Understand data protection with

epiq guidance

People. Partnership. Performance.

Introduction

Both individual and business data usage is rapidly increasing every day due to societal reliance on technology, as well as new and emerging data trends. This, and the recent implementation of the General Data Protection Regulation (GDPR), has caused a shift in thinking – there is more and more pressure to prioritize data protection than ever before. As a result, new and amended data security laws have recently surfaced in the United States. California is by far the leading state in the area of consumer privacy, with 2018 being the state's most progressive year yet. Last year, California passed two new pieces of legislation specifically dealing with consumer privacy and data security standards. The state also introduced a bill in early 2019 seeking to amend its data breach notification statute in order to address gaps in the law. Some states have already followed suit and begun discussing, amending, or drafting similar laws. However, it is still uncertain if or when legislators will enact a comprehensive federal privacy law. Legal practitioners in California, other states, and worldwide should remain updated on future developments and enforcement related to California's data privacy laws which go into effect January 1, 2020. California practitioners must also stay educated about any ethical obligations attorneys have regarding data security.

Overview of California's current data security laws

Below is a summary of the data security laws in California as they currently stand. Whether dealing with new or amended laws, the focus is protecting individual privacy in the digital sphere, which inevitably increases an organization's obligations and potential liability. Be aware that these laws are constantly evolving to account for new changes in technology and practice habits. Additionally, each law has specific enforcement mechanisms, including interpretation and compliance monitoring by the attorney general and different degrees of court intervention. Being educated on the main tenets of each law, compliance requirements, and enforcement power is crucial.

California Consumer Privacy Act: the bills

The most groundbreaking piece of data security legislation is definitely the California Consumer Privacy Act (CCPA). In June 2018, the California legislature enacted the CCPA which is the broadest data privacy law in the country and resembles many aspects of the European Union's GDPR. The issue of unprotected consumer data continues to become more prevalent globally as the volume of digital data increases. This is especially true with big tech companies that handle large amounts of data.

Without regulation, these organizations have the power to collect and disseminate private consumer information for essentially any purpose.

The CCPA provides consumers access and control over their personal information[1] and allows them to have a say in how organizations collect, use, and disseminate this data. Some key features include:

- Consumers will have direct access to their data and can request information about how and why organizations use their personal information
- Consumers have the right to delete and modify their personal data. Organizations must comply with data deletion requests (unless an exception applies).
- Consumers have the right to opt out of sales involving their personal information.
- Organizations must notify consumers when they collect personal information and when their personal data is compromised in a security breach.
- The attorney general has the power to enforce the CCPA's provisions. The attorney general also has rulemaking authority and is supposed to provide compliance guidance to businesses.
- Individuals can only seek relief in civil court if a breach occurs due to an organization's failure to have a comprehensive data security program in place that reasonably safeguards certain private information.
- Organizations are generally prohibited from charging a fee to consumers just for requesting information under the CCPA.

This law was quickly passed and is scheduled to become active in 2020. The original approved text was immediately met with opposition from both sides due to unclear language and exemptions. Big tech organizations have also scrutinized the CCPA because they want to limit consumer control. Many social media and other big tech organizations use consumer data to drive their advertisements and overall revenue, while also allowing free website usage. As such, many of these organizations have lobbied for amendments to California's law and for the creation of a less restrictive federal privacy law.

In response, lawmakers have been working vigorously to clean up the language and reach compromise on the disputed provisions before the law becomes active. This is tough because while the CCPA promotes a trend towards consumer openness and control, some want to stray away from the intent of the law by limiting consumer control. Below are some critical proposed amendments to the CCPA that are currently pending. All of these bills passed through the California Assembly, and have moved to the California Senate, where they need to pass by Sept. 13, 2019 in order to go before the state governor. The governor then must then decide whether to sign these bills into law by Oct. 3, 2019:

- Modifying the defenition of personal information to exclude data collection from job applicants, employees, contractors, or agents.[2] On July 10, 2019, the Senate judiciary committee amended and passed this bill to only require employers to disclose the type of data and reason for collection. Specific details regarding the data is exempt from disclosure. However, there is a time

[1] The statute currently defines "personal information" as information that is not publicly available and identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. While the list is long, some examples of this include: name, postal address, email, social security number, driver's license number, passport number, biometric information, geolocation data, professional or employment-related information, and Internet browsing history. CCPA, Section 1798.140(o)

[2] AB-25 California Consumer Privacy Act of 2018

limit on this bill until January 2021 so lawmakers can fine-tune the section regarding employee data collection. This bill was referred to the Senate appropriations committee.

- Defining the "publicly available" exception contained in the definition of personal information as lawful data from federal, state, or other local government records.[3] On July 10, 2019, the Senate judiciary committee passed this bill and referred it to the Senate appropriations committee.
- Adding exemption to the law for information disclosure resulting from compliance with government requests.[4]
- Adding exemption to the law for selling information in order to detect security breaches or fraud.[5]
- Adding exemption to the law for vehicle information used in relation to warranties or recall repairs.[6] On July 10, 2019, the Senate judiciary committee passed this bill and referred it to the Senate appropriations committee.
- Adding exemption to the law for insurance organizations in certain situations.[7]
- Prohibiting organizations from selling personal data to third-parties that they collected from loyalty programs.[8] On July 11, 2019, the Senate judiciary committee passed this bill and referred it to the Senate appropriations committee.

Legal professionals and interested organizations should be aware that this amendment list is not exhaustive and there are likely to be more proposed changes both before and after the

[3] AB-874 California Consumer Privacy Act of 2018

[4] AB-1416 California Consumer Privacy Act of 2018. According to the California legislature website, they cancelled the July 9, 2019 hearing on this matter. This likely means that the bill will not move forward.

[5] *Id.*

[6] AB-1146 California Consumer Privacy Act of 2018

[7] AB-981 California Consumer Privacy Act of 2018

[8] AB-846, California Consumer Privacy Act of 2018

CCPA's enactment. Assembly Bill 873 also made it into the Senate, but lawmakers rejected at its first hearing on July, 9, 2019. There was a heavy debate about how the bill would alter the definition of deidentified data, which is data not covered under the CCPA. The bill proposed changing the definition of deidentified data to "information that does not identify, and is not reasonably linkable, directly or indirectly, to a particular consumer, provided that the business makes no attempt to reidentify the information and takes reasonable technical and administrative measures designed to ensure that the data is deidentified, publicly commits to maintain and use the data in a deidentified form, and contractually prohibits recipients of the data from trying to reidentify it." When responding to a consumer request, an organization would not be required to reidentify data not maintained as personal information.[9] The bill also would have narrowed the definition of personal information. If passed, this would have been favorable to corporations because they could use this provision to limit disclosure requirements under the CCPA. Privacy advocates maintain that this strays away form the intent of the law. While lawmakers allowed for reconsideration of this bill, it probably will not gain enough traction to move forward.

Additionally, the legislature has already outright rejected several proposed amendments. Most notably was Senate Bill 561, which aimed to provide consumers with a broad and unrestricted right to file private lawsuits for any CCPA violation. The attorney general's office spearheaded this bill to attempt to shift some of the enforcement burden off the attorney general by providing a broader right to file private actions. This bill also aimed to remove the CCPA section requiring the attorney general's office to issue compliance opinions. If this bill passed, California courts would surely have seen an incredibly high number of class action lawsuits that would have overwhelmed judges and businesses, while also pulling focus from the CCPA's main goals and function.

California Consumer Privacy Act: the future

With a law that was rushed into drafting and that has the potential to affect several individuals and organizations, legal practitioners in California can expect to see more proposed changes to the CCPA before and after it becomes active. For example, one question is whether the law will actually become effective in 2020 as planned. While there has been no evidence to the contrary, lawyers should keep up to date on any new amendments that could influence the active date. A creation of a federal privacy law could also preempt the state law. However, enactment of a comprehensive federal privacy law in 2019 is not currently looking promising. Regardless of the final text, the CCPA will greatly affect organizations that handle California citizens' personal information on a regular basis. However, some of the passed amendments will limit the CCPA's reach and decrease potential violations. For example, the job applicant exemption under AB-25 would take many organizations out of the CCPA's reach.

Consumers and businesses will undoubtedly challenge the law's boundaries after it becomes effective. The attorney general's office will play a critical role in determining the CCPA's reach through compliance opinions, rules, and decisions regarding alleged violations. The attorney general's office will likely face a myriad of issues, including those contained in the rejected bills or regarding inconsistencies within the CCPA itself, as well as with other California statutes. The courts will also see challenges regarding the right to file a civil action for security breaches resulting from an organization's insufficient safeguards. When are these private

[9] AB-873 California Consumer Privacy Act of 2018

lawsuits appropriate? What factors need to be present in order to have a comprehensive data security program that reasonably safeguards private consumer information? It is likely that courts will try to limit these disputes as much as possible to avoid opening the floodgates and keep enforcement primarily with the attorney general. However, any new bills that broaden or limit enforcement mechanisms under the CCPA may affect the availability of civil relief for consumers.

Internet of things

Another new 2018 law deals with the security of connected devices, making California the first state to directly regulate the Internet of Things (IoT) as a whole. This has been a highly complicated and debated topic for years, which is why there has not been any state or federal laws enacted until now. In simple terms, IoT generally refers to any devices that are connected to a network that can share and analyze data. Basically, if a device or component of a device can connect over Wi-Fi and share information with people or other devices, it will be considered to be part of the IoT universe. Examples include smartphones, activity trackers, doorbell/camera systems, and smart medical devices.

There are many positive aspects of IoT, including universal connectivity and integration, speed, and data insight that can improve our way of living. However, allowing connection of such a large variety of devices over the internet inherently has several security risks. If these devices are not equipped with sufficient features, they are vulnerable and appealing to hackers. Depending on the device, hackers may be able to gain access to very personal data, such as voice conversations or video footage. With such vulnerability, consumers probably assume that these devices are equipped with top-notch security components. This is unfortunately not the case. When discussing the IoT bill, the California legislature pointed out how the state's booming economy and large number of consumers puts it at an increased risk for cyber attacks. The legislature considered the following incident:

> *Security researchers have found that an Internet connected doll called the 'My Friend Cayla Doll' has a security flaw that allows strangers to speak directly to children via the doll from up to 50 feet away, including through walls into a child's bedroom. For years there have been reports of strangers similarly talking to children through insecure baby monitors. Researchers have also concluded that thousands of insecure web cameras made by Chinese electronics firm Xiongmai were taken over by hackers and turned into a 'botnet' army that attacked and disabled major websites including those of Twitter, Spotify,*

New York Times, and Airbnb in 2016. The lack of basic security features on internet connected devices undermines the privacy and security of California's consumers, and allows hackers to turn everyday consumer electronics into cyber weapons.[10]

A 2017 report from the Department of Justice also noted that after a hacker installs malware on an IoT device, it can spread fast to other connected devices on the network. The frightening thing is that this can be triggered when a user simply turns on a device.[11] California's IoT law, which will also become effective on Jan. 1, 2020, seeks to remedy these issues and make it harder for hackers to gain access to a device in the first place. The statute will require any manufacturers selling connected devices in the state to install reasonable security features on these devices that are "appropriate to the nature and function of the device; appropriate to the information it may collect, contain, or transmit; and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."[12] Connected devices include "any device, or other physical object that is capable of connecting to the internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address."[13]

However, the following exclusions apply:

- Devices subject to federal law, regulations, or agency guidance
- Any person or entity seeking information from a device pursuant to HIPAA or California's Confidentiality of Medical Information Act
- Law enforcement agencies that are legally requesting data
- Manufacturers of unaffiliated third-party software and applications the user downloads
- Electronic store, gateway, and marketplace providers[14]

While the law does not contain a definition for "reasonable" security features, it does offer some helpful guidance and examples. If the manufacturer installs preprogrammed passwords on the device or requires that first-time users provide authentication to gain access to the device, they meet the reasonableness standard.[15] Some other security components that would likely meet this standard are things like fingerprint entry and facial recognition. Additionally, a manufacturer's responsibilities terminate after selling the device. This means that if the device user modifies it in any way, the manufacturer cannot be liable for any security issues that occur as a result if the device initially had reasonable security features from manufacturer installation.[16] Only the state can enforce any violations of this law because it specifies that there is no private right of action available for consumers.[17]

Unlike the CCPA, this law has no proposed amendments yet. However, it has received mixed

---

[10] SB 327, Senate Third Reading p. 4 (Aug. 24, 2018)

[11] U.S. DOJ Cybersecurity Unit, Securing Your "Internet of Things" Devices (Jul. 2017)

[12] Security of Connected Devices, Section 1798.91.04(a)

[13] Security of Connected Devices, Section 1798.91.05(b)

[14] Security of Connected Devices, Section 1798.91.06

[15] Security of Connected Devices, Section 1798.91.04(b)

[16] Security of Connected Devices, Section 1798.91.06(c)

[17] Security of Connected Devices, Section 1798.91.06(e)

feedback so expect to see some proposed changes or enforcement challenges in the future. The positive attributes of this law are that devices will be more secure at the outset and there is a foreseeable decrease in security breaches. The main issue with the text of the statute center around uncertainty about what types of security features satisfy the law's requirements. Device manufacturers, legal professionals, and consumers need to take note of when the state decides to seek enforcement and how the courts interpret the law. This will provide further guidance on what types of security features manufacturers need to install in order to be compliant, which will likely depend on the type of device and information that users store on it. Future challenges will also determine what penalties manufactures should expect after a violation, which may include a combination of injunctive relief and fines. Regardless, manufacturers should start implementing tighter security features in order to achieve compliance.

It will be interesting to see if any federal IoT bills will finally make it into law and how this would affect California's legislation. Additionally, this statute may also start a chain reaction in other states to pass their own dedicated IoT laws. It will likely cause a trend of manufacturers equipping all their devices with the same features, even if sold outside of California, to save costs and achieve device uniformity.

Data breach notification

California's data breach notification statute has been around for a while. It requires organizations to alert individuals after certain categories of data fall victim to a breach. However, the law is outdated and currently contains gaps that do not account for types of personal data that hackers commonly target and how new technologies influence data breaches. The legislature is currently analyzing California Assembly Bill 1130, which was introduced on Feb. 21, 2019, to amend the law. As it stands, the statute covers several categories of personal information, such as social security numbers, driver's license numbers, and health data. If enacted, the bill would add other government-issued identification numbers (like passports) and biometric data (like fingerprints) to this list. As of May 30, 2019, this bill moved to the Senate for review.

Including other forms of IDs, like passports, helps ensure consumer notification when important personal information is compromised. Many people use their passports in addition to or in lieu of driver's licenses/state ID cards in situations that require identification. The same goes for biometrics. Organizations are using biometric data more frequently as technology continues to evolve. As such, there are many positive aspects of this bill, such as making California one of the top states regarding consumer data breach notification protection and

stopping organizations from avoiding disclosure of data breaches.

However, there are concerns surrounding the bill. One issue is the broad category of "government-issued identification numbers." Critics want the amendment to specifically list what falls under this category so the statute will not include IDs that carry no risk value.[18] Another issue deals with determining when a biometric data notification is necessary. As it stands, the definition is "unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data." Some believe that the "other" category could include many different things that are irrelevant to data breaches.[19]

Lastly, some believe that this amendment will interact with the CCPA in the following ways:

- **Increasing civil suits**: By expanding the definition of personal information under the data breach notification law, more organizations will be liable and consumer litigation could potentially increase under the CCPA since consumers have the right to sue when their personal information is breached due to an organization's failure to have a comprehensive data security program in place that reasonably safeguards data.[20]
- **Conflicting biometric data definitions**: The CCPA includes both physical characteristics and behavior under its biometric data definition, while the amendment to the data breach notification statute appears only to apply to physical characteristics. This could cause future enforcement problems.[21]
- **Increasing costs**: The combined costs under the data breach notification law and CCPA can add up quickly. Organizations that fail to safeguard data and experience a breach will face costs associated with data breach notification, litigation under the CCPA, and improving security to successfully achieve future compliance.[22]

Legal professionals, consumers, and affected organizations should continue to monitor this bill to see if the amendment passes and if any tweaks are made to it based on the above concerns.

Ethical considerations in practice

The California State Bar has addressed several ways data security is crucial in legal practice. For example, the bar analyzed how to fulfill competency and confidentiality duties when using technology to transmit or store confidential client information if third-parties can gain unauthorized access to such technology. This could include using the cloud or conducting business over a Wi-Fi network out of the office. The opinion concluded that attorneys must act appropriately to prevent the risk of unauthorized disclosure. Additionally, "because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the

[18] AB 1130, California Assembly Committee on Privacy and Consumer Protection, p. 4 (March 26, 2019)

[19] Id. at 6

[20] AB 1130, California Assembly Committee on Privacy and Consumer Protection, p. 6 (March 26, 2019)

[21] Id.

[22] Jackson Lewis P.C. "California AG Seeks To Further Amend State's Data Breach Notification Law," JD Supra, p. 1-2 (Feb. 22, 2019)

efficacy of such steps."[23] Since technology is constantly changing and hackers are everywhere, the obligation to monitor and research appropriate security measures is ongoing.[24]

Attorneys should evaluate the following factors before employing a certain type of technology:

1. the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security;
2. the legal ramifications to a third-party who intercepts, accesses or exceeds authorized use of the electronic information;
3. the degree of sensitivity of the information;
4. the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product;
5. the urgency of the situation; and
6. the client's instructions and circumstances, such as access by others to the client's devices and communications.[25]

Balancing all of these factors will help determine whether the risk of using a certain technology is worth it and generally fulfill the ethical obligations of competency and confidentiality.

The committee generally advised against conducting business over public Wi-Fi (like at a coffee shop) unless the attorney takes extra steps to secure client data when conducting business. This includes encrypting files or using a virtual private network. Working at home is generally fine because the Wi-Fi is, more likely than not, secure. If an attorney does not have secure connection at home, the same responsibilities would be present as if they were conducting business over a public Wi-Fi network.[26]

The bar also issued an opinion on how to remain ethical while operating a virtual law office ("VLO") in the cloud. While the general duties of competence and confidentiality apply and attorneys do not have any extra ethical duties when operating a VLO, attorneys will need to take additional steps to meet these requirements due to the exclusively technology-based nature of this type of practice.[27] VLO attorneys must ensure that their vendor acts appropriately to satisfy client confidentiality, which would include having a data security system that would safeguard client data and communications. The committee further noted: "If Attorney lacks the necessary competence to assess the security of the technology, she must seek additional information, or consult with someone who possesses the necessary knowledge, such as an information technology consultant. (Rule 3-110(C); Cal. State Bar Formal Opn. No. 2010-179.) Only after Attorney takes these reasonable steps to understand the basic technology available and how it will work in this hypothetical VLO, and determines that her duty of confidentiality and competence can be met in the contemplated VLO, may Attorney proceed."[28]

It is also important to remember that security standards will change as technology evolves. Additionally, attorneys must be aware of where client

[23] State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179, p. 7 (2010)

[24] Id. at 1

[25] Id.

[26] State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179, p. 7 (2010)

[27] State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2012-184, p. 7 (May 23, 2012)

[28] Id. at 3

data will be transmitted in the cloud. The committee advised: "When selecting and contracting with her VLO vendor, Attorney should address and minimize exposure of the client to legal issues triggered by both the international movement, and/or storage, of information in the cloud, and the potential subcontracting out of the vendor's services to unknown third-party vendors, which may impact confidentiality, without the prior written consent of Attorney and affected clients."[29] As always, attorneys must supervise all of the individuals working with them in the VLO to ensure they are keeping data secure and meeting all ethical duties.[30]

Conclusion

Because of data's overwhelming presence in the legal practice and basically every aspect of the world today, lawyers must make data security a top priority. The three laws discussed in this white paper reflect new and amended California statutes that solely focus on data security as a response to the global reliance on data. However, legal practitioners should be aware that this is not a comprehensive list of all laws that touch on data security. Other California statutes also address this issue and include data security as a component, such as the state's HIPAA laws. However, it is important to remember that these laws are constantly changing in order to adapt to new technology usage and data trends. Attorneys should continue to monitor data laws, compliance opinions, new ethics opinions, and court decisions. Also keep an eye out for any trends among state legislation and steps towards passing a federal data privacy law.

[29] Id. at 4

[30] Id. at 7

Business Process Solutions
Class Action & Mass Tort
eDiscovery
Regulatory & Compliance
Restructuring & Bankruptcy

epiqglobal.com

People. Partnership. Performance.

epiq