Session 203 | CCPA Compliance: Lessons Learnt from the GDPR

As the fifth largest economy in the world, California is a marketplace inside and outside of the United States that businesses can’t ignore. Many global corporations that have already adapted to comply with Europe’s General Data Protection Regulation (GDPR) will have a head start on many of the changes that will be crucial for effective CCPA compliance. However, the two laws are very different in terms of scope, notice requirements, liability and enforcement risk, and required accountability measures. There is much to learn before the effective date (January 1, 2020) of the CCPA. This session will discuss applying the lessons learned from the GDPR to the CCPA. The program will discuss key considerations, such as: leveraging GDPR “data mapping” experience as a tool to account for the universe of “personal information” a business collects, developing CCPA-compliant service provider agreements, responding to consumer rights requests.

Moderator:
Ann Chen, Abbot

Speakers:
Alex Simpson, Microsoft
Michael Spadea, PricewaterhouseCoopers
Aaron Ting, Facebook
Xiaoyan Zhang, Reed Smith
CCPA Compliance: Lessons Learnt from the GDPR

July 10, 2019
Understand your organization’s governance, data and processing
GDPR records of processing

- Article 30 records of processing (data processing inventories) are the foundation stone of GDPR compliance.
- Most aspects of your privacy strategy flow from your records of processing.
- Many companies have not finished their records of processing or have allowed them to become out of date.
- Records of processing are living documents. Keeping them updated is an iterative process. When your company changes, your records of processing must change.
- Privacy fatigue is real. Many decision makers have moved on from GDPR (or privacy in general).
A (CCPA) Privacy Program

- Scoping
- Governance
  - Company policy matters (high level)
  - Risk assessment and tolerance
  - Allocation of resources
- Project management
  - Inventory / map
    - Priorities
    - Categories / layers
    - Access, uses, and permissions
      - Internal
      - Third parties
- Notifications (privacy policies)
- Procedures
  - Preference management
  - Vendor management
  - Incident response
- Training and awareness
Prepare for the exercise of data subject rights
Data subject rights requests in the EU

- **People in the EU know about their GDPR rights.** Public awareness of GDPR is relatively high. People are better informed about their GDPR rights than many other rights they enjoy.

- There has been a **significant up-tick** in people exercising privacy and rights since GDPR was introduced.

- Policies and procedures must be **stress tested**. First responders need to be trained. Training needs to be frequently refreshed.

- How can you **verify** a requestor’s identity?

- What about **third party websites** that facilitate requestors submitting many requests at once?

- GDPR is about **more than just subject access requests**.
CCPA

• **Know how seemingly similar rights under GDPR and CCPA vary.** Both CCPA and GDPR give consumers the right to access, erasure (deletion), portability, and a restriction of processing, but not in the same ways:
  - Portability
  - Deletion
  - Restriction/opt out of sale

• **Know the new rights consumers have under CCPA.** In addition to the above rights, where a business may already have a foundation in place to respond, businesses must consider new rights:
  - Non-discrimination concept
  - Financial incentive concept
CCPA (cont.)

• As the culture of privacy shifts, there will be an increase in requests as time goes on.

• Business must be prepared to respond within allocated timeframe.

• Processes must be implemented to verify requests to avoid holding up response time.

• As with other aspects of a privacy program, data subject rights procedures must be regularly tested, reviewed, and updated.
Address supply chain and business partner considerations
GDPR Article 28 contracts

- Many companies viewed 25 May 2018 as the ‘drop dead date’ to update their third party contracts with GDPR Article 28 language. This led to frantic and frenetic activity.

- Some companies are now struggling to understand which privacy terms apply to third party contracts. Many companies are engaged in ‘battle of the forms’ as it is not clear which company’s terms apply.

- Example: your ability to respond to a personal data breach affecting your vendor is inhibited if you do not know what their contractual privacy obligations to you are. You will lose precious time discussing things like liability, costs allocation, whether assistance is ‘reasonable’, ‘commercial’, and so on.

- Take the time to step back, segment your vendor ecosystem, organise and prioritise. Be proactive, not reactive.

- Systematic and systemic reviews are necessary. This takes time and resources.
The CCPA Players – “Business”

“Business” means

(1) A legal entity that is for profit that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000)...(B) Alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business.
The CCPA Players – “Service Providers”

“Service Provider” means a [] legal entity that is...for [ ] profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.
"Third Party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract: (i) Prohibits the person receiving the personal information from: (I) Selling the personal information. (II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract. (III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business. (ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them. (B) [similar safe harbor as for service providers]
Fundamentals, and Some Sort of Carrot

**A:** Diligence

**B:** Contract

**C:** Oversight/validation

Safe harbor under CCPA

- A business is not liable for a service provider’s actions “if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation.”
Contracting considerations

• Backward-looking and prospective
• Prioritization
• “Service providers” and “third parties”
  • Contract implications
  • Disclosure obligations
  • Data subject rights obligations
Document an appropriate information security program
GDPR security principles

• GDPR is not prescriptive about specific technical and organisational measures that companies must take. However, Article 32 does include examples types of security measures which may be appropriate depending on the nature and risks of your processing activities.

• Some information security concepts are mentioned in GDPR – encryption, pseudonymisation, ensuring ongoing system confidentiality, integrity, availability and resilience.

• A few of the EU member state regulators have issued local minimum security guidelines/recommendations.

• Principle of accountability: maintaining sufficient records is a key part of any GDPR information security program.
CCPA

- CCPA supplements existing law, including Cal. Civ. Code § 1798.81.5: duty of “reasonable security procedures and practices appropriate to the nature of the information.” Could be extended to data breaches where there is a violation of that duty.

- Similar to GDPR, “reasonable security procedures and practices” is not a clearly defined standard.

- There has been guidance from the CA AG:
  - “The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”
  - Emphasis on encryption and multi-factor authentication.
Develop methods for on-going compliance and assessment of accountability
What have clients learned from GDPR year one?

- GDPR compliance is **iterative, ongoing and never static**. Be able to demonstrate and measure it.

- Significant **regulatory enforcement is coming** (look at ICO’s intention to fine British Airways and Marriott). Be prepared. Privacy immature organizations will panic when big fines are handed down. Privacy mature organizations will look to the guidance provided by regulators through enforcement.

- Policies and procedures are important. **Stress testing** them, **training**, **refresher training**, **drills** are even more important. Focus on your front line responders. Who is most likely to receive a data subject request? Can they recognize it? Can they triage it? Do they know how to escalate it?

- Find a way to **fight privacy fatigue**. Enforcement actions will help but perhaps it’s time to refresh and focus minds.
What have clients learned from GDPR year one? (cont.)

• **Do what you can proactively.** You may think you have no time or resources now but compare this to when you’re reactively fighting privacy fires on more than one front.

• Figure out what **privacy compliance model** works best for your company. Privacy champions? Full time privacy posts? Hybrid?

• **Automated tools** are helpful but they cannot be your only line of defense.

• **Make privacy a competitive differentiator.** Don’t view it as a compliance burden, embrace it as something that your customers can use to trust you.
Accountability to Regulators: AG enforcement under the CCPA

- Under the CCPA, a business “shall be in violation of [the CCPA] if it fails to cure any alleged violation within 30 days of after being notified of alleged noncompliance.”

- The California Attorney General has the authority to seek injunctions and assess penalties against businesses that violate the CCPA.

- The California AG may assess statutory penalties not to exceed $2,500 for each violation or $7,500 for each intentional violation.
Accountability to data subjects: class action exposure under the CCPA

• “Any consumer whose nonencrypted or nonredacted personal information...is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.”

• Under this private right of action, affected consumers may seek: (1) damages in an amount between $100 and $750 per consumer per incident or actual damages, whichever is greater, (2) injunctive relief, or (3) any other relief the court deems proper.
Accountability to data subjects: class action exposure under the CCPA (cont.)

- A consumer may only bring a private action against a business for statutory damages if the consumer “provides a business 30 days’ written notice identifying the specific provisions of [the CCPA] that the consumer alleges have been or are being violated” before filing the action.

- If the violation can be cured and the business “actually cures [within 30 days] the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.”
Ongoing Compliance and Assessment of Accountability

• See Privacy Program (above)
• Resources and Toolkits
• Privacy engineering and design
• Third party management
• Review, update, and document relevant practices and procedures
  • Periodically
  • Upon changes in business processes
  • Upon changes in the law(s)
  • Upon conclusion of significant issues and incidents
Lessons

1. To be effective, a privacy program has to be implemented, maintained, tested, updated, and improved.

2. Not all third-party service providers and business partners are alike, yet most have access to some amount of personal data. The appropriate controls have to be imposed through contracts and technology.

3. Privacy protects, informs, and provides rights to individuals. The use of personal data by companies today changes (rapidly), and privacy measures must also be dynamic, in order to remain current.

4. Data subject rights can be tricky, and verification can be difficult. Be thoughtful and stay ready.

5. Currently, the key accountability measure in the CCPA is the prospect of litigation. Do what you can to avoid becoming a target.
Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward. Our belief is that by delivering smarter and more creative legal services, we will not only enrich our clients’ experiences with us, but also support them in achieving their business goals.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for the speedy resolution of complex disputes, transactions, and regulatory matters.

For further information, please visit reedsmith.com

This document is not intended to provide legal advice to be used in a specific fact situation; the contents are for informational purposes only. "Reed Smith" refers to Reed Smith LLP and related entities. © Reed Smith LLP 2019
California Consumer Privacy Act (CCPA)

Frequently asked questions (FAQs)
June 2019
Introduction

The California Consumer Privacy Act (CCPA) will provide new privacy rights that will have a significant impact on many businesses as of January 1, 2020. The unprecedented broad definition of covered personal information coupled with restrictions on the “sale” personal information and individuals’ rights to request access and deletion of their personal information, among other things, will require changes in business processes and controls.

Following the release of the CCPA and amendments, our IP, Tech & Data Group has received numerous thoughtful questions from clients regarding the implications of the new privacy law. In response, we are delighted to share some of the frequently asked questions that we have seen across sectors. Please note that there are numerous gaps and ambiguous areas in the law and recent amendment. Therefore, some the answers to the questions cannot always be a simple yes or no.

Please also note that there are several amendment bills currently moving through the State Legislature, some of which, if enacted, would substantially change the language and scope of key provisions of the CCPA. Our IP, Tech & Data Group will send our clients updates on material changes to the CCPA through webinars, client alerts, and Reed Smith’s Technology Law Dispatch blog, https://www.technologylawdispatch.com/. California also has a website that provides legislative information available here: http://leginfo.legislature.ca.gov/, and anyone can sign up for notifications regarding CCPA rulemaking developments through the California Attorney General’s Office: https://oag.ca.gov/privacy/ccpa.

Frequently asked questions

Q. What liability exists for a tax exempt organization that partners with a non-exempt service provider?
A. The CCPA does not apply to exempt organizations. An exempt organization, say a non-profit, likely would not lose its exemption by receiving services from an entity that meets the CCPA’s definition of “service provider.” However, an organization should analyze its potential obligations under the CCPA because if it is a CCPA-regulated business and it discloses personal information to a service provider, the organization is responsible for its own actions and also may be liable for the actions of its service provider if the organization had “actual knowledge or reason to believe” that the service provider intended to violate CCPA. §1798.145(h).

Q. Should CCPA-regulated businesses execute CCPA-compliant agreements with their service providers?
A. Yes. Businesses can exchange personal information with “service providers” as long as the service providers process such personal information on behalf of the business and execute a written contract that prohibits the third party from “retaining, using, and disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by [the CCPA] . . . .” §1798.140(v). Only under these conditions will the recipient be considered a “service provider” under the CCPA. A primary benefit of having such a contract in place is that businesses are not responsible for the CCPA violations of their service providers unless the businesses have actual knowledge or reason to believe that the service provider intended to violate the CCPA. Therefore an important method of reducing risk under the CCPA is to review and ensure that all agreements with service providers have the necessary provisions to meet CCPA requirements and to perform the diligence necessary to reasonably conclude that the service providers are not intending to violate the CCPA.

Q. What does it mean to say that regulated financial institutions are exempt from some of the CCPA? Do financial institutions still have to comply?
A. The amended CCPA states that with one exception it does not apply to “personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act.” Id., §1798.145(e). This provision makes clear for financial
institutions that nonpublic personal information subject to GLBA is generally not subject to the CCPA. However, in this same section, the CCPA creates an exception to the exemption by stating “[t]his subdivision shall not apply to Section 1798.150” which creates the private right of action for certain types of data breaches. Id. Therefore, it appears that financial institutions may be subject to the private right of action created by Section 1798.150 of the CCPA for data breaches of “personal information” under California’s data breach law.

**Q. Is there an exemption for clinical research data?**

**A.** Although the CCPA exempts certain clinical trial data, the underlying exemption language represents one of the law’s noted ambiguities. Specifically, the CCPA exempts “information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the [FDA].” Id., § 1798.145(c)(1)(C). As drafted, it is unclear whether the foregoing language exempts clinical trials only if conducted pursuant to the federal Common Rule (plus either of the two additional standards), which would not exempt certain privately funded research. Instead, commenters have requested that the language be construed more broadly to exempt clinical trial data if the research is conducted pursuant to any of the following: (a) the federal Common Rule, or (b) the ICH GCP standards, or (c) FDA human subject protection standards. Presently, without implementing regulations, it is unclear which of the foregoing interpretations will prevail.

**Q. What about health care information subject to HIPAA or CMIA?**

**A.** The amended CCPA exempts all “protected health information” collected by “Covered Entities” and “Business Associates” subject to HIPAA and “medical information” governed by the California Confidentiality of Medical Information Act (CMIA). Id., § 1798.145(c)(1)(A). The CCPA also exempts HIPAA Covered Entities and providers of health care governed by the CMIA, “to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information,” as described in the CCPA. Id., § 1798.145(c)(1)(B).

**Q. With respect to the requirement to produce a record of data collected, sold or disclosed pertaining to an individual, when does that requirement become effective?**

**A.** Consumers are entitled to submit access requests for information starting the day the CCPA becomes operative, i.e., January 1, 2020. Barring some additional interpretive guidance or further legislative changes, businesses subject to the CCPA should take steps to ensure that they are able to identify by category or categories the personal information collected, sold, or disclosed about each individual consumer in the preceding 12 months, beginning January 1, 2019, and record to whom that information was sold or disclosed. Id., §1798.130(a). Identifying and analyzing relevant systems and in particular how an organization might respond to mandatory consumer requests should be an early priority (and seeking budgetary resources to help ensure that systems are in place to address such requests).

**Q. Does the CCPA apply to employer-employee relationships?**

**A.** The CCPA’s applicability to the employer-employee relationship is ambiguous, largely because the CCPA defines “consumer” without describing the relationship between the individual and the entity that collects the individual’s personal information. The definition of “consumer” in the CCPA is broad and is any “natural person who is a California resident . . . however identified, including by unique identifier.” Id., §1798.140(g). The definition of “personal information” includes “professional and employment-related information.” Id., §1798.140(c)(1)(I). Employment-related information may include a wide range of employment records including employee personnel files. When the definitions of “consumer” and “personal information” are considered together, the CCPA could be interpreted to be applicable to employers with employees who are California residents if such employers are not exempt from the CCPA. The CCPA’s legislative history also does not provide guidance on whether lawmakers intended to exempt employees from the law’s protections. Interestingly, the terms “employer” or “employee” are never referenced in the legislative history. Rather, the legislative history focuses on the CCPA as it applies to “consumers” or “businesses.” The Federal Trade Commission has previously taken the position that “employees” are also “consumers” despite strong arguments suggesting such an interpretation dramatically expands compliance burdens and duplicates other regulatory agencies’ work unnecessarily and sometimes in conflicting ways. Therefore, it would not be surprising for regulators and courts to conclude that the CCPA applies to employers with respect to their California employee data.

The CCPA does not state that the business must be located in California for the CCPA to apply. Thus, if the CCPA applies to the employer-employee relationship, employers located outside of California that meet the applicability thresholds to qualify as a CCPA-covered “business” could be required to comply with the CCPA with respect to their California employees.
Q. Is a data inventory required under the CCPA? Or is that more of a practical “requirement” (unlike GDPR’s legal requirement for a registry/mapping)?

A. Unlike the GDPR’s express legal requirement to have a record of processing activities, a “data inventory” is not an explicit requirement of the CCPA. Rather, maintaining and understanding the data involved in your organization (e.g., applications, business processes, and data sharing) is an inherent obligation that may be necessary to comply with the requirements of the CCPA. The CCPA requires businesses to inform consumers as to the categories of personal information collected and the purposes for which the categories of personal information will be used. See § 1798.100. For example, consumers can request the categories of personal information collected, the categories of sources from which personal information is collected, the business or commercial purpose for collecting of selling the personal information, the categories of third parties with whom the business shares personal information, and the specific pieces of personal information the business has collected about the consumer. See § 1798.110. In order to comply with such a request, the CCPA requires that the business associate the information provided by the consumer in a consumer verifiable request to any personal information previously collected by the business and identify by category or categories the personal information collected about the consumer in the preceding 12 months. See § 1798.130(a)(3). A data inventory and internal controls that enable businesses to respond sufficiently to such requests in accordance with the requirements by the January 1, 2020, effective date (arguably to be able to look back at January 1, 2019, consumer data) appear necessary from a practical perspective even if not required on the face of the legislation.

Q. Does the CCPA also regulate organizations in other states that may serve a California resident like hotels, restaurants, etc.?

A. It would appear so, if the organization does business in California. The CCPA applies to any organization (even those operating outside of California) to the extent the organization operates for profit, collects California consumers’ personal information (directly or through others), and does business in California, in addition to satisfying one of three threshold requirements. See § 1798.140(c). The CCPA also applies to organizations that control or are controlled by a CCPA-regulated business that shares common branding. The flip side is that if an organization in another state does not do business in California and does not control or is not controlled by a CCPA-regulated business that it shares common branding with, the CCPA will not apply. Even CCPA-regulated businesses are exempted from the obligations to the extent the commercial conduct takes place wholly outside of California. See § 1798.145(a)(6).

Entities that are not technically regulated by the CCPA may be affected if they act as a service provider to a business that is. For example, CCPA-covered businesses may seek to enter into written contracts with service providers that operate outside of California. The contract might be drafted to meet the CCPA requirements of prohibiting the service providers from processing personal information other than to perform the specified services and requiring the service providers to delete personal information if the CCPA-covered business receives a deletion request. The California attorney general has the authority to bring a civil action against a service provider that fails to meet its CCPA obligations. §1798.155(a).

Q. Does gross revenue refer to income derived from California or gross revenue from U.S. territories (IRS reported), etc.?

A. The CCPA does not define “gross revenue,” so it is not clear whether annual gross revenue refers to California revenue or U.S. sales. For now, it seems advisable to assume the term is not restricted to California.

Q. When doing business with a CA organization, a company may obtain PI for a CA individual who holds an ownership interest in the CA organization or is an officer of the CA organization. Is this information subject to the Act even though it was provided in a business-to-business relationship for a commercial purpose? What if such information has to be obtained due to the Patriot Act, Know Your Customer, or other anti-money laundering laws?

A. In the context of doing business with a CA organization, any personal information obtained about a California resident seems to be subject to the CCPA. In other words, there is no express exception for collecting information that was provided for certain commercial purpose, such as information involved in commercial negotiations or business-to-business relationships. Under the CCPA, “collection” means “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means.” § 1798.140(e) (emphasis added).

Regarding information that has to be obtained due to the Patriot Act, Know Your Customer, or other anti-money laundering laws, the CCPA does not restrict or prevent a business’s ability to comply with federal, state, or local laws, or with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. See § 1798.145(a).
Q. Do you see the “per incident per consumer” calculation of damages to apply only to actions brought for violation of maintaining appropriate security or for all violations under the CCPA?

A. The private right of action under the CCPA applies only to consumers “whose nonencrypted or nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.” § 1798.150(a)(1). There is no private right of action for any other violation of the CCPA. In fact, specific lobbying efforts were made to clarify this point by explicitly noting that the cause of action is not to be based on violations of any other section. However, it is possible that the attorney general may consider per incident per consumer damage calculations when using its penalty authority for violations of other provisions. See § 1798.155(a). Unfortunately, past experience often suggests that regulators frequently take the most expansive interpretations of penalty authority when seeking to negotiate consent decrees and other relief.

Q. Are there any exceptions for small companies?

A. No, there are no explicit exceptions depending on the size of a company; however, the revenue threshold may be a proxy for the size of the company. However, even if the revenue threshold is not met, a company may meet the other CCPA criteria. To have CCPA obligations, an organization must: (1) have annual gross revenues in excess of $25 million; (2) alone or in combination, annually buy, receive for the organization’s commercial purposes, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or (3) derive 50 percent or more of its annual revenues from selling consumers’ personal information. See § 1798.140(c). To the extent an organization does not meet these requirements, the CCPA does not apply.

Q. Is sales history considered “personal information”?

A. Sales history is considered personal information under the CCPA if it “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” § 1798.140(o). The CCPA specifically contemplates “commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies” to be personal information if it satisfies that criteria. See § 1798.140(o)(D).

Q. Is GLBA a true exception from all requirements including disclosure, notice, and access/deletion requests?

A. Yes. The CCPA as a whole does not apply to personal information “collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations.” § 1798.145(e). Note that a CCPA-regulated business could still be subject to the CCPA for any other personal information that is not regulated by the GLBA, as the exception applies to the type of personal information rather than to the type of organization.

Q. Do GLBA-regulated entities need to comply with disclosure, notice, and access/deletion requests for information that may not fall within GLBA’s scope (e.g., IP address)?

A. Yes. CCPA- and GLBA-regulated entities likely need to comply with the CCPA’s disclosure, notice, and access/deletion requests for personal information that is not “collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations.” § 1798.145(e). This is one of the more challenging areas of the law and is an example of how, while the exception may appear to be broad, operationalizing it could be quite difficult and expensive in terms of determining how and when information is not collected, processed, sold, or disclosed” pursuant to the GLBA. As a practical matter, to the extent that personal information (as defined by CCPA) is linked to information that is collected “pursuant to” GLBA it seems likely that a reasonable interpretation would be to exempt such information from the CCPA. However, at present there is not yet any meaningful guidance and the legislation does not appear to address this specific consideration directly.

Q. We are about to embark on a data life cycle management/data classification project. Do you think this can help address the CCPA as we build out the process?

A. Absolutely. It is important to embed privacy-by-design into processes from the start, but remember to resist the temptation to act without a thoughtful plan. Make sure the data life cycle management/data classification project is integrated into a larger CCPA compliance plan that involves the phases we discussed: (1) assess and define boundaries; (2) conduct detailed scoping; (3) design solutions; and then (4) develop and implement them.
Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.

Our belief is that by delivering smarter and more creative legal services, we will not only enrich our clients’ experiences with us, but also support them in achieving their business goals.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for the speedy resolution of complex disputes, transactions, and regulatory matters.

For further information, please visit reedsmith.com.
Private and Confidential
By Electronic Mail

To: Potentially Affected Clients

Subject: California Consumer Privacy Act of 2018 (CCPA) Compliance Next Steps Guide

This memorandum provides an analysis of the California Consumer Privacy Act of 2018 (CA A.B. 375) (the “CCPA” or the “Act”) and identifies certain key compliance measures that companies might find helpful to consider as they begin implementation efforts. The CCPA was drafted and adopted over a very short timeframe. As a result, the Act presently has a number of redundancies, inconsistencies, and uncertainties that must be considered carefully.

In an attempt to clarify certain provisions and resolve drafting errors, the California Legislature has already amended the CCPA. Namely, on September 23, 2018, Governor Jerry Brown signed SB 1121, which amended the CCPA. SB 1121 does not change the effective date of the CCPA, which is January 1, 2020. However, the Attorney General (“AG”) is precluded from beginning an enforcement action under the CCPA until 6 months past the effective date or after July 1, 2020, whichever is sooner. Such a 6-month period is intended to allow businesses sufficient time to ensure compliance with the Act.

Businesses potentially subject to the CCPA should keep a close eye on continuing developments with the Act. However, it is likely the core requirements will stand. Therefore, we have strived to provide practical recommendations to help direct efforts to comply with the CCPA.

EXECUTIVE SUMMARY

The CCPA is applicable to any for-profit company that does business in the state of California, collects consumer personal information (“PI”) or determines the purposes and means of processing such PI, and meets at least one of the following criteria:

1. The company has annual gross revenues in excess of $25 million;

2. Alone or in combination, it annually buys, receives for commercial purposes, sells, or shares for commercial purposes, the PI of 50,000 or more consumers, households, or devices; or

---

1 This memorandum is intended to provide an overview and a guide of general, practical items to consider in connection with CCPA compliance. It is not intended to be legal advice, as individual company needs may vary.

2 Other key changes under SB 1121 include: (i) The AG now also has until July 1, 2020 to adopt regulations meant to “further the purpose” of the CCPA; (ii) consumers are no longer required to notify the AG within 30 days of filing such a private action; (iii) SB 1121 specifically prohibits the application of the CCPA to a financial institution that collects, processes, sells, or discloses personal information pursuant to the federal Gramm-Leach-Bliley Act or the California Financial Information Privacy Act; (iv) SB 1121 also does not extend to protected health or medical information governed by the federal Health Insurance Portability and Accountability Act or the California Confidentiality of Medical Information Act; and (v) SB 1121 clarifies that any business in violation shall be subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation.
3. Derives 50% or more of its annual revenues from selling consumers’ PI.

Any company that satisfies the definition above is considered a “business” under the CCPA and is therefore subject to the Act. We recommend that any company subject to the Act conduct a data inventory and collection assessment as a preliminary step, if they have not already done so, to identify what consumer PI the company currently collects, utilizes, stores, and, if applicable, sells or discloses to third parties. The assessment should also identify how the company handles consumer PI and where it currently stores consumer PI. Attached to this memorandum as Exhibit A is a condensed reference of key CCPA compliance measures, and attached as Exhibit B are high-level sample questions to help assess the kinds of PI that a company may hold.

Once the relevant data sets and systems have been identified, the company can turn to implementation of key compliance measures in the following areas:

1. Customer notices and disclosures (at or before the point of data collection), which may require revisions to the company’s online privacy policy and homepage;

2. Development and implementation of processes to intake and respond to “verifiable” consumer requests to receive specific information regarding the collection, handling, sale, and disclosure of their PI and/or to delete their PI;\(^3\)

3. Development and implementation of processes to allow adult consumers to opt out of the sale of their PI, and, if applicable, to allow adult parents or guardians to provide opt-in consent for the sale of minors’ PI;

4. Assessment of whether the company will choose to put into effect financial incentive programs for the collection, sale, or deletion of consumers’ data; and

5. CCPA training for affected employees.

---

\(^3\) Due to the CCPA’s expansive definition of PI, the depth and complexity of information required to respond to consumer information requests under the Act, and the short timeframe required for a company to respond, this requirement likely presents the most difficulty.
ANALYSIS OF COMPLIANCE MEASURES

I. Customer Notice Requirements – Website and Privacy Policy Updates

The Act requires that “at or before the point of collection” of a consumer’s PI, companies must make specific and detailed disclosures to the consumer regarding the categories of PI to be collected, the purposes for which the categories of PI will be used, the consumer’s right to request information regarding his or her PI, to restrict the sale of his or her PI, his or her right to receive non-discriminatory treatment regardless of whether the consumer has restricted the company’s use of his or her PI, and the right to request the company to delete his or her PI. Companies are barred from collecting categories of PI other than those they have specified in their disclosures and are also barred from using PI for additional purposes unless the consumer has been notified. See 1798.100(b).

For most companies, this will mean necessary disclosures will need to be included in their online privacy policy prior to January 1, 2020 and that policy – including any California-specific description of consumers’ privacy rights – must be updated every 12 months and include the following elements:

- Description of a consumer’s rights under the CCPA (described in detail in each relevant section below) and identification of at least one of the company’s designated methods for submitting information requests;
- List of the categories of PI (statutory definition provided below) the company has collected about consumers in the preceding 12 months;
- List of the categories of consumer PI the company has sold in the preceding 12 months or a statement it has not sold consumers PI in the preceding 12 months;
- List of the categories of PI it has disclosed about consumers for a business purpose in the preceding 12 months, or a statement that it has not disclosed consumer PI for a business purpose in the preceding 12 months; and
- Description of a consumer’s rights pursuant to Section 1798.120 (relating to selling PI) and a separate link to the “Do Not Sell My Personal Information” Internet Web page;
- Description of the consumer’s right to request the deletion of the consumer PI.4

See 1798.130(a)(5); 1798.135(a)(2).

---

4 1798.105(b) of SB 1211 reads: “A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer’s rights to request the deletion of the consumer’s personal information.” However, SB 1211 also notes that SB 1211 “would modify that requirement [for a business to disclose the consumer’s right to delete PI on its Internet Web site or in its online privacy policy or policies]” by requiring a business . . . to disclose the consumer’s right to delete [PI] in a form that is reasonably accessible to consumers and in accordance with a specified process.”
II. Process and Procedure to Respond to Verifiable Consumer Requests

Under the CCPA, consumers can request various information regarding the collection, sale, and disclosure of their PI and request that a business delete their PI. PI is defined 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, among other things, the following “if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household”:

- identifiers, commercial information, biometric information, Internet or other electronic network activity information, geolocation data, audio, electronic, visual, thermal or olfactory information, professional or employment-related information, education information, and even inferences drawn from PI to create consumer profiles. See 1798.140(o).

The CCPA definition of PI is broad, and it expands the universe of data subject to the Act even further beyond what is defined by the General Data Protection Regulation ("GDPR"). GDPR defines “personal data” as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” Regulation (EU) 2016/679, Article 4(1). This is compounded by the circular and unhelpful definition of “Verifiable consumer request”: “a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, … to be the consumer about whom the business has collected [PI].” 1798.140(y).

As such, we anticipate that development and implementation of a process to identify the relevant data elements, track how they have been handled, accept, process, and respond to consumer information requests in a timely manner will be quite burdensome.

a. Submission of Verifiable Consumer Requests

The CCPA requires companies to provide two or more designated methods for submitting requests for information, including, at a minimum, a toll-free telephone number and a web site address. See 1798.130(a) (1).

---

5 “A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.” 1798.140(y).

6 This particular phrase was inserted by SB 1121.

7 Section 1798.100 describes the right of consumers to request that companies disclose the categories and specific pieces of PI the company has collected about them. See 1798.100(a). However, the provision is redundant in that the ability to request such information is covered in Sections 1798.110 and 1798.115, and provisions that relate to the information requests usually reference only 1798.110 and 1798.115. It is therefore ambiguous whether the CA legislature considers 1798.100 to be a separate type of request. For purposes of clarity, we are not treating the provision as a separate type of request.

8 “Designated methods for submitting requests” means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or
b. Responding to Verifiable Consumer Requests

Any PI collected from a consumer in connection with verifying a consumer’s request may be used solely for the purposes of verification. See 1798.130(a)(7). However, a company does not need to retain PI collected for a single, one-time transaction or to re-identify or otherwise link any data that is not maintained in a manner that would be considered PI in order to comply with verifiable consumer requests if the company does not already do so in the ordinary course of business. See 1798.100(e); 1798.110(d). For purposes of responding to verifiable consumer requests, categories of PI refer to the enumerated category or categories of PI under the CCPA that most closely describes the PI. See 1798.130(c). Further, all responses must cover the requested information pertaining to the 12-month period preceding receipt of the request. See 1798.130(a)(2).

The Act requires that companies must disclose and deliver to the consumer the requested information free of charge within 45 days. The disclosure must be in writing and delivered through the consumer’s account with the company, if applicable, (although companies cannot require a consumer to create an account to make a verifiable request) or otherwise “by mail or electronically at the consumer’s option in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.” 1798.130(a)(2).

The time period to respond to a verifiable consumer request may be extended by 45 days if reasonably necessary upon notice to the consumer within the first 45 days and up to 90 days depending on the complexity and number of requests if the consumer is informed of the reasons for delay. See 1798.130(a)(2); 1798.145(g)(1). In the event a company does not take action on a request, the company must notify the consumer of the reasons for not taking action and any rights the consumer may have to appeal the decision. See 1798.145(g)(2).

In some cases, companies may refuse to take action or may charge a reasonable fee where requests are manifestly unfounded or excessive. See 1798.145(g)(3). Additionally, companies are not obligated to provide information to the same consumer more than twice in a 12-month period. See 1798.130(b); 1798.100(d).

c. Collection Information Requests Pursuant to § 1798.110

If a company collects a consumer’s PI, the consumer has a right to request that the company disclose:

- The categories of PI it has collected about that consumer;
- The categories of sources from which the PI is collected;
- The business or commercial purpose collecting or selling PI;
- The consumer's right to request information and the processes that businesses must follow when they receive such a request.

(End of Excerpt)
• The categories of third parties with whom the business shares PI; and
• The specific pieces of PI it has collected about that consumer.
See 1798.110(a).

To comply, a company must identify the consumer by associating the information provided by the consumer in the verifiable request to any PI previously collected and identify by category or categories the PI collected about the consumer in the preceding 12 months. See 1798.130(a)(3).

d. Sale/Disclosure Information Requests Pursuant to § 1798.115

If a company sells\textsuperscript{11} a consumer’s PI or discloses it for a business purpose, the consumer has the right to request that the company disclose:

• The categories of PI that the company collected about the consumer;
• The categories of PI that the company sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold; and
• The categories of PI that the company disclosed about the consumer for a business purpose.
See 1798.115(a).

To comply, companies must:

• Identify the consumer and associate the information provided by the consumer in the verifiable request to any PI previously collected about the consumer;
• Disclose in a list:
  o The category or categories of consumer’s PI that the company sold in the preceding 12 months; and
  o The categories of third parties to whom the consumer’s PI was sold in the preceding 12 months; and
• Disclose in a separate list
  o The category or categories of consumer’s PI that the business disclosed for a business purpose in the preceding 12 months; and
  o The categories of third parties to whom the consumer’s PI was disclosed for a business purpose in the preceding 12 months.
See 1798.130(a)(4).

e. Deletion Requests Pursuant to § 1798.105

A consumer also has the right to request that companies delete any PI about the consumer that they have collected. See 1798.105(a). To comply, a company must delete the consumer’s PI from its records and effecting, directly or indirectly, a commercial transaction. “Commercial purposes” do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism. See 1798.140(f).

\textsuperscript{11}“Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s PI by the business to another business or a third party for monetary or other valuable consideration. See 1798.140(t).
direct any service providers to do the same. See 1798.105(c). The CCPA does not require companies to comply with a deletion request if maintaining the consumer’s PI is necessary to:

- Complete the transaction for which the PI was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business’s ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- 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;
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business;
- Comply with a legal obligation; or
- Otherwise use the consumer’s PI, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

See 1798.105(d).

III. Implementing Opt-In/Opt-Outs Regarding Sale of PI

a. Provide Opt-Out of Selling PI Through “Do Not Sell My Personal Information” Link on Internet Homepage or California-Specific Homepage

A consumer has the right to “opt out” at any time of allowing a company to sell his or her PI. See 1798.120(a). A company is prohibited from selling an adult consumer’s PI once it has received direction from the consumer to stop. For minors (defined by the statute as 16 and under) affirmative opt-in consent must be obtained. See 1798.120(d);\(^\text{12}\) 1798.135(a)(4). The company must respect an adult consumer’s

\(^{12}\) In the original CCPA, this was 1798.120(c); pursuant to SB 1121, it is now 1798.120(d).
decision to opt out for at least 12 months before requesting the consumer authorize the sale of the consumer’s PI. *See* 1798.135(a)(5).

To accommodate the right to opt out of selling PI, the Act requires that a company must provide a clear conspicuous link on its homepage\(^{13}\) titled “Do Not Sell My Personal Information”. This link must direct the consumer to a page that enables a consumer or authorized person to opt out of the sale of the consumer’s PI, and the Act does not permit companies to require that a consumer create an account in order to opt out. *See* 1798.135(a)(1); *see also* 1798.135(c) (consumers can authorize others to opt out on their behalf pursuant to regulations adopted by the Attorney General).

As an alternative, a company may maintain a separate and additional homepage dedicated to California consumers that includes the required links and text and take reasonable steps to ensure that California consumers are directed to it. *See* 1798.135(b). In either case, any PI collected from a consumer in connection with submitting an opt-out request must be used only for the purposes of complying with the request. *See* 1798.135(a)(6).

b. **Provide Notice of Third Party Resale of PI**

Similarly, in the context of third parties reselling a consumer’s PI, companies must ensure that all consumers receive explicit notice of third-party resale and were previously provided with the opportunity to exercise their right to opt out of the sale of their PI as detailed above. *See* 1798.115(d).

c. **Require Opt-In to Sell PI of Consumers Under 16**

The Act prohibits the sale of a consumer’s PI where the company has actual knowledge that the consumer is less than 16 years of age, unless a minor between 13 and 16 years or the minor’s parent or guardian affirmatively authorizes the sale of the minor’s PI. *See* 1798.120(d). However, this requirement may not even provide companies with valid legal consent if a company were to rely on the opt-in consent of a minor between 13 and 16 years old. We generally recommend that if it is part of a company’s strategy to sell minors’ data, such company should require opt-in consent for any consumer who is 16 years or younger.

IV. **Require Opt-In to Financial Incentive Programs**

The CCPA has anti-discrimination provisions that prohibit companies from discriminating against a consumer for exercising these new rights. Specifically, companies cannot deny, charge different prices or rates for (including discounts or other benefits or imposing penalties), or provide a different level or quality of goods or services in retaliation. *See* 1798.125(a)(1).

---

\(^{13}\) Under the CCPA, “homepage” means the introductory page of an Internet Web site and any Internet Web page where PI is collected. In the case of an online service, such as a mobile application, homepage means the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.
However, the Act provides an exception in situations where charging a consumer a different price or rate or providing a different level of quality is “reasonably related to the value provided to the consumer by the consumer’s data.” See 1798.125(a)(2); 1798.125(b)(1) (redundant provision that instead uses the term “directly related”).

To that end, a company may offer financial incentives (such as compensating consumers for the collection, sale, or deletion of PI) as long as they are not unjust, unreasonable, coercive, or usurious in nature. See 1798.125(b)(4). To enter a consumer into a financial incentive program, the company must obtain prior opt-in consent that is revocable at any time after notice that clearly describes the material terms of the program. See 1798.125(b)(3).

V. Train Employees in CCPA Compliance

The Act requires companies to ensure that all individuals responsible for handling consumer inquiries about the company’s privacy practices or compliance are informed of the requirements and how to direct consumers to exercise their rights. See 1798.130(a)(6); 1798.135(a)(3).

CONCLUSION

As described above, putting in place a CCPA compliance program may be challenging and will require careful consideration of the company’s data collection and management processes. While the date to comply with the CCPA is January 1, 2020 and additional amendments are possible, implementation of compliance measures is likely to require a significant amount of time and resources. As such, a proactive approach will serve to lessen the burden of compliance in advance of the deadline. Please contact a member of our dedicated CCPA compliance team included in Exhibit C with questions.
EXHIBIT A

CONDENSED REFERENCE OF KEY COMPLIANCE MEASURES

1. Verifiable Consumer Request Process
   a. Identify and locate consumer PI
   b. Adopt verification method
   c. Implement two intake mechanisms: toll free telephone number and web address
   d. Develop process for Collection Information Requests
   e. Develop process for Sale/Disclosure Information Requests
   f. Develop process for Deletion Requests
   g. Note there 45 days to respond
   h. Put in place mechanism to request additional 45 days

2. Opt-Out/Opt-In Process
   a. Provide link on Homepage – “Do Not Sell My Personal Information”
      i. Must be clear and conspicuous
      ii. Website with opt-out form linked to process
   b. Develop opt-in process for minors
   c. Address third-party resale
   d. Develop opt-in process for Financial Incentive Program (if necessary)

3. Customer Notifications and Disclosures
   a. Include description of all customer rights
   b. Link to “Do Not Sell My Personal Information”

4. Evaluate whether Financial Incentive Program is needed

5. Employee Training Program
EXHIBIT B

SAMPLE QUESTIONNAIRE FOR ASSESSMENT OF PI AT COMPANY

1. What kinds of services does the company offer?

2. What is the geographic scope of the company?

3. What categories of personal data or information (the “PI”) is the company collecting and/or processing (e.g., names, financial data, IP addresses, etc.)?

4. Whose PI is the company collecting and/or processing (e.g., end users, consumers, etc.)?
   a. Does the company know the physical location of these individuals? If so, how does the company know?
   b. If physical location information is available, what are the implicated locations?

5. What is the source of the PI? (e.g., third-party vendors, company’s website, etc.)? And, how is the PI collected (e.g., monitoring website behavior)?

6. Where is the source of the PI located (e.g., locations of third-party vendors, etc.)?

7. What is the company’s purpose for collecting and/or processing the PI?
   a. Does the company only process the PI for its customers as a support function in order to enable the delivery of services and/or goods to those customers?
   b. Does the company use the PI for analytics (e.g., marketing)?
   c. Does the company use the PI for other business purposes? If so, which?

8. How is the PI processed?

9. Where is the PI stored? How is it secured?

10. Are there systems, applications, or other locations (shared drives/home drives, SharePoint, cloud storage, etc.) that the company uses to access or process the data? If so, what are they?

11. Are employees able to access and/or store the PI locally on their laptops, work stations, or mobile devices? If so, which employees?
   a. Are the laptops, work stations, or mobile devices encrypted?
   b. What is the default saving setting on laptops, work stations, or mobile devices?

12. Would any of the PI be in email systems (e.g., are there any restrictions on what kinds of data can be emailed)?

13. Does the company utilize a backup system? If so, how often is data backed up?

14. Does the company transfer the PI to any third parties? Does the company store the PI with any third parties? Are there any agreements in place with such third parties?

15. Does the company sell or otherwise monetize the PI?
1. **What did regulators do during GDPR year one?**
   - The first year of GDPR saw regulators take a relatively relaxed approach towards enforcement. They focused on staffing their offices, building GDPR awareness among the public, and initiating investigations. We expect the next 12 months will see many of these investigations conclude with significant penalties and decisions that provide instructive precedents.
   - The CNIL fine of €50 million against Google was a massive outlier in terms of how regulators enforced GDPR during its first year. By comparison, the average GDPR enforcement fine in Germany, a conservative enforcement jurisdiction, has been just under €6,000 (across 81 cases).

2. **What are regulators saying?**
   - Regulators are very clear that they are not just focusing on large technology or social media companies. The chairperson of the European Data Protection Board has specifically stated that regulators are interested in any company that processes personal data: “the more data you’re collecting, the more data you’re using, the more concerned I am, and the more careful you should be”.
   - Elizabeth Denham, UK Information Commissioner, has stated that businesses want to see “from regulators sanctions, fines, real cases that interpret the law”. Helen Dixon, Irish Data Protection Commissioner has stated that she wants “all the cases [she] conclude[s] to be of precedential value to data controllers. The only way to raise data protection standards is to make it clear to companies what the objection to specific practices are…”
   - Regulators have cautioned that in-depth GDPR investigations take time. They cannot be completed in less than six months. We are about to enter the phase where significant GDPR investigations start to conclude.

3. **What predictions can we make for GDPR year two?**
   - Many companies will continue to struggle with privacy fatigue. The conversation has moved on from GDPR and towards CCPA and the pending ePrivacy regulation. This is often the case even where companies’ GDPR compliance projects have significant gaps.
GDPR year two – **Enforcement primer**

- **Significant enforcement actions are coming** (look at the ICO’s announcement that it intends, as lead supervisory authority, to fine British Airways £184 million and Marriott £99 million). Initial fines may tend to focus on tech giants but any company that processes personal data should carefully read regulators’ judgments. They will provide valuable guidance about how regulators expect companies to process personal data.

- **Your company is not immune just because it isn’t Google.** Some companies think that they are less likely to be investigated by a regulator because they are not technology companies. This is dangerous. Regulators primarily care about companies that process personal data as a core part of their business.

- **Do not expect GDPR sanctions to be harmonised (or always logical).** The EU is 28 separate countries with 44 separate privacy regulators (28 national regulators plus Germany’s 16 regional privacy regulators). The European Data Protection Board can attempt to standardise interpretation, but each regulator will have its own priorities and enforcement agenda.

- **GDPR year two is all about ongoing compliance.** GDPR compliance is iterative, collaborative, ongoing and never static. The lead up to GDPR was all about massive compliance projects. GDPR year one was about operationalising new policies and procedures. The coming year will be about ensuring that a culture of privacy and data protection beds down within companies. Mistakes will be made and weaknesses identified. A mature company will learn from these. They will also look behind headline-grabbing regulatory enforcement decisions to understand how they can leverage the regulatory guidance contained within such decisions.