer Data Protection Act of 2018	Sen. Ron Wyden	X	X		X			X
Data Breach Prevention and Compensation Act	Sen. Elizabeth Warren						X	X
Innovative and Ethical Data Use Act of 2018	Intel Corporation		X			X	X	X
Data Care Act of 2018	Sen. Brian Schatz						X	
Internet Bill of Rights	Rep. Ro Khanna	X	X	X	X		X	
Social Media Privacy and Consumer Rights Act of 2018	Sen. Amy Klobuchar	X					X	
Privacy Bill of Rights Act	Sen. Edward Markey	X	X	X	X	X		

Bill	Sponsors	Right of access	Right to correct or delete PI	Right to data portability	Opt-in consent	Private right of action	Data breach notifications	Risk assessments
Algorithmic Accountability Act of 2019	Sens. Cory Booker and Ron Wyden; Rep. Yvette Clarke							X
Do Not Track Act	Sen. Joshua Hawley				X			
Designing Accounting Safeguards to Help Broaden Oversight and Regulation on Data	Sens. Mark Warner and Josh Hawley	X	X					
Information Transparency and Personal Data Control Act	Rep. Suzan DelBene				X			

Table 2. Support for Provisions within a Sub-Sample of Comments Submitted to NTIA*

* A marked box indicates only that the proposal explicitly favored inclusion of this right or principle, albeit with exceptions in some instances; an empty box should not necessarily be considered lack of support for or objection to inclusion (some entities are policy-neutral and took no position).

	Right of access	Right to correct or delete PI	Right to data portability	Opt-in consent	Private right of action	Data breach notifications	Risk assessments
Access Now	X	X		X	X		X
Amazon	X						
American Civil Liberties Union				X	X		
American Library Association							
Association of National Advertisers, et al.							
Association of Research Libraries		X	X	X		X	
Association for Computing Machinery	X	X				X	X
AT&T Services Inc.	X						X
Bellovin, Steven M.	X	X		X	X		
Brave				X		X	X
BSA | The Software Alliance	X	X					X
Californians for Consumer Privacy	X	X		X	X		
Center for Democracy and Technology	X	X	X				

	Right of access	Right to correct or delete PI	Right to data portability	Opt-in consent	Private right of action	Data breach notifications	Risk assessments
Center for Digital Democracy	X	X	X	X	X	X	X
Center on Privacy & Technology at Georgetown Law	X	X			X	X	
Centre for Information Policy Leadership	X	X				X	X
Charter Communications, Inc.				X			
Computer & Communications Industry Association	X	X	X			X	X
Consumers Union	X		X	X	X		X
Council of Better Business Bureaus							
DuckDuckGo							
Electronic Frontier Foundation	X		X	X	X	X	
Electronic Privacy Information Center	X	X			X	X	
European Commission	X	X			X	X	X
Federal Trade Commission Staff							
Future of Privacy Forum	X	X		X		X	X
Google	X	X	X			X	
GSM Association							

	Right of access	Right to correct or delete PI	Right to data portability	Opt-in consent	Private right of action	Data breach notifications	Risk assessments
Information Accountability Foundation	X	X					X
Intel Corporation					X		X
International Association of Privacy Professionals							
Internet Association	X	X	X			X	X
ISACA	X					X	X
Landua, Susan							
Motion Picture Association of America, Inc.							
Mozilla	X	X				X	
National Retail Federation							X
Network Advertising Initiative	X						
Privacy Law Scholars	X	X	X	X	X		X
Software & Information Industry Association	X	X	X			X	X
TechFreedom	X	X			X	X	
U.S. Public Interest Research Group	X	X	X		X	X	X
Verizon	X			X		X	
World Privacy Forum							