Debevoise Update D&P

The California Consumer Privacy Act: Compliance Strategies for Financial Institutions

May 2, 2019

Financial institutions are, and should be, acting now to plan for compliance with the new California Consumer Privacy Act. The CCPA exempts personal information covered by certain financial privacy laws. That is not surprising, since the law was enacted mainly with the privacy practices of major tech companies in mind. But the limited exemption for financial data is not a "get out of jail free" card for financial institutions. With the statute taking effect on January 1, 2020, now is the time to chart the path to compliance. For most financial institutions, that path will start with data mapping and other factual diligence. From there, the path will continue to gap analysis and then the implementation of any needed policies, procedures, and technical measures.

In broad strokes, what does the CCPA do? The CCPA provides consumers with broad new rights to access and delete their personal information held by most major for-profit companies. Consumers also are empowered to stop companies from selling their personal information. Companies are required to implement practices that will give teeth to the new consumer rights. Notably, a "do not sell" button will have to appear on many webpages. Policies, procedures, and training will be required to ensure prompt response to access and deletion requests.

Compliance challenges are magnified because key terms are defined very broadly. A "sale" is virtually any sharing of data with a third party. A "consumer" is any natural person who resides in California. "Personal information" is virtually anything that directly or indirectly identifies a consumer or her household, including "inferences." Data can be exempted from CCPA requirements if it is "deidentified," but that requires meeting a rigorous set of procedural and technical requirements.

Can I plan for compliance based on the existing law? Yes and no. The CCPA is a bit of a moving target. One round of amendments has already been enacted into law. More amendments appear to be on the way, including one that (if enacted) would narrow the law by carving out employee data and another that would add a private right of action for privacy violations.

Another possible amendment would “eliminate a consumer’s right to request a business to delete or not sell the consumer’s personal information” it if is necessary to retain the information to complete an insurance transaction that is regulated by California’s Insurance Information and Privacy Protection Act. The amendment would also add privacy protections for consumers—including notification obligations for insurance institutions and agents—to California’s Insurance Code.

The California Attorney General also is due to issue implementing regulations. All that said, many of the core elements of the statute as it now stands seem unlikely to change.

What are the first steps toward compliance with the CCPA? For most financial institutions, the best starting place will be a diligence and data-mapping exercise. The goal is to determine what sort of personal information is being collected, held and shared by the institution, and where that information lives. This step will require a wake-up call to stakeholders who may be thinking of “personal information” in terms of older, narrower legal definitions. Based on the results of the diligence process, financial institutions should conduct an analysis to identify gaps between the institution’s current policies and practices and the obligations under the CCPA. The next step will be to develop or update policies, procedures and technical measures to comply with the CCPA.

Where do third parties fit in? A key consideration under the CCPA is that sharing with a third party is not a “sale” if the third party is contractually restricted from using the data for its own benefit. A rigorous effort to update vendor agreements to include such a restriction may well be indicated.

And then? New policies and procedures are likely to work best if robustly tested. Financial institutions may want to consider a cybersecurity-style “tabletop” exercise. Stakeholders from across the company would be gathered in a room and required to respond in real time to a hypothetical scenario: When a customer asks to access or delete her records, or to tag her data “do not sell,” how exactly will you act on those requests?

What about those exemptions for data that’s covered under other financial privacy laws? All through these compliance steps, financial institutions should take care to consider what data fits within the statutory exemptions. The September 2018 amendments to the CCPA created an exemption for “personal information collected, processed, sold or disclosed pursuant to” the federal Gramm-Leach-Bliley Act, and its implementing regulations, and for information governed by the California Financial Information Privacy Act. To the extent that you can get comfortable that you are handling data “pursuant to” one of these two laws, you can carve the data out of your CCPA compliance program.

How broad is the GLBA exemption under the CCPA? Not as broad as financial institutions would likely prefer. Unlike the HIPAA exemption that applies categorically to HIPAA "covered entities or business associates," the federal GLBA exemption and the California FIPA exemption apply to information, not institutions. Financial institutions thus will be well advised to consider, dataset by dataset, whether their data is covered by GLBA or FIPA. One critical component to understanding the reach of the exemption is examining the definitions of "consumer" and "personal information" under the CCPA on the one hand, and "consumer" and "nonpublic personal information" under GLBA on the other.

Who is a consumer under GLBA? A consumer is an individual who obtains a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes.

What information is regulated by GLBA and therefore outside the CCPA? The GLBA Privacy Rule protects a consumer's "nonpublic personal information." Nonpublic personal information is "personally identifiable financial information" that:

- Is "provided by a consumer to a financial institution";
- "Result[s] from any transaction with the consumer or any service performed for the consumer"; or
- Is "otherwise obtained by the financial institution."

The Privacy Rule sets out the definition for "personally identifiable financial information"—it is information:

- that a consumer provides to a financial institution "to obtain a financial product or service" from the financial institution;
- "about a consumer resulting from any transaction involving a financial product or service" between the financial institution and a consumer; or
- that the financial institution "otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer."

What information is regulated under the CCPA? The CCPA applies to "personal information," that is any data 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."

What information would likely fall under the GLBA exemption? The core data generated in opening a financial account, or servicing it day to day, will likely be exempt. For example:

- Receiving and reviewing a loan application for a family car from a consumer.
- Opening a credit card with a financial institution for personal, family or household purposes.
- Opening a checking or savings account for personal, family or household purposes.

What personal data that a financial institution handles would not fall under the GLBA exemption? Hopefully the legislature or attorney general regulations will clarify this. For now, generally speaking, it seems likely that information collected through the following activities would be examples of personal data falling outside the exemption:

- A sole proprietor opening a business checking account.
- Personal details of representatives from corporate clients, third-party vendors, or non-account holder visitors to a physical facility.
- Data gathered from a visitor to a financial institution's website or mobile application, when the visit is outside the context of account opening or service.
- Marketing or analytics data.
- Subject to the pending amendment mentioned above—the data of job applicants, contractors, and employees currently is covered by the CCPA.

What should we do about employee data right now? Perhaps put it at the back of your compliance queue while the amendment mentioned above is pending. As noted, the proposed amendment would eliminate job applicants, contractors and employees from the CCPA's definition of "consumer." The proposed amendment has made it through a State Assembly committee. A fair guess is that the amendment will eventually become law. With all the other CCPA compliance tasks facing financial institutions, why not defer the challenge of employee data in hopes the amendment will indeed pass?

The amendment reinforces the need for a financial institution to go dataset by dataset in considering where CCPA compliance steps are needed. Consider Jane Jones, an employee of Big Bank who also holds an account there. The amendment would exempt Ms. Jones' HR file from the CCPA, but only if the information in that file is collected and used solely within the context of her role as an applicant, contractor or employee. Ms. Jones' account data would also be exempt from the CCPA, but on different grounds: the existing GLBA carve-out.

What about information governed by California FIPA? California FIPA's definitions of nonpublic personal information and personally identifiable financial information are nearly identical to the definitions under GLBA. Consumer is also similarly defined under California FIPA, except that consumers are limited to California residents for the purposes of California FIPA.

* * *

Our team would be pleased to discuss these issues with you.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Jeremy C. Beutler
jcbeutler@debevoise.com

D.C.

Luke Dembosky
ldembosky@debevoise.com

Satish M. Kini
smkini@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com