WHITEPAPER

A PLETHORA OF PRIVACY LAWS:
IG Challenges for Financial Sector

BY JOHN ISAZA, ESQ.,
VICE PRESIDENT INFO GOV, ACCESS

Contents

1 The Impact of CCPA
2 Responding to Consumer Requests
3 The Employee Temporary Exemption
4 Comparison with GDPR
4 Other State and Federal Concerns
5 IG Best Practices for Financial Sector
6 Conclusion

As if the financial sector did not already have to deal with enough compliance regulations, now comes a patchwork of privacy regulations across all 50 U.S. states and, of course, the rest of the globe if you are a multi-national company. The much-anticipated California Consumer Privacy Act (CCPA) is now in force as of July 1 of 2020, and a couple of dozen other states are entertaining their own privacy regulations, each with their own bent.

This whitepaper provides an overview of the most salient and impactful CCPA requirements, including a summary of recent clarifying amendments. It also provides a comparison of CCPA requirements against the European Union's GDPR, and finally a brief CCPA comparison with other state pending legislation and Federal oversight. We conclude with best practices for the financial sector to stay abreast of this ever-dynamic area of law.

The Impact of CCPA

Before jumping into the specifics of the CCPA, let's recap why CCPA is so significant. As noted in an article this author co-wrote with Professor John Rothchild of Wayne State University Law School for a Business Law Today article:

> **"When it comes to privacy legislation in the United States, there is no single statute you can consult to provide the needed advice. In the United States, the law of privacy is commonly referred to as "sectoral," meaning that there is no overarching legal regime covering privacy generally, but rather a series of federal laws (and, often, accompanying regulations) each governing a particular subject matter. Nor is privacy protection in the United States exclusively at the federal level: federal law does not generally preempt state privacy laws, and state legislatures have not been shy about enacting their own regulations of privacy."**

This is where California comes in. CCPA is, to date, the most expansive and far reaching omnibus privacy law enacted by any state, made more significant by the fact that it represents the 5th largest economy in the world.

Responding to Consumer Requests

The CCPA grants consumers more control over and understanding of their personal information. It defines personal information broadly 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 basically means that any piece of data that could be linked or associated with a person in California must be given special treatment to ensure CCPA compliance. Seemingly innocuous data such as cookies accessed from a user's computer, or incidental demographic data collected when a visitor goes to a business website, would fall under this definition.

To comply, the financial sector must be prepared to address the following consumer requests and, by extension, include within their privacy policy:

- Requests to disclose the categories and specific personal information collected about the consumer;
- Requests to disclose categories of sources from which the information is collected;
- Requests to provide the business purposes for collecting and/or selling the information;
- Requests to disclose categories of third parties with which the information is shared;
- Requests to delete personal information;
- If the business sells the consumer's personal information, or discloses it for a business purpose, requests to disclose the categories of information and the identity of third parties to which the information was sold or disclosed.

Additionally, and perhaps most unique to CCPA, a business cannot discriminate against a consumer who opts out of the sale of their personal information. If this opt-out is selected, businesses are prohibited from discriminating against consumers for exercising this right. Prohibited discrimination could include charging a different price for consumers who opt out, or for attempting to provide a different or lower quality of goods or services for doing so. That said, businesses may offer financial incentives to collect the consumers' personal information.

Finally, unless consumers under the age of 16 specifically and affirmatively opt in, businesses are prohibited from selling their personal information. Consumers between the ages of 13 and 16 years may opt in without parental authorization, but parents must provide authorization for consumers under the age of 13.

While the California Attorney General will enforce the CCPA, consumers also have a private right of action to sue for the unauthorized access and exfiltration, theft, or disclosure of their nonencrypted or nonredacted personal information. Finally, note that California has a ballot initiative (the California Privacy Rights Act) scheduled for a vote on November 3, 2020 which delves deeper into the rights of consumers. Should CPRA pass, a new and perhaps deeper analysis of the issue will be warranted.

The Employee Temporary Exemption

Since California legislators created the CCPA in haste (approximately 72 hours), it has resulted in many areas of confusion. As a result, California legislators have been busy enacting various clarifying amendments, some of which range on one end from simple as grammatical corrections to the other end with substantive carve outs.

One of the more substantive amendments impacts the extremely broad definition of a consumer. Under the original legislation, the definition of a consumer was interpreted to include employees of the organization. This prompted the much-publicized "employee exemption" to CCPA, signed by the governor on October 11, 2019. The exemption is basically a one year reprieve from compliance for employee data and was designed to give California legislators a one year deadline to pass a separate employee privacy bill. Note that if an employee privacy bill does not pass, the one year deadline will expire and employee data will need to be afforded the same treatment as any other California consumer data.

For the time being, per this exemption the following requirements will not apply to personal data in the following categories of individuals:

- Job applicant
- Employee
- Owner
- Director
- Officer
- Medical staff member
- Individual contractor

This employee exemption will only apply if the business collects or uses the personal information exclusively within the context of the individual's role or former role in the business.

The "employee exemption" also excludes emergency contact information that the business may collect, as well as information needed to administer benefits. Nevertheless, the exemption still requires notice on the use of employee data, while the employee still has a private right of action for mismanagement of employee data. This means that employers with employees or contractors in California should still review and revise employee privacy notices accordingly.

Related to the "employee exemption" is a new exemption that is also set to expire in one year. Under this new exemption, personal information that a business collects in a business-to-business (B2B) transaction is exempted from most CCPA requirements, but only if such data is collected when a California resident makes a written or verbal communication or transaction with a business

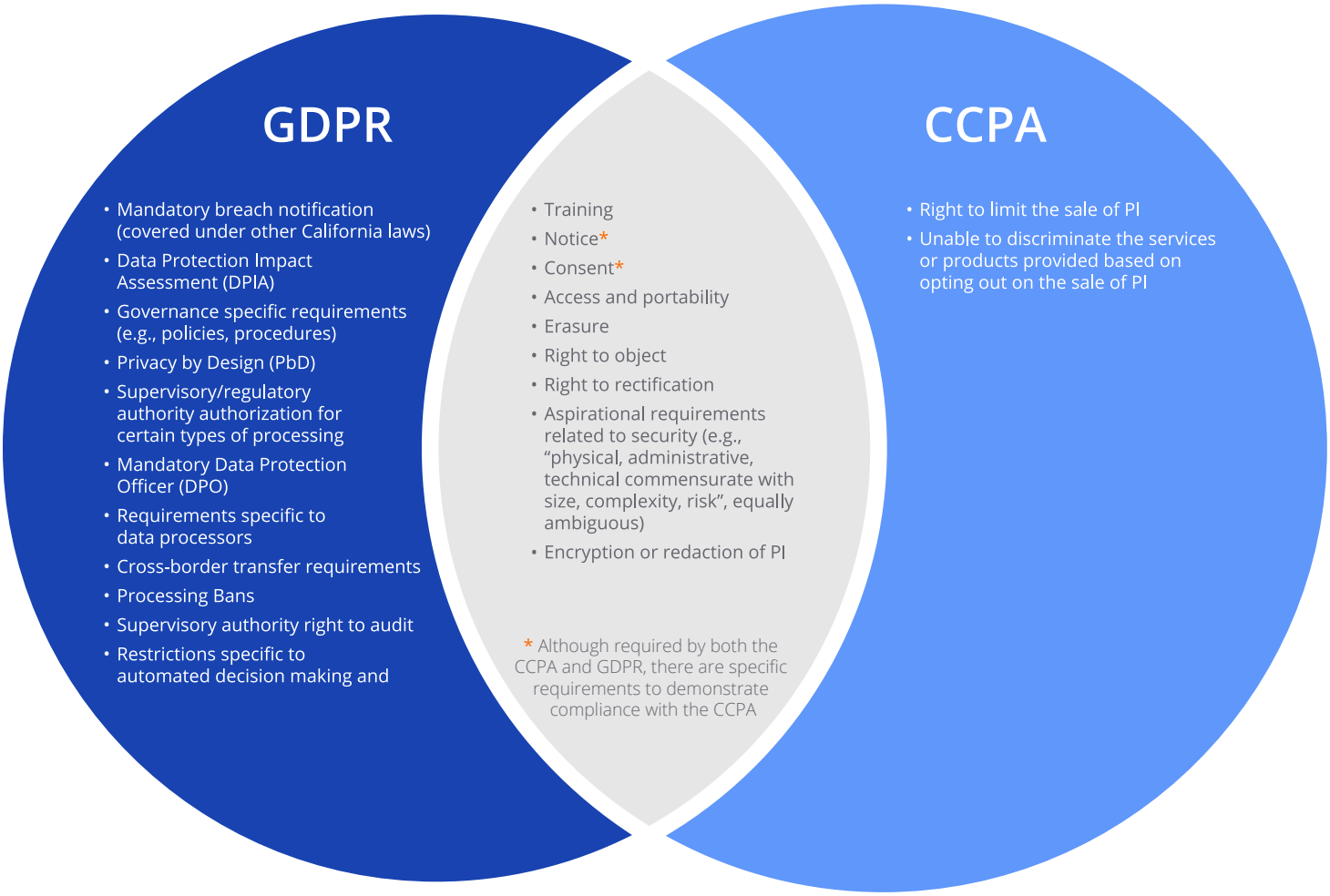
> **"within the context of the business conducting due diligence regarding, or provision or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency."**

Even so, a consumer private right of action for breach continues to apply in the B2B context. Also, opt-out and non-discrimination rights continue to apply, so business contacts may still opt-out from having their information "sold" to third parties, while a business may not deny goods or services or charge different prices to business customers because they have opted out. Note that this B2B exemption does not extend to cold-calling or other marketing communications. As such, a business must comply with all CCPA requirements such as notice, access, deletion, opt-out and deletion if the personal information belonging to potential business/customer contacts were obtained from a third party, such as a marketing list provider, until a communication or transaction occurs with the business "within the context of the business conducting due diligence regarding, or provision or receiving a product or service to or from" such business.

Comparison with GDPR

As the old adage goes, a picture is worth a thousand words. The following illustration provides a great overview of the overlap and differences between CCPA and the European Union's General Data Protection Regulation.

Leveraging GDPR Preparedness for the CCPA



Orignially published in the Wall Street Journal, and downloaded on January 16, 2020 from deloitte.wsj.com/riskandcompliance/2018/12/16/eu-gdpr-after-the-deadline-what-comes-next/

Other State and Federal Concerns

Since 2017, a few Federal agencies have issued opinions that continue to focus on the measures taken to protect the data, and not on limits on collecting it or even monetizing it. The Federal Trade Commission, for instance, has deemed that failing to reasonably secure personal information, including financial information, health information and contents of communications, constitutes a "deceptive or unfair" commercial practice.

The Securities and Exchange Commission (SEC) is also pursuing lawsuits for what are essentially privacy violations. The SEC alleged, for instance, that Facebook Inc. was making misleading disclosures regarding the risk of misuse of Facebook user data. This resulted in a $100M settlement with Facebook. Multiple states have filed HIPAA data breach lawsuits for failure to protect electronic personal health information. Finally, the Consumer Fraud and Abuse Act has been invoked to stop scraping of data from other websites, but at least one case actually confirms that data collected from a public source is fair game.

At the state level, ever since the adoption of CCPA many other state legislatures have begun to consider similar omnibus privacy laws, often based on either the CCPA or on GDPR. This has led to adoption of comprehensive privacy laws in a few more states, including Maine, Nevada, Oregon, and Washington. Another 13 states have either active bills or ongoing studies that could progress to legislation over the next 2 years. In general, the new omnibus legislation proposed in these states shifts the state law focus from data security and breach notification to giving data subjects rights to opt-out of use or sale of their data, along with the right to request deletion of their data.

The trend in the states is to take a more active role to preserve data privacy within their borders instead of a federalist approach to enforcement, as has been done in Europe. Prior to the passage of CCPA, focus of the state regulations was primarily on the act of protecting the data, and not as much on the rights of consumers to dictate how it is used, barring exceptions for removal of the data of minors as required in California. Now, newer statutes and amendments to existing statutes place an increased focus on providing opt-out provisions to enable consumers to prevent storage and use of their personal information.

IG Best Practices for Financial Sector

In order to stay compliant with the numerous state and global privacy regulations, the following should be implemented at minimum:

- ✓ Designate a data protection officer.
- ✓ Stay abreast of global record retention laws applicable to the organization, so that you can justify retention of certain data even if considered personal information.
- ✓ Create and maintain a records retention schedule that takes into account not only global retention requirements but also business need and statute of limitations considerations. The retention schedule is the first line of defense not only in discovery, but also in justifying retention when faced with privacy claims.
- ✓ Survey data to determine the source and subject of data, where it is stored, and what can be retained and used.
- ✓ Segment US usable data from EU data, so that it may legally process it in the US for marketing and other efforts.
- ✓ Segregate data originating from individual European data subjects, so that such data can be processed, disposed of, or monetized in compliance with the stricter dictates of the GDPR.
- ✓ Dispose of non-usable EU source data that is no longer being used for case administration.
- ✓ Segment data derived from U.S. sources to isolate data related to restricted content, such as health care data, data related to children, and certain personally identifying information such as social security or taxpayer ID numbers, names of minors, financial account numbers, or full birth dates.
- ✓ Draft a privacy policy that comports with current trends of strict data security.
- ✓ Develop procedures, guidelines and protocols to assure compliance with its published privacy policy.
- ✓ Designate a compliance program and conduct training for employees.
- ✓ Implement controls of privacy by design, allowing for privacy issues to be handled along the way of a consumer's digital footprint.
- ✓ Secure any third-party's cloud platforms.
- ✓ Encrypt personal information when it is being stored and transmitted, and store the encryption keys separately from the encrypted data.
- ✓ Develop procedures, guidelines and protocols to address securing data, restricting access to data, and disposal of data.
- ✓ Develop procedures and guidelines to respond to consumer requests.
- ✓ Along with Privacy Policy, post notice (i.e., revise the existing Privacy Policy) that (i) identifies categories of covered information, (ii) describes how consumers may review or request changes to their covered information, (iii) describes the process by which the Operator notifies consumers of material changes to the notice, (iv) discloses whether a third party may collect covered information, and (v) states the effective date.
- ✓ Develop audit and compliance oversight over all of the above noted recommendations.

Conclusion

The bottom line is that the rights given to consumer over their data have landed on our shores. The rest of the country is starting to fall in line, with at least 13 other states from Hawaii to Maine proposing different flavors of privacy omnibus legislation. If you are doing business that in any way touches California consumers, it would be prudent to fall in line with CCPA compliance, beginning with a close look at your retention schedule, its supporting research, your Privacy Policy and those of your third party vendors with whom you may be sharing data. If you think you are staying out of California, which is very hard to avoid given the sheer size of its population, then you need to keep an eye on the several other states with pending legislation.

It appears that the east coast is more likely to align itself with GDPR, while the west coast is aligning with CCPA. In any event, privacy in the United States is not an issue where you can simply tick off a box once and forget about it. Policies should be reviewed annually depending on the growth of your business and the different privacy laws of the states where you may be accessing consumer data.

About the Author

John Isaza is a California-based attorney, Vice-President of Information Governance Solutions at Access Corp, featuring a cloud-based software for records information management and global research he co-created called Virgo™. He is also a partner at Rimon Law, where he chairs the privacy, records management and information governance practice. Mr. Isaza is one of the world's foremost experts in the field. He has developed information governance and records retention programs for some of the most highly regulated Global 1000 companies. He is co-author of 7 Steps for Legal Holds of ESI & Other Documents, a contributing author to the ABA's Internet Law for the Business Lawyer, 2nd Edition, as well as Editor-in-Chief and co-author of Handbook on Global Social Media Law for Business Lawyers. Mr. Isaza is past co-Chair of the American Bar's Social Media Subcommittee, a Fellow of ARMA International, and current co-Chair of the ABA's Consumer Privacy and Data Analytics Subcommittee.

John may be reached at John.Isaza@RimonLaw.com or on his cell at 949.632.3860