Double, Double Toil and Trouble: Data Privacy and the Double Trouble of the California Consumer Privacy Act of 2018 and the Push for a Federal Privacy Standard

William Denny, Partner, Potter Anderson Corroon, Wilmington, DE

The California Consumer Protection Act of 2018 represents a seismic shift in how we will be dealing with personal information in the U.S. The vastly expanded rights afforded to California residents and the burdensome obligations imposed on businesses by the CCPA, together with the influence of the GDPR on American companies engaged in international commerce, is propelling the U.S. Congress toward creating a new and pre-emptive federal privacy framework. This presentation will focus on the influence of CCPA and the prospect and challenges of new federal legislation.
WILLIAM R. DENNY BIO

Mr. Denny is a partner at Potter Anderson & Corroon LLP in Wilmington, Delaware, where he leads the practice area of cybersecurity, data privacy and information governance. Bill is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals (IAPP). He has represented both public and privately held companies in a wide range of technology-related transactions, including counseling clients on compliance with cybersecurity laws, development of data security and privacy policies, contracting with cloud service providers, outsourcing of IT services, mergers and acquisitions, technology licensing, software development, sales of internet domain names, and website terms of use. Clients include local, regional and international companies who rely on information technology and customer data for their core business functions, as well as software developers and service providers. Bill frequently writes and speaks on topics of cybersecurity and data privacy.
The California Consumer Privacy Act of 2018 (CCPA) represents a seismic shift in how businesses in the U.S. will deal with personal information. The vastly expanded rights afforded to California residents and the burdensome obligations imposed on businesses by the CCPA, together with the influence of the GDPR on American companies engaged in international commerce, is propelling the U.S. Congress toward creating a new and pre-emptive federal privacy framework. This paper discusses the factors leading to enactment of the CCPA, analyzes the key elements of the CCPA, and examines the prospect and challenges of new federal legislation.

I. California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 represents a continuation of California’s pioneering work in data privacy litigation, as well as a dramatic leap from the traditional approach toward privacy in the U.S., that of notice, to an approach strongly influenced by the GDPR to afford significant rights and controls to individual consumers. The CCPA, with its broad jurisdictional sweep, will require many businesses to re-design their data security and privacy practices to avoid potentially significant liability. Even companies beyond the reach of the CCPA would be wise to consider the guidance that it offers with respect to the collection and protection of personal data in specific situations that have not, until now, been regulated in the U.S.

A. Factors Leading to Enactment of the CCPA

For years, individuals have become increasingly uncomfortable with the myriad ways that companies harvest and monetize their personal data, and have called on companies and legislators to do a better job at protecting their data privacy.

1. Cambridge Analytica Scandal

In March 2018, the Cambridge Analytica scandal broke. The public learned that private data was harvested from millions of Facebook users without their knowledge and consent, and that the Trump presidential campaign used this private data to target political advertisements. This significantly increased demand for better data privacy rules. Although neither Cambridge Analytica nor Facebook acted illegally in collecting and processing the information, individuals were offended by the lack of transparency of what was happening to their data and upset by their inability to prevent such usage.

Cambridge Analytica paid approximately 320,000 voters between $3 and $5 apiece to download an app and take a detailed personality/political test that required them to log into their
Facebook accounts. The app then collected data such as likes and personal information from the Facebook accounts. The personality quiz results were paired with Facebook data to seek out patterns. Algorithms then combined the data with other sources to create a superior set of records of 2 million people with hundreds of data points per person. The targeted individuals then received highly personalized advertising based on this data.

2. Influence of GDPR

At the same time, companies involved in international transactions were coming to grips with the European Union’s General Data Protection Regulations (GDPR), which came into force on May 25, 2018. The express purpose of the GDPR was to protect the personal data of EU residents. It further established data protection as a fundamental right, established a much broader definition of personal data, gave control of that personal data back to EU residents who were the data subjects, addressed the export of personal data from the EU, and established significant fines for violation. The GDPR also overcame the problem with the previous EU privacy directive by being enforceable across the EU without the need for national implementing legislation.

American companies found themselves falling under the potential reach of the GDPR even if they did not have any established business presence in the EU. Rather, by its terms it applied to companies if they processed personal data of EU residents as part of either the offering of goods or services to data subjects in the EU, or the monitoring of the behavior of data subjects in the EU. “Offering” goods or services has to be more than mere internet access, but must somehow exhibit an intent to target customers in the EU. “Monitoring” refers to tracking individuals on the internet and any subsequent use of that data to profile an individual.

3. Effect of the Ballot Initiative

In May 2018, supporters of a California ballot initiative on data privacy filed more than 600,000 signatures in support of presenting the initiative to voters, nearly twice the number of signatures required to do so. Californians for Consumer Privacy led the campaign in support of the measure. Alastair Mactaggart, a San Francisco-based real estate developer, chaired the campaign. As of June 28, 2018, Californians for Consumer Privacy had raised $3.05 million, with 98.4 percent of funds from Mactaggart. Mactaggart’s interest in privacy began when he asked a Google engineer at a cocktail party if he should be concerned about the issue. Mactaggart recalled the engineer saying that if people knew what we knew about them, they’d be freaked out. That got him thinking that if the law required transparency, there would be change.

But ballot initiatives are an imperfect way to make public policy on a complex subject like data privacy. Before enactment, it can be difficult for stakeholders to help improve an initiative’s content. And after enactment, an initiative can be difficult to amend. Therefore, California legislators hoped to do better, but they faced a deadline.

June 28 was the last day the initiative’s sponsor could remove it from the ballot, and the sponsor told the legislature that he would do so only if they passed data privacy legislation first. Legislators rushed to meet this deadline, but that rush meant privacy advocates didn’t have much
chance to weigh in before it was passed. The CCPA was signed into law on June 28, 2018, only a few days after it was first introduced to the California legislature.

4. California’s History of Taking the Lead on Privacy Legislation

California has long taken the lead in the development of privacy law in the U.S. In 1972, California voted to include the right of privacy among the “inalienable” rights of all people. That right gave individuals the ability to control the use, including the sale, of their personal information.

California’s Online Privacy Protection Act of 2003 (CalOPPA) required commercial websites and online services that collect personal information on consumers in the state to post the company's privacy-related policies, including policies on the personal information collected, online tracking practices, and the types of third parties who the information could be shared with. The CCPA goes farther, requiring businesses, upon a consumer's request, to disclose the specific information collected and allow consumers to opt-out of having the information sold or disclosed.

California has also led by enacting Privacy Rights for California Minors in the Digital World Act and Shine the Light Law, which is intended to give Californians the “who, what, where, and when” of how businesses handle consumers’ personal information.

However, the developments cited above regarding the GDPR and Cambridge Analytica, as well as recent highly-publicized data breaches, convinced Mactaggart and others that California had not done enough. The CCPA states that “California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information.” It cited the “devastating effects for individuals” with loss of privacy and the “misuse” of data by Cambridge Analytica. The law states that “California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information.” “It is possible for businesses both to respect consumers’ privacy and provide a high level transparency to their business practices.”

B. What Is the CCPA?

The CCPA grants consumers the right to know what information companies are collecting about them, why they are collecting that data and with whom they are sharing it. It gives consumers the right to tell companies to delete their information as well as not to share their data. Businesses have extensive reporting and record-keeping obligations under the CCPA and consumers and the California Attorney General have broad remedies, including a private right of action in the event of a data breach that provides for statutory damages of up to $750 per individual per incident.

C. When Does the CCPA Become Effective?

The CCPA comes into force the earlier of July 1, 2020, or six months after the California Attorney General issues implementing regulations. However, the effective date can be
misleading, because companies must have dramatically enhanced recordkeeping systems in place 12 months prior to the effective date, or as early as January 1, 2019, for compliance.

D. Who Must Comply With the CCPA?

The CCPA applies to any for-profit legal entity that collects or sells personal information from or about consumers, and that (1) has annual revenues in excess of $25 Million, (2) annually buys, sells, receives or shares for commercial purposes personal information of 50K or more consumers, households or devices; or (3) derives 50% or more of its annual income from selling consumers’ personal information. “Consumer” is defined broadly as any California resident, including employees, students, tenants, customers and even California residents temporarily living outside of California. “Sells” includes any transfer of information, including to affiliates, for any valuable consideration, which may not be monetary.

E. Broad Definition of Personal Information

The CCPA defines personal information as information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” This includes the basics such as name, contact information, IP address, biometric information, geolocation data, financial information, health information. It also includes commercial information, including consuming history or tendencies, internet and other electronic network activity information, audio, electronic, visual, thermal, olfactory or similar information, professional or employment-related information, and even inferences drawn from any personal information.

The list of what constitutes personal information under the CCPA is very long, and includes some novel categories, such as a consumer’s appearance or a marketing profile that the consumer did not even create, and it is likely to grow. How these categories relate to our conventional understanding of what is private is an interesting theoretical question and one likely to spur debate as the concept of privacy changes over the ensuing years. But practically speaking, we seem to heading to a presumption that virtually any data point collected about an individual consumer is private.

There are, however some exclusions. Personal information does not include publicly available information from government records, health information covered by HIPAA, clinical trial information subject to the Common Rule, sale of personal information to or from a consumer reporting agency, financial information covered by GLBA and information subject to Driver’s Privacy Protection Act. The last two exceptions do not apply to a private right of action.

F. Basic Rights Granted Under the CCPA

The CCPA creates four basic rights for California consumers:

- A right to know what personal information a business has about them, and where (by category) that personal information came from or was sent.
• A right to delete personal information that a business collected from them or to require that personal information not be shared.

• A right to opt-out of sale of personal information about them.

• A right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act, but with significant exceptions.

G. Record-keeping and Disclosure Requirements

The CCPA also imposes significant record-keeping obligations on businesses. They must (1) track consumer information from collection through sale or deletion, and (2) they must create a system to promptly respond to requests. The 12-month requirement requires every bit of potentially private information to be retained for a full year and to track how it is used both internally and by third parties. There must be at least two systems for receiving consumer requests, requests must be answered within 45 days plus one 45-day extension, and all systems must be designed to keep personal information private.

Requests from consumers must be verified as coming from the actual consumer. However, what is sufficient for verification is unclear. Businesses face the jeopardy that inadequate verification may cause them to disclose personal information to the wrong party, in effect a data breach. Also, there is a tension between the business’s need to retain sufficient data to demonstrate that it adequately verified the consumer and a consumer’s request that all of his or her data be deleted.

Businesses also have enhanced disclosure requirements. Privacy notices must describe consumer rights and how to exercise them, list categories of personal information collected, sold and disclosed in the prior 12 months and updated every 12 months, link to a “Do Not Sell My Personal Information” page, identify categories of third parties who will receive the personal information, and identify financial incentives offered by the business.

H. California’s Confusing Anti-Discrimination Rule

The CCPA broadly gives consumers a right against having to pay a different price for goods or services because they don’t share their information. But the CCPA also carves out two enormous exceptions. First, retailers remain free to offer “financial incentives” for sharing information, an exception clearly intended to encompass the already widespread practice of offering discounts or coupons to consumers who subscribe to mailing lists. To offer financial incentives, retailers must provide notice to consumers (but the law references sections with no notice requirements), consumers must give the retailers prior opt-in consent, which the consumers may revoke at any time, and incentives must not be “unjust, unreasonable, coercive or usurious.”

Second, the CCPA allows retailers to offer lower prices to consumers who share their information if the discount is “reasonably related to the value provided to the consumer by the consumer’s data.” It is deeply unclear how to interpret this value provision, an invitation to litigation. Business therefore are likely to stick with the broad-based, financial incentives that
are plainly acceptable and wait until regulations or judicial decisions clarify the precise meaning of the nondiscrimination provision.

I. The Right to be Forgotten

Consumers have right to request that business delete from its systems the consumer’s personal information or to request that the information not be shared with third parties. However, the language of the statute suggests that this right only applies to information that the business collected directly from the consumer, thus creating operational challenge to track source of each piece of data. The right to ask that information not be shared may prove more difficult for retailers than simply deleting it altogether, especially since the term “third party,” as defined in the statute, includes virtually anyone, even parent or affiliated companies.

Business must also “direct any service providers to delete the consumer’s personal information from their records.” However, the definition of “service provider” is limited to entities with whom the business has a “written contract” that contains certain express prohibitions.

There are limited exceptions to the right to delete personal information. For example, a business need not delete a consumer’s personal information if the business needs it to “exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.” Also, a business may keep personal information “to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business.” Confusingly, another exception uses similar language, and it’s unclear how these interact. See Section 105(d)(9) (“Otherwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information”).

Deletion is a particularly tricky aspect of data privacy, because it raises First Amendment concerns. If a statute can compel an internet service provider to delete all copies of a post made by a data subject, it could take away the ability of others to re-post the information and comment on it.

J. Financial Institutions Under the CCPA

The CCPA has a limited exclusion relating to financial information covered by the Gramm Leach Bliley Act (GLBA). The CCPA does not apply to personal information collected, processed, sold or disclosed pursuant to the GLBA, but with two enormous caveats: (1) the definition of “personal information” is so broad that it reaches far beyond information covered by the GLBA, and therefore it is likely to apply to some of the data collected by financial institutions, and (2) the exclusion relating to information covered by the GLBA does not apply to the private right of action and statutory damages available to individuals in the event of a data breach.

1. The Varying Scope of Personal Information under GLBA and CCPA

Because of the broad definition of “personal information” under the CCPA, financial institutions would remain subject to the provisions and requirements of the CCPA for all
activities falling outside of the GLBA, which could include activities conducted by their wealth management businesses and information they collect online.

The GLBA regulates financial institutions' management of “nonpublic personal information,” which is defined in 15 U.S.C. § 6809 as personally identifiable financial information: 1) provided by a consumer to a financial institution; 2) resulting from any transaction with the consumer or any service performed for the consumer; or 3) otherwise obtained by the financial institution. In contrast, the CCPA defines “personal information” as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. It is not limited to financial information. The CCPA definition of personal information includes, for example, internet protocol addresses, browsing history, search history, biometric information, geolocation data, consuming histories or tendencies, professional or employment-related information, and inferences drawn from a consumer’s interaction with a website. “Inferences drawn” can include a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

For all information relating in any way to a California resident that is not financial information under GLBA, financial institutions will be subject to all of the reporting, disclosure and record-keeping requirements of the CCPA, and must have in place processes to respond to consumer requests. Consumers have a robust right to know the categories and specific pieces of information collected about them, the sources of that information, the purposes of collecting, and the identity of all third parties with whom the information is shared, including affiliates. They also have a right to access that information, to restrict its transfer and to require its deletion. Businesses subject to the CCPA must be able to provide this information and these rights for the past 12 months, meaning that for requests received after January 1, 2020, when the law comes into effect, businesses must have detailed record-keeping going back to as early as January 1, 2019.

2. How Would the Private Right of Action Under CCPA Apply to Financial Institutions?

The CCPA provides that its exemption of non-public personal information governed by GLBA "shall not apply to Section 1798.150." This carve-out from the exemption means that Section 1798.150 will apply to financial institutions, including to its non-public personal information governed by GLBA. The impact of this cannot be overstated. Section 1798.150 sets forth a private right of action for consumers to seek statutory damages of not less than $100 and not greater than $750 “per consumer per incident or actual damages, whichever is greater” if the consumer's information “is subject to an unauthorized access, exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices.” In other words, GLBA-regulated entities will still be subject to millions of dollars of potential damages through class-action lawsuits if they experience a data breach.
II. The progress toward a federal data privacy law

Big tech companies are pushing for a federal bill to preempt California's law. But California Attorney General Xavier Becerra warned on November 28, 2018, that Congress should not pass a relatively weak online privacy bill to protect consumer data and use it to take precedence over a new California law. U.S. lawmakers are drafting a privacy bill, expected to be finished early in the next session of Congress.

Various industry and consumer groups have ramped up their lobbying efforts to persuade Congress to adopt a new and pre-emptive privacy framework before more states follow the California model and possibly add even more onerous requirements. The pressures building to enact such legislation include the multiple, inconsistent state and sectorial federal laws governing privacy in the U.S., the broad reach of the GDPR and its effect on business practices, and the radically new approach to privacy taken by the CCPA.

There appears to be a growing consensus about the broad parameters of a new federal law. As with the GDPR and the CCPA, a new federal law would likely require transparency in how information is being collected, used, shared and stored. Consumers would require real notice and content to use and share personal information and have the flexibility to move data between services. However, it is unclear what the breadth of the definition of personal information would be, and what would be required for consent.

However, the challenges to adopting any federal legislation are numerous, and many interest groups, most notably the giant data companies Facebook, Amazon and Google, are already heavily lobbying. Certain international businesses and perhaps the FTC would want the federal legislation to meet the GDPR adequacy standard, which would facilitate international data transfer. Other businesses would want an easier privacy standard, and would want that new standard to preempt the U.S. sectorial approach, including state laws such as the CCPA.

A. The U.S. Sectoral Approach

With multiple privacy laws already on the books in all states and federal laws addressing particular sectors, U.S. companies are already faced with multiple different approaches, standards, and enforcement authorities. Some laws are more protective of privacy than others. In consequence, any new federal privacy laws will necessarily raise privacy standards in some areas and lower them in others. Moreover, the authorities currently enforcing existing laws are likely to resist losing their jurisdiction.

B. Congressional Gridlock

Getting anything through congress is another giant obstacle. Multiple congressional committees have overlapping jurisdiction with respect to privacy. There are at least six legislative committees in the House of Representatives with jurisdiction over some existing privacy law or agency. Other committees, as well, may claim interest in a privacy bill, including the powerful Appropriations Committee. If the proposed new legislation has to be reported out of multiple committees, and with the prospect of jurisdictional fights, the chance that they all would agree on the same proposal is vanishingly small.
C. Fight Over a Private Right of Action

A private right of action would allow consumers to sue data controllers and may include class action lawsuits on behalf of multiple consumers. Damages under such scenario could be huge. Privacy advocates would favor private rights of action, because federal and state regulators simply will not have the resources to police privacy laws effectively. On the other hand, most businesses would see class actions as unwarranted expenses that would benefit no one. Even meritless cases may be settled for large amounts if they survive the motion to dismiss stage, principally benefiting only the plaintiffs’ lawyers.

A likely outcome might be to allow state AGs to enforce the federal law in addition to the federal agency, probably the FTC, charged with enforcement. The FTC is likely to be given explicit rulemaking authority and additional resources to focus on enforcement. One possibility that would allow private rights of action would be for the law to include some significant barriers to private actions but to allow them under certain limited circumstances. There might be monetary damage limits as well.

D. Federal Preemption

The business community is looking to a new federal standard to preempt the CCPA and other state laws that impose multiple and inconsistent requirements on them. On the other hand, consumer groups feel that the new federal standard should represent a floor on compliance obligations and not a ceiling, and that therefore states should be free to impose additional protections for data privacy. Some states may attempt to get around preemption in the way that California is seeking to circumvent the FCC’s ruling ending net neutrality. They may restrict their own state governments from contracting with companies that are not complying with some stricter privacy standard. Thus, states with significant market influence could us the market to impose their own higher standards.

E. Disagreements within the Business Community

Larger, multinational companies would want the U.S. to move toward international data protection standards, which to them would be the least costly solution and would facilitate data flow across borders. On the other hand, smaller or more localized companies would prefer a weaker federal law that would impose fewer obligations and would totally preempt state law. Then the third faction, consumer groups, will want to get as much protection as they can get. Lobbyists for all groups will be active.

No matter what the contours of the eventual federal legislation, the EU will decide for itself whether the new U.S. law meets the adequacy standard of the GDPR. It is unlikely that the EU will give the U.S. the benefit of the doubt.

F. Proposed Framework from the NTIA

In September, the U.S. Department of Commerce’s National Telecommunications and Information Administration (NTIA) proposed a high-level framework for consumer privacy protection. This framework articulated a set of organizational practices focused on data transparency, minimization of collect, the storage, use and sharing of data, security, and risk
management. It also sought to reconcile a diverse regulatory patchwork and ensure that proper resources would be allocation to enforcement.

The NTIA received public comments from over 200 governmental, academic and private sector organizations on developing the Administration’s approach to consumer privacy. Not surprisingly, the focus of many comments was on the GDPR and the CCPA. The European Commission (EC) submitted comments, predictably advocating for better integration and reconciliation of disparate privacy laws, which would provide more certainty to businesses and better transparency and predictability to consumers. The EC did recommend greater attention on two principles present in the GDPR that were absent from the NTIA proposal, namely (1) requiring consent or other lawful bases to process data, and (2) specifying a purpose for data processing.

Many commentators approved of the initial steps taken by the NTIA, but interested parties will need to see more details concerning the proposal before it is possible to predict where U.S. federal privacy law will land.