MLRC Media Law Resource Center
BULLETIN

2019 Issue No. 1 May 2019

LEGAL FRONTIERS IN DIGITAL MEDIA

520 Eighth Avenue, North Tower, 20th Floor, New York, NY 10018
www.medialaw.org | medialaw@medialaw.org | (212) 337-0200

Overview of Potential Data Privacy Legislative Proposals

By Jonathan H. Blavin and Zoe Bedell[1]

Since the beginning of 2018, several high-profile privacy scandals involving prominent U.S. technology companies have helped drive home for consumers—and legislators—the scope of many companies' data-sharing and handling practices, as well as the associated potential dangers and privacy concerns. In response, members of Congress from both parties have expressed significant interest in federal oversight of companies' use of personal data. Perhaps seeing the writing on the wall, some tech companies have also concluded that it's better to be part of the discussion to shape the solution. These forces have combined to generate a flurry of legislative proposals addressing various data privacy concerns.

In this article, we provide an overview of the major federal proposals currently being considered by Congress and the tech industry. While the approaches are varied, they raise a number of important issues for debate, including whether, and to what extent, a new national federal privacy law may preempt state privacy laws and how such a law would interact with (or replace) existing federal privacy laws; how much increased authority to give to federal agencies, such as the Federal Trade Commission, to craft and enforce new regulations in the privacy space; and whether consumers should have a private right of action to enforce a federal privacy law beyond the regulatory enforcement authority given to federal agencies.

The Current State of the Law

As an initial matter, there is currently no comprehensive legal regime governing data privacy. At the federal level, existing law focuses on specific sectors and types of data. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) provides privacy and security standards for medical and health information, while the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect sensitive customer information. Similarly, the Children's Online Privacy Protection Act (COPPA) imposes a number of federal requirements relating to the collection and use of data regarding minors under the age of thirteen. Companies also face a host of different regulations and requirements at the state level, the most common of which focus on reporting and disclosure requirements in the event of a data breach.

However, California in 2018 passed a first-of-its-kind comprehensive data privacy law, the California Consumer Protection Act, that could create significant new requirements for companies doing business on the internet. The CCPA creates several basic rights for California residents in their personal information:

- The right to know what personal information is being collected about them, and the right to access that information.

[1] Jonathan H. Blavin is a partner at Munger, Tolles & Olson. His practice focuses on high-technology privacy and platform liability disputes. Zoe Bedell is an associate in the Washington, D.C., office of Munger, Tolles & Olson, where she practices commercial litigation.

- The right to know whether their information is sold or disclosed, and to whom.
- The right to opt out of the sale of personal information.
- The right to have a business delete their personal information upon request (unless that information is necessary for a specified set of tasks).
- The right of individuals to equal services and prices, even when exercising their privacy rights.

In addition to disclosure and information sharing requirements intended to protect these rights, the law requires businesses to provide a link on the business's home page allowing consumers to opt-out of the sale of their information. (For consumers under the age of 16, businesses must obtain affirmative consent before selling any data.) And the right to equal services and prices means that businesses cannot deny, charge different prices for, or provide a different quality of goods or services to consumers who opt out, unless the difference is "reasonably related to the value provided to the consumer by the consumer's data."

The CCPA protects California residents and applies to for-profit businesses of a certain size that collect California residents' personal information. But given California's size and the difficulty in tailoring online experiences to users in different states, the law will likely have a sweeping effect on most companies doing business online in the United States.

California's law does not go into effect until 2020, and both privacy advocates and technology companies are trying to amend the law before then and/or influence implementing regulations to be adopted under the law (not surprisingly, with different goals in mind; Wired discusses some of the currently pending amendments here). However, the specter of a patchwork of sometimes conflicting and potentially stringent state-level privacy requirements—or even just the threat of having to comply with California's requirements—has further motivated some companies and legislators to prioritize uniform federal standards, including the possibility of a state-law preemption provision.

Focus on the Federal

Though there is a level of shared interest in some degree of federal oversight, consensus on the details has been slow to emerge. No bill introduced in 2018 made it out of committee (or in the Senate, out of the Subcommittee on Commerce, Science, and Transportation), and no bill introduced in 2019 has yet made it any farther. Moreover, the proposals all differ in important respects, including on fundamental topics like the FTC's role and authority, preemption of state laws, opt-in requirements, and the entities covered. The preemption point has proven particularly controversial. At this point, it is simply too early to guess at what consensus might ultimately emerge—or if Congress (and the Administration) will be able to reach an agreement at all.

Senate Proposals

American Data Dissemination Act of 2019 (ADD) (S. 142)

Senator Marco Rubio (R-FL) was the first out of the gate in 2019, introducing the American Data Dissemination Act of 2019 in January. His bill would impose privacy and security requirements on private businesses similar to what federal agencies already must comply with under the 1974 Privacy Act. However, the bill operates somewhat indirectly, requiring the FTC to generate proposals that Congress would then be able to consider, modify, and implement. (If Congress does not act within two years of the passage of the ADD, then the FTC could implement final regulations on its own.)

The ADD does provide the FTC with some guidance, directing the final resulting rules to apply to any person or entity that "provides a service that uses the internet" and "collects records"—in other words, nearly every business in the United States with a website. But in the interest of protecting innovation and ensuring that the regulatory environment does not entrench big tech corporations, the bill narrows its broad scope somewhat by directing the FTC to exempt small, newly formed businesses. In exchange for its fairly broad scope, however, the ADD and any resulting other laws or regulations would preempt any state laws that relate to any records covered by the ADD, or any other personally identifiable information.

The ADD also directs the FTC to include in its proposal (or final rule) requirements that allow consumers to access their data records and amend records that are shown to be "not accurate, relevant, timely, or complete." Covered businesses would also be required to keep an accounting of information disclosures about a user, making that accounting available to that user upon request. Finally, the FTC is required to develop a mandatory code of "fair information practices," though the bill does not dictate what must be covered within that code.

Social Media Privacy Protection and Consumer Rights Act of 2019 (S. 189)

Senators Amy Klobuchar (D-MN) and John Kennedy (R-LA) followed Senator Rubio, reintroducing their Social Media Privacy Protection and Consumer Rights Act at the beginning of January. Some of the bill's provisions are fairly modest in their aims. For example, the Act is somewhat conservative in its approach to the FTC, granting the agency enforcement power, but no new rulemaking authority. The bill would codify the "notice-and-consent" approach already common in the industry by requiring online platforms to develop and publish an easy-to-understand privacy program. Finally, the bill would protect users' expressed privacy preferences by preventing website operators from introducing new products or changes that override expressed preferences without first obtaining "affirmative express consent from the user."

But the bill breaks new ground in other areas. For example, it would create a right for users to access the personal data that a website has collected on them, including a list of who the website has shared the data with. It would also require websites to allow users to opt out of the collection of personal data. Unlike California's opt-out, however, online providers would be allowed to restrict or deny access to certain services, or the website entirely, if opting out "creates inoperability in the online platform." This undefined carve-out could create significant opportunities for tiered services based on privacy preferences.

The bill would also establish the first uniform federal standard for notifications in the event of a data breach or other transmittal of data in violation of the privacy programs—in other words, notification requirements would extend beyond hacking scenarios. Platforms would be required to notify users of the breach or violation within 72 hours. The notification must also provide users with the opportunity to withdraw their consent for the platform to collect their personal data and to demand that all their data be erased.

Whatever its other strengths or weaknesses, the Act as currently written is unlikely to satisfy most tech companies because it does not preempt state laws. In fact, similar to COPPA, states are encouraged to participate in enforcing the law, as state attorneys general or other state-authorized consumer protection officers are authorized to bring enforcement actions under the Act in federal district court. The section on state enforcement makes clear it should not be understood to preempt any state civil or criminal laws. However, also like COPPA, state officials must hold off if the FTC (the federal agency otherwise charged with enforcement authority) institutes a civil or administrative action regarding the same company and the same conduct. Identical provisions regarding state enforcement authority are included in many of the other legislative proposals in this area.

Privacy Bill of Rights

Senator Markey (D-MA) has introduced one of the more privacy-protective (and detailed) proposals of 2019, and while he does not yet have any co-sponsors, he does have the support of the digital rights groups Public Knowledge and Free Press. The Act directs the FTC to promulgate rules granting individuals rights to receive notice of companies' collection, retention, use, and sharing of their personal information; opt in to the collection and use of their information; access information about how companies use their data; correct errors; and request that companies delete their personal information. The Bill of Rights would also create a right of equal access that would prevent companies from denying or limiting services or from offering financial incentives to opt in. The Act would also prevent companies from using data for "unreasonable" purposes, such as profiting from biometric data or engaging in marketing that discriminates on the basis of race, religion, gender, or source of income. Companies are also prohibited from collecting more data than is "adequate, relevant, and necessary" for specified purposes.

The Act would generally be enforceable by the FTC, though certain entities (for examples, banks, insurance companies, or air carriers) would be regulated by agencies already primarily responsible for overseeing those industries, which is similar to the GLBA's enforcement provisions. Notably, the Act allows enforcement by state AGs *and* creates a private right of action allowing individuals to enforce their rights. This provision also renders unenforceable any pre-dispute arbitration agreement that relates to requirements under the Act or associated regulations, effectively amending the Federal Arbitration Act. The Act is silent on state law preemption.

Algorithmic Accountability Act (AAA)

Senators Wyden (D-OR) and Booker (D-NJ) introduced, in April 2019, a somewhat more narrowly focused bill concerned with automatic decision-making processes. The AAA would

require risk assessments for "high risk" automated decision systems (e.g., algorithms and other forms of machine learning/AI) that are particularly likely to pose a risk to privacy; create a danger of bias; involve personal information relating to sensitive characteristics like race, political opinions, religion, health data, gender, sexuality, or criminal convictions; or "systematically monitor[] a large, publicly accessible physical place." These risk assessments must evaluate the design and training of the system "for impacts on accuracy, fairness, bias, discrimination, privacy, and security." Covered entities must also conduct "data protection impact assessments" for high-risk information systems, evaluating "the extent to which an information system protects the privacy and security of personal information the system processes." These risk impact assessments would not have to be made public or shared with the FTC.

Deceptive Experiences to Online Users Reduction (DETOUR) Act

The bipartisan DETOUR Act, introduced by Senators Warner (D-VA) and Fischer (R-NE), is also more narrowly focused on preventing exploitative and deceptive practices by online operators that trick users into handing over their personal data. The Act takes aim at three practices. First, it would prevent large online operators from designing websites intended to manipulate users into providing their consent or obscure the choices that the user is making in consenting. Second, it regulates the psychological experiments conducted on website users without their consent. And third, it would prohibit web services designed to "cultivat[e] compulsive usage" among users under the age of thirteen. Enforcement and rulemaking authority would fall to the FTC under this proposal.

CONSENT Act (S. 2639) (2018)

2018 saw a flurry of legislative proposals, especially after the Facebook/Cambridge Analytica news broke. Senators Markey and Blumenthal were among the first to put forth a legislative proposal. The CONSENT Act does much as it name suggests: it requires websites to let customers know when their sensitive personal data is collected, used, or shared, and requires customers to opt in before a website can use, sell, or share (though not collect) that personal information. The bill also requires protection of anonymized data so that it cannot be re-associated with an individual, though the bill does not require data anonymization in the first instance. The Act would grant the FTC new rulemaking authority, with enforcement by the FTC and state AGs. The Act is silent on the question of preemption.

Data Care Act of 2018 (S. 3744)

This proposed bill of Senator Schatz (D-HI) takes a slightly different approach of creating fiduciary obligations—duties of care, loyalty, and confidentiality—on businesses collecting individual identifying data over the Internet. These terms are defined fairly broadly, and the bill does not list specific responsibilities or requirements with respect to data management practices. However, the bill does limit these duties. For example, the duty of loyalty would not stop a company from using a consumer's data to its benefit and at the consumer's expense unless doing so would result in "reasonably foreseeable and material physical or financial harm" or when the use would be "unexpected and highly offensive to a reasonable end user."

The bill grants the FTC authority to promulgate regulations under the Act, including regulations regarding data breach notification requirements. The FTC is also directed to determine guidelines for exempting categories of online service providers from compliance based on their size; the complexity, nature, and scope of their offerings; the sensitivity of the information they handle; and the costs and benefits of their compliance with the Act's requirements. State attorneys general and other consumer protection officers are empowered to enforce the Act, and the bill specifically provides that it should not be construed to prohibit state court proceedings for violation of state laws.

Consumer Data Protection Act (CDPA)

Senator Wyden (D-OR) posted this draft bill on his website at the end of 2018, inviting public comment (but not yet introducing the bill in the Senate). Senator Wyden's proposal is perhaps the most aggressive at protecting user privacy and transforming the legal landscape. It amends the FTC Act so that the FTC's already-existing unfair and deceptive practice authority would include noneconomic injuries and injuries "creating a significant risk of unjustified exposure of personal information." The bill also creates a Bureau of Technology at the FTC that is tasked with carrying out the agency's new rulemaking authority. That said, it is also one of the more narrowly focused, applying only to data brokers or "other commercial entit[ies] that, as a substantial part of their business, collects, assembles, or maintains personal information concerning an individual who is not a customer or an employee of that entity in order to sell or trade the information or provide third-party access to the information."

The bill would task the FTC with creating a universal opt-out database along the lines of the Do Not Call registry. Instead of a consumer having to decide and communicate her privacy and data management preferences for each website, this centralized "Do Not Track" registry would communicate a user's preferences to all covered entities. Under the Act, if users register and opt out, companies would be barred from sharing those consumers' personal information, or from storing or using personal information shared by non-covered entities. (Collection of personal information, however, would still be permitted.) This approach would also regulate data brokers' prolific use of consumer information—even though consumers generally have never interacted with (and thus have never had the opportunity to establish privacy or data management preferences for) these companies. The CDPA's opt-out function would be retroactive, meaning that companies would have to delete information they already possess on consumers who opt out. To avoid a one-size-fits-all approach, though, the bill requires the FTC to create a mechanism allowing consumers who have generally opted out to nonetheless choose to opt in for certain services, or to continue to opt out but to pay a fee to receive the underlying service.

The bill also requires risk assessments for "high risk" automated decision systems, as well as "data protection impact assessments" for high-risk information systems. These provisions appear to have been the basis for Senator Wyden's Algorithmic Accountability Act, and they are substantially similar to the provisions of that bill.

The bill does include some of the more common elements seen in other privacy proposals, including a consumer right to access and correct data, a requirement that companies undertake security measures, and a consumer right to request and receive a list of the third parties with which a company has shared that consumer's data. But Senator Wyden attempts to give these

provisions some teeth that do not exist in other proposals: Executives at covered entities are required to certify their companies' compliance with regulatory requirements, and an executive who signs knowing that her company has not complied with the Act's standards risks fines and potential imprisonment for up to 20 years.

Data Broker Accountability and Transparency Act of 2017 (S. 1815)

Though introduced in 2017, the Data Broker Accountability and Transparency Act (with a companion bill in the House, H.R. 6548) is also worth mentioning because its sponsors have played a meaningful role in the data privacy debates: Senators Markey (D-MA), Blumenthal (D-CT), Whitehouse (D-RI), and Sanders (D-VT). But despite its sponsors' sometimes tough talk in this area, the Act itself is relatively modest. It would only regulate data brokers, preventing them from obtaining data through duplicitous means, and requiring them to establish procedures to ensure "to the maximum extent practicable" that the information they collect is accurate. The Act also creates a process—similar to that in place for credit agencies—allowing consumers to verify their information for free at least once a year and correct inaccurate information. The bill would also allow consumers to express a preference not to have certain information used for marketing purposes. State AGs would have enforcement power along with the FTC, and the Act does not expressly preempt state laws.

House Proposals

The House of Representatives has been a bit quieter on the data privacy front, with no proposals yet introduced in 2019 (except for the House companion bill to the Algorithmic Accountability Act, introduced by Rep. Clarke (D-NY)). In September 2018, however, Rep. DelBene (D-WA) introduced the Information Transparency & Personal Data Control Act (H.R. 6864), which would give data privacy rulemaking authority to the FTC, require easily understood privacy and data-use policies, and require annual audits for website operators collecting sensitive personal information with more than 500 employees. The Act would also establish consent requirements based on data type: Website operators that collect or maintain personal information (including data brokers) would be required to obtain opt-in consent for "any functionality that involves the collection, storage, processing, sale, sharing, or other use of sensitive personal information," while consumers must only have the option to opt out of the collection, storage, processing, selling, sharing, or other use of non-sensitive personal information.

However, the Act contains several caveats and exceptions that could end up substantially limiting its effects. For example, data used for "[m]onitoring, or enforcing agreements between the covered entity and the individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity" is not subject to the Act's requirements. This provision could end up creating a broad loophole allowing companies to contract out of the Act's requirements through their terms of service or privacy policies. Moreover, any regulations promulgated under the Act regarding opt-in consent "shall not apply" where the data use "does not deviate from purposes consistent with an operator's relationship with users as understood by the reasonable user."

The House has also generated some more narrowly focused laws. For example, the Consumer Information Notification Requirement Act (H.R. 6743) would amend the GLBA "to provide a

national standard for financial institution data security and breach notification." The bill would allow the Federal Reserve to establish standards for preventing data breaches, though enforcement would remain with the states. The Act would allow for limited preemption, though only of state laws that establish standards that are less protective than the those under the Act and any accompanying regulations. The Application Privacy, Protection, and Security Act of 2018 (H.R. 6547) provides minimal requirements for the collection of data via mobile phone applications, including notice requirements and an opportunity for a user to request that the app provider stop collecting and using the consumer's data when the consumer stops using the app. The Act creates a safe harbor for any app developer following a consumer data privacy code of conduct and preempts state laws providing less protection than the Act or the regulations promulgated thereunder.

Industry Proposals

Congress isn't the only party getting into the federal regulation game. The Information Technology and Innovation Foundation (ITIF), a think tank supported by major names in the tech industry such as Google, Amazon, and Facebook, has offered up its own "Grand Bargain," consisting not of specific legislative proposals, but of general guiding principles. The ITIF recommends that any legislation enshrine principles of transparency, data interoperability, opt-out for normal data collection, and opt-in to the collection of sensitive data. The ITIF would also establish a uniform federal standard for data breach notification requirements and preempt all state laws on the subject. The think tank also recommends repealing and replacing existing federal laws on data privacy (including HIPPA, COPPA, and FERPA), exempting de-identified data and publicly available information from any requirements, and preempting all state laws in the data privacy field. It also includes a number of general recommendations intended to "protect innovation" and "minimize compliance costs," including "Do not include limitations on data retention," "Do not include a right to deletion," "Do not include a private right of action," and "Do not include privacy-by-design provisions" (that would embed privacy into the design and structure of systems). Several leading Democrats have already expressed intense skepticism about ITIF's bargain, with Senator Blumenthal letting Big Tech know that "they should be embarrassed" by their proposal.

Intel also released a draft bill, the Innovative and Ethical Data Use Act of 2018, that seems similarly unlikely to win support from legislators otherwise interested in robust privacy protection. Intel's bill would allow tech companies to collect personal data that is "relevant and necessary" to accomplishing purposes identified (and made public) by each company. A company would then only be able to use that data for either the identified purposes, uses consistent with the identified purposes, or purposes for which the consumer has provided her consent. Intel's proposal would also require a company to perform a risk and accuracy assessment before engaging in automated processing of data, including processing by "algorithmic, machine learning, or artificial intelligence processing or predictive analytics, without human intervention."

Intel's proposal also creates a notice scheme requiring explicit notice for the collection of sensitive data, including geolocation, biometric, health, or "sexual life" data, and a general notice regime for "articulating the processing practices" of a covered entity. Intel proposes a right of "reasonable access" to data for consumers, including the right to correct errors or add

information. Covered entities would also be required to establish an oversight program to ensure that any third parties with which they share information also maintain appropriate privacy controls and practices.

Finally, Intel's proposed bill would grant the FTC rulemaking and enforcement authority. However, an entity could avoid enforcement actions and civil penalties if it certifies to the FTC that it is in material compliance with the Act. The law would preempt state laws "primarily focused on the reduction of privacy risk through the regulation of personal data collection and processing activities," but it would not preempt states' consumer protection laws. The Act also excludes from preemption data breach notification laws, as well as general law principles that might apply in the data protection context (for example, laws on trespass or tort laws).

* * *

As with any legislation in today's highly partisan political environment, there's reason to question whether any of the proposed bills will actually pass. That said, unlike many issues dividing Congress today, the need for some level of greater privacy protection at the federal level appears to enjoy bipartisan support and, thus, there is good reason to believe that at least one of the proposed bills, or some combination of them, may become law and substantially alter the regulatory landscape for privacy issues. Stay tuned.