FEDERAL RESERVE BANK OF SAN FRANCISCO

Fintech Edge **Special Report**

The 2018 California Consumer Privacy Act: Understanding Its Implications and Ambiguities

The views expressed in this publication are solely those of the authors and do not necessarily represent the position of the Federal Reserve Bank of San Francisco, the Board of Governors of the Federal Reserve System, or any other parts of the Federal Reserve System.

Acronym List

ABA	American Bankers Association
CCPA	California Consumer Privacy Act
COPPA	Children's Online Privacy Protection Rule
FCRA	Fair Credit Reporting Act
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
SIFMA	Securities Industry and Financial Markets Association

Relevant Laws and Regulations

California Consumer Privacy Act
California Consumer Privacy Act, September 2018 Amendment
California Financial Information Privacy Act
Children's Online Privacy Protection Rule
Fair Credit Reporting Act
Gramm-Leach-Bliley Act Privacy Rule
Gramm-Leach-Bliley Act Safeguards Rule
Health Insurance Portability and Accountability Act
Federal Reserve Regulation P

Authors

Kaitlin Asrow, Fintech Policy Advisor
Joanne Xu, Fintech Policy Advisor

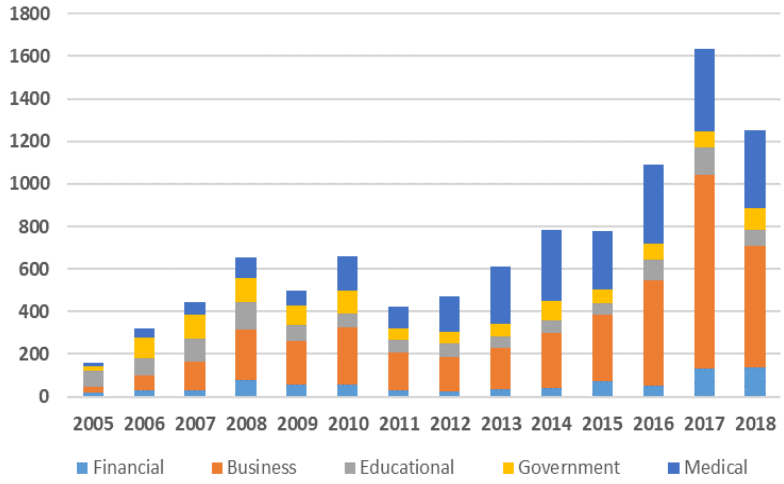
Publication Date

April 25, 2019

Introduction

Data privacy is quickly becoming a top-of-mind issue for consumers, businesses, regulators, and legislators following the steady stream of media reports about data breaches and data misuse. Data breaches have been occurring for years (Figure 1[1]), but there is a renewed focus on digital privacy as technology enables exponential growth[2] in information collection (Figure 2[3]), and questions arise regarding the appropriate use of personal data by companies. This highlights the important difference between data security—the technical protection of company assets from attack and human error—and privacy, which focuses on consumers' ability to control and direct how their data are used. Privacy requires principles and processes in addition to technical security specifications.[4] The increasing focus on these principles and processes is one of the factors that led to the development of new legal frameworks, such as California's Consumer Privacy Act of 2018 (CCPA). Federally, the United States has a patchwork of data privacy laws and statutes, and it is common for certain states to take the lead on consumer protection rulemaking across industries. As online commerce and digital companies blur physical boundaries, though, it is unclear whether state-by-state privacy legislation will exacerbate, or fill in, the existing patchwork of consumer protection laws. This tension has given rise to multiple federal proposals, while market actors and international jurisdictions consider and implement their own approaches. Furthermore, the rapid pace of innovation can make legislation challenging, and promising new technologies are emerging that could supplant the need for some regulation. Despite these unknowns, the state-level approach of the CCPA is an important catalyst to spark debate around federal preemption, consistent consumer protection, and the appropriate market environment for ongoing innovation.

Figure 1: Number of Data Breaches by Industry



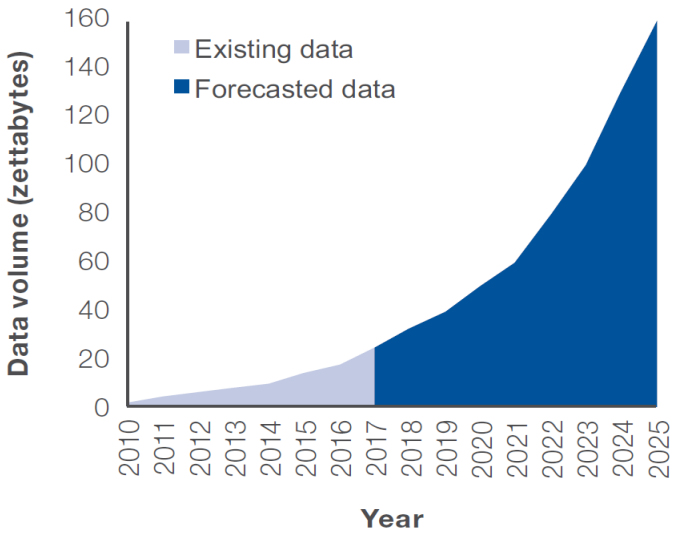
This report is intended to highlight some of the questions and implications that have arisen from the passage of the CCPA. It is the authors' hope that reports like this one will inform the increasingly wide-ranging conversation and debate about consumer data privacy in the United States.

[1] "ITRC Multi-Year Data Breach Chart 2005-2018", *Identity Theft Resource Center,* Link
[2] "Data brokers: regulators try to rein in the 'privacy deathstars", Financial Times. 7 Jan 2019, Link
[3] 'The Appropriate Use of Customer Data in Financial Services", *World Economic Forum.* Sept 2018, Link
[4] "Data Privacy vs. Data Protection: Understanding the Distinction in Defending Your Data", Forbes Technology Council. 19 Dec 2018, Link

Overview of CCPA

California passed the CCPA[5] in June 2018 as a direct response to data breach and misuse scandals at various firms[6]. The law is the first of its kind and seeks to expand data privacy rights for California residents, including the right to:

Figure 2: Annual Global Data Volume



- Know what information is being collected and resold
- Refuse the resale of information
- Access the information collected in a readily usable format
- Have certain information deleted
- Equal service and price
- Seek remedy in the event of a data breach.

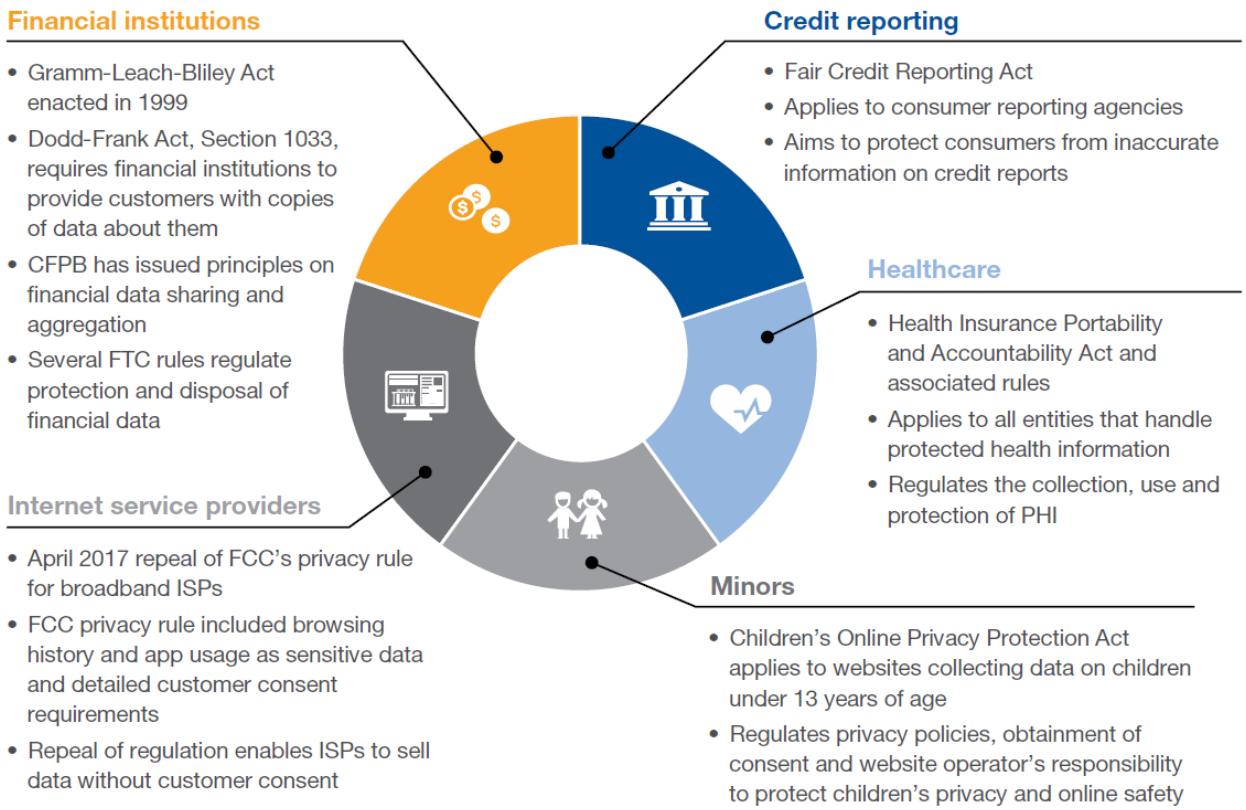
Under the CCPA, personally identifiable information (PII) is any non-publicly available information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household or device. This is a significant expansion of the traditional definition of PII[7] because it acknowledges the increasing ability to link seemingly innocuous data to consumers; examples include IP address, geo location, and browser history.[8] The law applies to entities that do business in California or collect the personal information of California residents, and meet one or more of the following three criteria: 1) has annual gross revenues in excess of $25 million, 2) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or 3) derives 50 percent or more of its annual revenues from selling consumers' personal information.[9] The California legislature drafted the law in expedited fashion to preempt a ballot initiative that would have been harder to amend than direct legislation. It was subsequently amended on September 23, 2018[10] to clarify certain provisions. The Attorney General (AG) of California is responsible for writing rules based on the final legislation during 2019 calendar year, with the law set to go into effect on January 1st, 2020.[11] There may be additional legislative amendments prior to the rulemaking, and it remains unclear how the AG will both oversee and enforce the law on an ongoing basis.[12]

[5] "California Consumer Privacy Act", Assembly Bill No. 375, Chapter 55, *California Legislature*. 29 June 2018, Link
[6] "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens", New York Times. 19 Mar 2018, Link
[7] Regulatory guidance has commonly used name, address, income, social security number, and financial information such as credit scores, account and routing numbers, and transaction information as examples of PII, such as the FTC summary here. The Federal Reserve guidance expands this and references "information obtained through internet collection devices", Reg P., Pg. 3
[8] "California Consumer Privacy Act", Assembly Bill No. 375, Chapter 55, 1798.140 (o),-(k) *California Legislature*. 29 June 2018, Link
[9] "California Consumer Privacy Act", Assembly Bill No. 375, Chapter 55, 1798.140 (c), *California Legislature*. 29 June 2018, Link
[10] "California Consumer Privacy Act Amendment", Senate Bill No. 1121, Chapter 735, *California Legislature*. 24 Sept. 2018, Link
[11] "California Consumer Privacy Act", Assembly Bill No. 375, Chapter 55, 1798.185, 1798.198, *California Legislature*. 29 June 2018, Link
[12] "Re: California Consumer Privacy Act of 2018", *Xavier Becerra, CA AG*. 22 Aug 2018, Link

The Patchwork of U.S. Privacy Laws

An impetus for the CCPA was the fact that the United States does not currently have an overarching privacy regime, but instead considers data privacy through a number of federal and state laws that are specific to sectors and applications (Figure 3[13]). At the federal level, the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Availability Act (HIPAA), and the Children's Online Privacy Protection Rule (COPPA) all deal with consumer data privacy protection. GLBA and HIPAA pertain to certain types of institutions, financial and health related, respectively, while FCRA and COPPA protect categories of consumers, those seeking credit and those under the age of 13. California also has existing privacy laws that predate the CCPA, including the California Financial Privacy

Figure 3: U.S. Federal Legislation Applicable to Customer Data



Notes: CFPB = Consumer Financial Protection Bureau; FTC = Federal Trade Commission; FCC = Federal Communications Commission; ISP = internet service provider; PHI = protected health information.
Sources: Jolly (2017); King and Raja (2013); Raul (2016)

Act, the Confidentiality of Medical Information Act, and the Driver's Privacy Protection Act. Additionally, federal entities and many states have information security specific laws that touch on breach notification, consumer disclosures, and cybersecurity standards.[14] In combination, these laws create a number of business requirements which are also within the scope of the CCPA. Due to these overlaps,

[13] "The Appropriate Use of Customer Data in Financial Services," *World Economic Forum*. Sept 2018, Link
[14] "State Laws Related to Internet Privacy", *National Consumer Law Center*. 24 Sept. 2018, Link

the CCPA provides exceptions to businesses that are in compliance with the other laws, but the depth and breadth of those exceptions is unclear. Legal experts generally interpret an exception if the CCPA is preempted by or conflicts with other laws, but not if the CCPA provides non-conflicting additional protections.[15] This collection of privacy approaches, combined with the CCPA's expectation of additional protections, are of particular concern for financial institutions because the spectrum of data they collect may fall within multiple federal and state-level legal frameworks.[16]

Relevance to Financial Institutions

Despite the CCPA's exceptions to information covered under financial privacy and security laws, such as GLBA, the law may still apply to supervised financial institutions in a number of ways. The CCPA exceptions do not exempt financial institutions as a category, only the information they handle that is already covered by other laws. The most immediate way that CCPA could impact financial institutions is through the use of personal information beyond what is explicitly defined in GLBA. GLBA encompasses consumer data that are provided for, or generated from, the provision of financial products and services. The CCPA defines data elements, such as IP addresses, geolocation elements, and consumer profiles, which may be collected and shared for activities outside of providing a specific financial product or service to a customer, such as website improvement, targeted advertisement, and marketing strategies. Whether these kinds of activities still fall under the CCPA's GLBA exception may be further clarified in the upcoming rulemaking process.

This broad language, combined with the relatively low thresholds for the law's applicability, indicate that CCPA could apply to a significant number of financial institutions.[17] Another important aspect of the law for financial institutions is that consumers have a private right to action for data breaches, even if the data are covered by GLBA. Consumers do not have to demonstrate harm to have a right to statutory damage amounts.

Applicability questions and litigation risks will likely create even greater challenges for financial institutions that serve consumers across state lines. The CCPA is a residency-based law; therefore, financial institutions that have footprints within or beyond California need to determine who has residency in the state and understand when that changes.[18] The need for more granular data management goes beyond just tracking which entities the law applies to, but is also necessary to differentiate GLBA- or FCRA- covered data from CCPA-covered data and to enable consumers to view and control their information. This level of data management can be especially difficult in legacy banking systems and data infrastructures that have been combined through mergers and acquisitions. An example of this challenge can be found in the report issued by the House Oversight and Government Reform Committee about the 2017 Equifax data breach, which cites "complex and outdated IT systems"' as a key finding.[19] Another relevant area for financial institutions is third-party risk management. Bank

[15] 'U.S. Banks & Data Privacy, California, GDPR & Beyond Webinar," *Source Media*. 17 Dec 2018.
[16] Rubin, Joe. "Banks must brace for renewed privacy fight', *American Banker*. 20 Dec 2018, Link
[17] Based on publically available data from the FDIC and FFIEC there is a minimum of 120 institutions that could be subject to the CCPA, ranging from the largest banks in the country to a variety of community institutions. Please note, though, that the scope and applicability of the law will be determined by the California AG in rulemaking.
[18] "California Consumer Privacy Act", Assembly Bill No. 375, Chapter 55, 1798.140 (g), *California Legislature*. 29 June 2018, Link. The term "resident," as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents.
[19] "Scathing Congressional report released on historic Equifax data breach", *Gray DC News Bureau*. 13 Dec. 2018, Link

vendors may also need to comply with CCPA and financial institutions will have to consider this dynamic in their partner oversight programs.

Potential for Federal Law

The complexity of sector- and state-based privacy laws in the United States, combined with incessant data misuse revelations,[20] have prompted serious consideration of a comprehensive federal privacy law. The CCPA model of state-by-state regulation of digital concepts could make it difficult for both new and established businesses to expand, and may result in inconsistent protections for consumers in different parts of the country. The state-by-state data breach notification laws represent a pattern that privacy regulation could follow, with 54 variations on company requirements.[21] Business leaders argue that this has created a focus solely on compliance rather than on innovation in broader cybersecurity operations,[22] and companies are unable to simply confirm to the strictest law because process requirements often vary.[23] Alternatively, the power for states to establish these laws independent of the federal government can prompt stronger protections and create a snowball effect that leads to wider change. Already, states including New Jersey, Washington, and Vermont are circulating and passing state privacy laws that share similarities with, but also differ from, the CCPA. For example draft bills in New Jersey have not included exceptions for GLBA covered data.[24] In May 2018 Vermont passed a law regulating data brokers[25] and the AG in that state is calling for additional privacy protections.[26] Additional states, including Massachusetts, Illinois, New York, and Florida, have historically been more assertive on privacy issues and could also follow California's lead.

The potential for piecemeal state privacy laws, in addition to the existing sector- and consumer-specific laws, has prompted businesses to join with consumer advocates in calling for federal legislation.[27] While these different groups agree on the concept of a federal law, they vary significantly on how it would be implemented, what it would contain, and how it would interact with existing legal frameworks. Federal data privacy protection could potentially be achieved through the existing authorities of agencies, such as the Federal Trade Commission (FTC) or the Federal Communications Commission (FCC), or through legislation that expands or creates new authorities.

There have been a series of Senate hearings with the FTC on the topic of data breach, including suggestions to expand the FTC's authority to address a federal data privacy need.[28] The FTC has conducted a series of its own hearings to explore expanded jurisdiction and updates to existing laws.[29] The National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) have also been actively developing privacy approaches. The NTIA

[20] Abril, Danielle, "Privacy Group Pressures FTC after Latest Revelations about Facebook's Data Sharing, *Fortune Magazine.* 19 Dec 2018, Link
[21] "Security Breach Notification Laws", *National Consumer Law Center*. 29 Sept 2018, Link
[22] "Goldman CISO Says Regulation Patchwork Hampers Corporate Cyber Efforts", Chernova, Yuliya, *Wall Street Journal*. 11 Dec 2018, Link
[23] "Data Breach Charts", *Baker Hostetler*. Jul 2018, Link
[24] "Legislating Cybersecurity: 2018 Adds Patches to the Quilt of Data Privacy Law Across the US", *New Jersey Law Journal.* 28 Nov 2018. Link
[25] Dellinger, AJ, "Vermont Passes First-of-its-kinds law to regulate data brokers. *Gizmodo*. 27 May 2018, Link
[26] Landen, Xander, "AG Says Vermont should take more steps to protect data privacy. *VTDigger*. 30 Dec 2018. Link
[27] "In the Wake of GDPR, Will the U.S. Embrace Data Privacy", Meyer, David, *Fortune Magazine*. 29 Nov 2018, Link
[28] "Senate Examines Potential for Federal Privacy Legislation", *Inside Privacy, Covington*. 1 Oct 2018, Link
[29] "FTC Hearing 9: Dec. 11 Opening Remarks and Session 1 Presentations on Data Breaches", *FTC.gov*. 11 Dec 2018, Link

released a request for comment on developing the current administration's approach to consumer privacy[30] and NIST is creating a privacy framework to complement their cybersecurity framework.[31]

In the realm of new legislation, Senators Elizabeth Warren (MA) and Mark Warner (VA) released a federal data breach bill titled the 'Freedom from Exploitation Act' in late 2017 following the Equifax breach, but it did not gain traction in Congress.[32] In April 2018, Senators Amy Klobachar (MN) and John Kennedy (LA) introduced bipartisan legislation to protect online privacy[33] and, in November 2018, Senator Ron Wyden introduced a bill that would increase the privacy authority of the FTC and create a 'Do Not Track' online registry.[34] In December 2018, Senator Brian Schatz, along with 15 other senators, introduced a bill entitled the Data Care Act, which would apply fiduciary responsibilities to organizations that handle data. This bill focuses more on security than consumer control; it gives additional authority to the FTC to levy fines and there are currently no GLBA exemptions.[35] Despite the potential benefit for both consumers and businesses of a consistent approach to data privacy, achieving a comprehensive federal solution is a significant challenge given the technological complexities of consumer data practices, as well as the challenge of states' rights and preemption.

International Law

Regulators and legislators outside of the U.S. are also increasingly focused on data privacy. In 2018, Australia enacted legislation covering data breach notifications. Australia is also in the process of creating a broader consumer data rights framework.[36] The European Union implemented the General Data Protection Regulation (GDPR) to protect consumer data and privacy, while India submitted legislative recommendations on data privacy management. GDPR is the most significant of these efforts and its implementation is having a ripple effect across the globe because it applies to any company, across industries, with European customers, including those in the U.S. GDPR has already had some constructive data privacy impacts, such as investment in data infrastructure and increased breach reporting,[37] but there are notable implementation challenges. A recent survey by the International Data Corporation found that less than half of European small and midsize businesses (SMBs) have taken steps to prepare for the GDPR; rates are significantly lower among non-European SMBs.[38] This highlights the risk of privacy laws favoring large incumbent firms who can more readily comply. These laws also highlight the United States' fragmented approach, with foreign countries raising concerns over digital trade with varying levels of privacy protection for their citizens in the U.S. or from U.S. companies.[39] While there remain differences between countries, legal similarities are beginning to surface, for example between the GDPR and CCPA.[40]

The GDPR and the CCPA both codify consumers' right to transparency with regard to their data and enable consumers to assert some control over this asset, including the right to have information deleted

[30] "Developing the Administration's Approach to Consumer Privacy", *Federal Register, NTIA*. 26 Sept. 2018, Link
[31] Brumfield, Cynthia, "Why NISTs privacy framework could help security efforts", *Cyberscoop*. 9 Nov 2018. Link
[32] "Legislation to Hold Credit Reporting Agencies Like Equifax Accountable for Data Breaches", *Warren Senate Office*. 10 Jan 2018. Link
[33] "Klobuchar, Kennedy to Introduce Bipartisan Legislation to Protect Privacy of Consumers' Online Data", Klobuchar Senate Office. 18 Apr 2018. Link
[34] "Wyden Releases discussion draft of legislation to provide real protections for Americans' privacy", *Wyden Senate Office*. 1 Nov 2018, Link
[35] "Schatz Leads Group of 15 Senators In Introducing New Bill To Help Protect People's Personal Data Online", *Schatz Senate Office*. 12 Dec 2018, Link
[36] "Consumer Data Right", *Australian Treasury*. 9 May 2018, Link
[37] Ram, Aliya. "Reports from whistleblowers on data breaches almost triple", *Financial Times*. 16 Dec 2018, Link
[38] "IDC Finds Varying Degrees of GDPR Awareness and preparation among global small and midsize businesses", *IDC*. 3 April 2018, Link
[39] Chee, Foo Yun. "EU urges US to nominate permanent data privacy ombudsman", *Reuters*. 19 Dec 2018, Link
[40] "Comparing privacy laws: GDPR v. CCPA", Future of Privacy Forum. Link

and the ability to port data between entities. Both laws also provide dual enforcement mechanisms through regulatory fines and private rights of action. There is, however, a fundamental distinction: GDPR's focus is on when data collection itself is acceptable, outlining six permissible purposes, while the CCPA is focused on consumer rights after collection has occurred. Additionally, under GDPR, consumers have the right to rectification to ensure the accuracy of their data; the CCPA, by contrast, only provides a right to transparency. Other U.S. laws, such as the FCRA, provide a similar right to error resolution, but are more narrowly applicable. As companies increasingly use nontraditional consumer data in financial services, it may become necessary to consider whether the data collection methods and the avenues that consumers have to correct false information remain appropriate. Another difference is in the consumer consent requirement. Under the CCPA, companies need to provide consumers with an opportunity to opt out of the sale of their personal information. But under the GDPR, consumers need to opt in to give companies a legal basis for collecting, processing, or transferring personal information. Having to opt in at the initiation of a data sharing relationship can raise more awareness among consumers instead of relying on them to digest disclosures and request to opt-out after a relationship is established.

Market Views on CCPA and Privacy

In addition to domestic and international legislation, there are also examples of self-regulatory initiatives that can help tackle security and privacy issues, including the Payment Card Industry Security Standard[41] and the Consumers Union Digital Standard.[42] As the CCPA is further amended and implementation rules are written, it is worthwhile to examine interactions with market standards and potential impacts on market participants.

Legal experts indicate that financial institutions with California-based consumers are likely preparing for at least some of the data they collect to fall within the scope of CCPA.[43] Institutions will need to invest in data infrastructure and legal guidance to navigate these new requirements. This could put smaller banks at a disadvantage compared to large banks and technology companies. In a joint letter responding to the NTIA's privacy efforts, the Bank Policy Institute, American Bankers Association, and Securities Industry and Financial Markets Association state that the CCPA "greatly expands the scope of personal information covered . . . and this dramatic expansion will have significant impacts on the financial services sector."' Trade associations have argued that a patchwork of state privacy laws will pose a costly compliance burden.

Financial data aggregators may consider much of the data they handle as subject to GLBA, and therefore exempt from the CCPA, but they are still working towards compliance in order to prepare for other states that may not include a GLBA exception. These companies are reevaluating and investing in their internal data structures to prepare for such developments, which reinforces the challenge that legacy core banking systems and smaller firms may face. Data aggregators may also be concerned that aspects of the law, such as the right for consumers to request their information, will require them to identify

[41] "PCI Security Standards Council", Link
[42] "Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace", Consumer Reports. 6 March 2018, Link
[43] "Update for Financial Institutions Regarding the California Consumer Privacy Act—This New Law May Apply to You", *Perkins Coie*. 11 Oct. 2018. Link

consumers in anonymized data sets that they otherwise could keep de-identified, and therefore more secure.

Fintech companies may also feel that they fall within the CCPA's GLBA carve-out, but likely vary widely in their focus on regulatory applicability based on growth stage. Fintech companies specializing in payment services could be considering a CCPA carve-out that exempts data used in fraud prevention. There may be general concern that CCPA could reduce the flow of consumer data needed for future uses, such as developing new features. Some fintech companies may also be waiting to engage with the law until the final rules are set, and potentially because the law seems targeted at digital advertising and social media, putting specific pressure on data resale business models. A state-by-state regulatory approach will be challenging for early-stage fintech companies engaging in data-focused activities, such as personal financial management. Larger fintech payment and lending companies already have state-specific approaches because of licensing requirements and therefore may be more likely to have compliance systems in place. Across all companies, there is likely a concern that the private right of action will result in significant legal costs and may create a complicated network of precedence.

Consumer advocacy organizations offer an alternative view to the challenges and opportunities of privacy legislation at both the state and federal levels. Many groups feel that the CCPA does not go far enough and would have liked the law to also address consumer choice and transparency in the initial collection of data, not just resale. Advocates are not concerned with the exemptions for other privacy laws, but are focused on strengthening the private right of action to apply to more types of data and instances beyond breach. With regard to a federal privacy law, consumer groups consistently state that any national law should be a floor of protection, not a ceiling that would preempt stronger state laws.[44]

Many market participants are also concerned with a potential lack of consumer understanding of CCPA exemptions and, more generally, their rights under the law. There is broad agreement that this topic is especially challenging and the current legislative and rule-making process is complex.

The Potential of Technology

The complexity of developing and implementing data privacy legislation and standards could potentially be assisted by advances in technology that reshape what elements of consumer protection would even require oversight. Innovations such as zero-knowledge computing and digital identification have the potential to accomplish some privacy goals without detailed frameworks.

Zero-knowledge computing allows for data to be processed while encrypted, enabling analytics without exposing consumer information.[45] This technology could negate the need for some privacy oversight on third-party data processors and could even result in CCPA not applying to organizations that only work with encrypted data. ING Belgium is using this technology through their XOR Secret Computing Engine, which builds analytical models using data from multiple countries. While the computation is done in datacenters around the world, no private information is exported from any jurisdiction.[46] In addition to boosting privacy and security for individual consumer data, the technology allows for the sharing of

[44] "U.S. PIRG and Leading Groups Demand Real Privacy Protection and Digital Rights", U.S. PIRG. 17 Jan 2019. Link
[45] Loftus, Tom. "'Zero Knowledge' Tech Catches JPMorgan's Attention", *WSJ*. 14 Nov 2018, Link
[46] Castellanos, Sarah. "ING Belgium Sees Opportunities for 'Secret' Sharing of Encrypted Data", *WSJ*. 1 Jun 2017, Link

training data sets among different institutions, and the monetization of data insights without revealing underlying information.

Digital identity is another example of a technology concept that could reduce the need for companies to store personally identifiable information at all. Government systems for digital identity have been implemented in India and Estonia, and multiple consortiums and companies have been established to develop commercial identity systems.[47] These kinds of systems create a central repository for verification, and with the addition of tokenization, the sharing and storage of private information for customer identification could be greatly reduced. Additionally, digital identity can give direct control to consumers, which is a central privacy goal. Consumers could choose what identifiable information to disclose and when to rescind access. Currently, once a consumer gives out identification information, companies commonly retain it, and some monetize identification services based on that storage. While digital identity offers a host of privacy benefits, it is not without downside. Some industry participants believe that in centralizing consumer private information, it makes the host an attractive target for hackers and, once a breach happens, it could be financially devastating. Central government identity systems can also run afoul of corruption or create barriers for the population to access fundamental products and services if that is the only form of identity accepted. India's Supreme Court recently addressed this issue, stipulating that the government-issued digital identity, Aadhaar, cannot be mandatory for opening bank accounts, obtaining mobile phone access, or enrolling in school.[48]

These kinds of technology advancements may need to be considered in conjunction with the development of privacy regimes. Some elements of protection may not be necessary with new innovation, and it is important to consider how prescriptive laws could limit the development of new innovations that further protect consumers.

Conclusion

Data privacy is a global movement, and the United States' current approach may present challenges in effectively addressing the breadth and volume of today's data practices. The CCPA, and laws like it, have prompted positive debate about how this patchwork can be improved, but significant ambiguity remains. Wrestling with questions of federal preemption, market implications, the role of technology, and interactions with international frameworks is an important step in creating a system for consistent consumer protection in the digital age.

[47] https://sovrin.org/
[48] "Aadhaar: India Supreme Court upholds controversial biometric database", *CNN*. 26 Sept. 2018. Link