Procopio

Maximize Your Cyber-Insurance Coverage

By Carole J. Buckner, Partner and General Counsel

Because cyberattacks are ever increasing, prevention is challenging, and liability to regulators and class action plaintiffs is escalating, cyber-insurance is becoming more prevalent. Annual premiums are expected to increase to $7.5 billion by 2020. Cyber-insurance is a relatively new type of insurance coverage, and increasingly becoming an important risk management tool. One prediction shows the cost of global cybercrime will hit $6 trillion by 2021. As of 2018, another study pegged the average cost of a cyber breach at $369,000.

Unlike other types of insurance, there is more variation in cyber-insurance policies in terms of scope, sub-limits, coverage and exclusions. It is important to understand what is covered by your cyber-insurance policy as well as what may not be covered. In addition, because cyber insurance is a newer line of insurance, insurance carriers may require more detailed information in the application for the policy which may include a technical questionnaire. Once the insurance is in place, if a claim does occur, it is important to tender the matter to the cyber insurance carrier in a timely manner.

Traditional Insurance May Not Cover a Cyber Attack

While many companies depend on comprehensive general liability policies for coverage of losses arising from data breaches, recent legal decisions regarding traditional liability insurance have determined that such policies often do not cover cyber incidents on the grounds that data and information are not tangible, and therefore not covered. Because cyber related claims can arise in class actions, often with significant damages exposure, it is important that a business carefully consider whether or not existing insurance policies provide coverage for cyber incidents.

More and more comprehensive general liability policies now contain an exclusion for cyber related events. One court decided that an exclusion for damages arising out of the loss of

electronic data applied such that a business owner could not recover on the policy for a network hack resulting in stolen credit card information. *RVST Holdings, LLC v. Main St. Am. Assur. Co.,* 136 A.D.3d 1196, 25 N.Y.S.3d 712 (N.Y. App. Div. 2016). As a result, the insurance carrier also had no duty to defend the litigation against the insured.

Another issue is whether a cyber incident involving publication of stolen private information falls within traditional coverage for advertising injury. In one case, the court determined that there was no coverage under a comprehensive general liability policy where third party hackers had stolen and published private information. *Zurich Am. Ins. Co. v. Sony*, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. N.Y. County Feb. 24, 2014). The court held that the theft of the information was not a publication by the insured and therefore not covered.

Understand Your Cyber Policy Coverage

Given the limitations on traditional insurance coverage it is important for businesses to consider obtaining separate coverage for cyber incidents, and to understand that scope of that coverage.

Cyber insurance typically provides first party coverage, which includes loss mitigation as well as incident response and investigation services triggered by the discovery of a security or data privacy incident. First party coverage may also include expenses associated with business interruption and system failure. Such insurance may also cover the costs associated with a ransom payment demanded by a perpetrator.

Third-party coverages typically include liability for defense and compensatory damages associated with regulatory proceedings, as well as privacy liability to third parties and liability for failures of network security and disclosure of otherwise confidential information. This coverage may include legal expenses, and public relations expenses, as well the cost of notifications to consumers.

Cyber-insurance policies also typically provide coverage for network security errors that result in liability of an insured for damages and expenses. Such coverage extends to include actions of rogue employees or third party vendors. Privacy liability coverage addresses

privacy incidents such as unauthorized disclosure of personal information or confidential corporate information.

Coverage for privacy breach expenses usually insures against expenses related to privacy incidents including attorneys, accountants, public relationship consultants and other third parties as well as the costs of forensic analysis necessary to determine the cause of a privacy incident. Some policies provide for reimbursement while others provide for payment on behalf of the insured. This distinction can in turn influence which providers will be used.

Some types of common expenses that an insured will incur after a privacy breach will not within the scope of cyber-insurance coverage, including costs to correct deficiencies and upgrade systems, and salary and overhead expenses of the insured incurred in dealing with the breach. Voluntary payments, such as breach notifications that are not required by law, may also be excluded from coverage.

Cyber extortion coverage is another important part of many cyber insurance policies. Such coverage addresses ransomware incidents, among other cyber-related threats. Such coverage can be triggered by a threatened attack, or by the threatened disclosure of information. Policy provisions vary, with some requiring an immediate and credible threat in order to trigger coverage. Notification to the insurance carrier is critical as policies may require the insurance carrier to provide consent prior to payment of a ransom.

Business interruption loss is also covered by cyber insurance to cover losses incurred during a restoration after a cyber incident. Such policies often narrowly define business interruption income loss related to a business's profitability. Expenses incurred to improve systems are typically excluded from coverage. Cyber policies also cover expenses incurred by insureds in responding to state and federal regulatory authorities following a privacy incident, to include formal investigations, as well as responding to subpoenas.

Some cyber policies assign sub-limits to specific types of coverage. Common exclusions involve criminal, fraudulent and dishonest acts, and payment of fines and penalties. Because cyber-insurers are constantly changing the terms of coverage as they reevaluate risk, businesses must assess their needs against a detailed evaluation of the potential coverage available in the market.

In one case involving a cyber insurance policy, the insured incurred significant expenses in investigating and remediating a cyber breach in which hackers obtained 60,000 credit card numbers and posted them on the Internet. The insured also faced the expense of defending multiple class actions. While the policy covered privacy injury and notification expenses, the exclusion for losses resulting from contractual liability barred the insured's recovery for an additional $2 million to cover fees and charges its credit card service providers charged back to the insured. *P.F. Chang's China Bistro v. Federal Insurance Co.*, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016).

Another pending case involves two ransomware attacks in which the insurance carrier under an all risk policy covering physical loss or damages to electronic data is asserting that the act of war exclusion warrants denial of coverage, on the grounds that the attack involved a hostile or warlike action by a government agent. *Mondelez Intern'l, Inc. v. Zurich American Ins. Co.,* 2018 WL 4941760 (2018). Alleged losses exceed $100 million.

Issues may also arise depending on the cyber-insurance policy definition of what constitutes a claim, with some policies requiring notice of charges, and others providing coverage for informal administrative proceedings.

Provide an Accurate Application/Questionnaire

Rigorous underwriting of cyber insurance applications is now standard practice. Applications for cyber insurance coverage may be more detailed than applications for other types of insurance, and may require that the insured follow specified practices. Applications should be completed in collaboration with the company's technology team, in order to assure accuracy, and to permit the technology team to carry through on appropriate safeguards.

Many applications now involve security questionnaires designed to provide an understanding of the applicant's security posture, but often covering a substantial range of sub-topics including access control, data collection, technical security practices, relationships with service providers, loss history, and organizational policies and procedures.

In one recent case, an insured hospital network suffered a substantial data breach involving patient medical information which was publicly disclosed after unauthorized entry into the

insured's servers. Three regulatory investigations were commenced by state and federal authorities. A class action followed, which the insured ultimately settled for $4.125 million. The insurance carrier funded the settlement, but reserved the right to seek reimbursement of the entire settlement amount from the insured.

The insurance carrier then filed an action for declaratory relief, seeking to deny coverage for all damages, and seeking reimbursement for the $4.125 million paid to settle the matter. The insurer also sought recover of all expenses incurred in responding to the breach, in the amount of $860,000, and defense costs of $168,000. In addition, the insurer sought rescission of the cyber policy on the grounds that the insured failed to follow the minimum practices required in the cyber policy application. At the same time, the insured filed an action in state court, also concerning the coverage dispute.

The carrier asserted that the application contained misrepresentations regarding whether the insured had exercised due diligence, checked and maintained security patches, and replaced default settings to assure information security. As a result, the carrier claimed that the misrepresentations in the application rendered the policy null and void. *Columbia Ca. Co. v. Cottage Health Sys.,* C.D. Cal. No. CV 15-03432 DDP (AGRx) (May 7, 2015). The case was dismissed without prejudice so that the parties could pursue alternative dispute resolution pursuant to the terms of the policy. *Columbia Ca. Co. v. Cottage Health Sys.,* C.D. Cal. No. CV 15-03432 DDP (AGRx) 2015 U.S. Dist. LEXIS 93456 (July 17, 2015).

One lesson is that using outdated security protocols may result in damages while the business may also lose the benefit of cyber-insurance coverage after paying high premiums.

Tender in a Timely Manner

It is critical to make a timely tender to the cyber insurance carrier after a cyber incident. In one reported matter, the insured experienced a cyber-attack that compromised two million credit and debit card numbers. The insured incurred millions of dollars in legal fees, forensic investigation fees, and expenses for TV, radio and newspaper ads. The policy provided coverage for reasonable expenses other than internal corporate costs, incurred with the insurer's prior written consent, and provided that as a condition precedent to coverage,

written notice to the insurer was required at the earliest practicable moment or within 90 days of discovery.

The insurer alleged that it had not provided written consent to the insured to incur the expenses and that the insured had not provided notice within the 90 day period. The cyber insurance carrier claimed that coverage should be denied on the grounds that late notice was provided to the insurance carrier regarding the cyberattack. *Beazley Insurance Co. Inc. v. Schnuck Markets Inc.,* No. 1:13-cv-08083, Compl. 2013 WL 6167107 (S.D.N.Y. Nov. 13, 2013). In the same case, the insurance carrier declined coverage in part because the consent of the insurance carrier was not obtained to the settlement of the dispute involving the cyber breach.

Conclusion

Cyber-insurance provides major risk management benefits for businesses, but coverage varies and it is important to understand what is appropriate for your business. Careful compliance with cyber-insurance policy requirements during the application process and at the time of tender of a potential claim will help avoid later arguments that could defeat coverage on the grounds that the policy is void.

Carole J. Buckner is a Partner and General Counsel at Procopio and a member of its Privacy and Cybersecurity Practice Group. Her practice focuses on legal ethics, professional responsibility and the law of lawyering, including advising lawyers and law firms, and rendering expert opinions. She also serves as an expert consultant on issues involving legal ethics including legal fees, billing, fee arrangements, conflicts of interest, fee sharing, referral fees, unauthorized practice of law, withdrawal from representation, modification of fee arrangements, client trust accounting, and other issues.

BIBLIOGRAPHY

Najiya Budaly, Law360, *Brokers Urged to Be Vigilant for Cyber Insurance Flaws* (May 19, 2019)

2 DATA SEC. & PRIVACY LAW §S 14:6 14:17-14:25 (2018)

Daniel Garrie and Peter Rosen, Law360, *'Act of War' Questions in Cyberattack Insurance Case* (April 23, 2019)

Benjamin Horney, LAW360, *Insurer Says Policy Doesn't Cover Grocery's Data Leak Claim* (Nov. 15, 2013)

1 INSURANCE COVERAGE FOR IP CLAIMS, §§ 5.18, 5.21 (2019)

James McQuaid, et al., *Meeting the New Challenges of Cyber Insurance Coverage: Think You're Covered? Think Again,* ALI-CLE (2018)

Sahsa Romanosky, et al., *Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?* Journal of Cyber Security (2019)

Jill D. Rhodes and Robert S. Litt, THE ABA CYBERSECURITY HANDBOOK, (2d ed. 2018).

Minjhquang N. Trang, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches,* 18:1 Minn. J. L. Sci. & Tech 299 (2017)

David L. Vicevich, *The Case for a Federal Cyber Insurance Program,* 92:2 Neb. Law R. 555 (2018)

Procopio

Top Cyber Safety Tips for Employees

By: Elaine F. Harwell, CIPP/US

Every business employee should know and understand that they are on the front lines of information security. As a company, you may have cutting-edge security software, but unless your employees stay on guard to help assure company assets and data are safe and secure, cyber risks will persist. Educate your employees on the small things that contribute to cybersecurity and emphasize the importance of cybersecurity within your organization starting with these quick tips:

1. Utilize Strong Passwords: Use a strong mix of characters or a long passphrase or sentence. Do not use the same password for multiple sites and avoid using information that is easily discovered (including information on your social media sites, e.g., birthdays, children's or pets' names, or your favorite hobbies). Do not share your password and certainly do not write it on a post-it note stuck to your computer monitor. Do consider using a password manager like LastPass, Keeper, or Dashlane.

2. Think Before You Click: Do not immediately trust links provided within email messages, PDFs, or search engine results, even if you think you recognize the sender or source. If you become suspicious or have second thoughts, do not click on the link. Pick up the phone to confirm requests for sensitive information or changes to wire instructions.

3. Lock Your Devices: Before walking away from your desktop computer or other device (for any length of time) lock it up so no one can use it while you are gone. The Windows key, plus "L" is a quick shortcut to lock your computer.

4. Avoid Public WiFi: Public WiFis, at hotels, coffee shops, airports, or anywhere else, are generally unsafe. Unsecured connections can allow others to see important emails or encrypted messages and could also open your device to malicious attacks. If you must work remote, utilize a virtual private network (VPN) or mobile hotspot, if possible. Ensure you have a firewall enabled, update your device with security patches, and make sure you are covered by good anti-malware software.

5. Watch Out for Social Engineering: Social engineering refers to a broad range of malicious activities intended to trick someone into divulging information or falling for a scam, *e.g.*, phishing attacks through email or phone calls. Investigate any requests for personal information, money, or anything of value before turning it over. If it seems to be too good to be true, assume it is.

6. Monitor Your Accounts: Monitor online accounts regularly for any suspicious activity. If you see something unusual or unfamiliar, it could be a sign that you have been compromised.

GENERAL PRIVACY AND DATA PROTECTION ASSESSMENT QUESTIONNAIRE

The purpose of this questionnaire is to highlight the key considerations for organizations regarding data protection and privacy. Data, often one of the most important assets a company has, is exchanged globally at a rapid and large volume. Identifying problems and preventing missteps with sensitive information before they occur should be a top priority for any organization. Conducting an internal review of your organization's privacy and data protection status is an important step to implementing sound policies and for managing emerging risks.

		Complete	N/A
1.	**Are you prepared for a data breach?** Do you and your employees know and understand your obligations when a data breach occurs? Do you have an appropriate incident response plan in place? It is generally accepted data breaches are not an *if* but *when* for businesses operating in today's connected world. One of the most critical aspects of recovering from a data incident is preparing for one well before it occurs. Indeed, meaningful preparation is essential to getting through the incident with minimal business interruption.	☐	☐
2.	**Do you use or collect personal data?** Can you demonstrate compliance with global and local data privacy regulations? For example, if you collect the personal data European citizens or California residents, it is possible data protection laws such as Europe's General Data Protection Regulation (GDPR) or the new California Consumer Privacy Act (CCPA), set to take effect January 1, 2020, may apply to your business. The GDPR and the CCPA provide businesses with a blueprint for handling personal information and significant penalties may apply for noncompliance.	☐	☐
3.	**Have you determined what personal data is collected and how and where it is stored?** Conducting an inventory and data mapping exercise is important to meeting obligations under various data privacy and protection regulations. Determining what information your organization has and where it is located is the first step towards compliance.	☐	☐
4.	**Do you have processes and resources in place to support access requests from individuals?** Under the GDPR and the upcoming CCPA, individuals can request access to the data you hold on them. Requests must be responded to within a specific period of time and the information generally must be provided free of charge. Your business must have in place mechanisms to not only identify all the information maintained on a particular individual, but to erase, destroy, or securely transfer the data to the individual in a useable format if so requested. Having in place an effective solution that allows for requests to be met in a consistent and repeatable manner will be important for efficient operations. Additionally, companies will need to implement processes to authentic requests, *i.e.*, verify the identity of persons submitting requests.	☐	☐
5.	**Is there a legitimate business purpose or need for the personal information you are maintaining?** Given the proliferation of data protection laws and changing risks, businesses should consider whether the information maintained is necessary for the successful operation of the business. Any personally identifiable information or sensitive business information improperly accessed by hackers could be used to compromise your network, put you at significant risk of fines associated with data breaches, or lead to serious reputational damage. Businesses should not ask for more information than is necessary.	☐	☐

		Complete	N/A
6.	**Have you updated your privacy notices and privacy policies?** New data protection laws, including the CCPA, require transparency with regard to the collection and processing of personal data. For example, in California, if you own or operate a commercial website, online service, or app that collects and maintains personal data from California residents, current law requires the website or app to feature a conspicuous privacy policy stating exactly what information is collected and with whom it is shared; it also requires the operator of the website or online service to comply with the site's privacy policy. Additionally, after January 1, 2020, the CCPA will require updates to your privacy policy, including a dedicated link or button specifically titled "Do Not Sell My Personal Information," and annual maintenance thereafter.	☐	☐
7.	**Do you maintain records of all data processing activities?** Accurate recordkeeping is extremely important in this era of increased focus on data protection and privacy rights. Indeed, many data protection laws, like the GDPR, require organizations involved in collecting and processing personal information to keep a record of all processing activities performed or risk heavy fines in certain instances.	☐	☐
8.	**Do you have a data retention and destruction policy in place?** Data retention and destruction policies, while required under some data protection laws, is also good housekeeping within your organization. Developing and implementing a schedule will not only improve your operational efficiency, but it will also assist in demonstrating compliance with regulatory recordkeeping requirements and reduce litigation risks.	☐	☐
9.	**Do you have an ongoing audit procedure set up for the future?** Assessing your organization's privacy-related exposures should be a process, rather than a one-time effort. Doing so will assist in identifying the most effective way to comply with data protection obligations and meet evolving expectations of privacy. An ongoing audit procedure will also allow organizations to identify and remediate problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.	☐	☐
10.	**Do you have cyber/privacy insurance in place?** Currently, cyber and privacy insurance policies are not standardized and often differ dramatically in terms of what they cover and what they exclude. Understanding your organization's exposures and the coverages available will increase the value of the insurance to your organization. Additionally, given the rapidly changing legal landscape and coverage trends, it is important to review your cyber/privacy insurance policy annually to ensure the protections appropriately align with your organization's mission, exposures, and operations.	☐	☐

For More Information, Contact:

Elaine F. Harwell, Senior Counsel
619.906.5780
elaine.harwell@procopio.com

Procopio

What Will the California Consumer Privacy Act Actually Bring in 2020?

By: Elaine F. Harwell, CIPP/US

California's passage of a landmark data privacy and protection law, the California Consumer Privacy Act (CCPA), has rightly drawn significant attention. You may be aware that this sweeping new privacy legislation has its fair share of ambiguities, drafting errors, and contradictions, and has already been amended once. The law, which will become effective January 1, 2020, with enforcement delayed until the following July, grants new rights to California residents, including the right to access their information in a portable format and the right to opt-out of the sale of their personal information.

We recently reported on an important proposed amendment, SB 561, which would expand the private right of action to any violation of the CCPA and remove the ability to cure within 30 days of notification. The bill, which also authorized the Attorney General to provide general guidance on compliance, had the backing of Attorney General Xavier Becerra. On April 29, 2019, the California Senate appropriations committee placed this bill on the "Suspense File," which is a way to consider the fiscal impact of the bill to the state. On May 16, 2019, a hearing was held in committee and the bill was taken under submission, which means the bill has been blocked and is effectively dead.

Several other key proposed amendments, however, are still pending at various stages in the California legislature:

Amd No.	Analysis	Status
AB 25	This bill proposes to redefine "consumer" to exclude a person's personal information only to the extent that it is collected and used solely within their employee role, or similar role within the employment context.	On 5/1/19, the appropriations committee passed this bill. It was ordered to a third reading on 5/9/19 and will move to a vote by the full assembly and then potentially on to the Senate.
AB 873	This bill proposes to narrow the definition of "personal information" by removing information that is "capable of being associated with" a particular consumer and information that could be linked to a particular "household." It also redefines "deidentified" data.	On 5/15/19, the bill passed the assembly appropriations committee. It has been ordered to a third reading as of 5/16/19 and will move to a vote by the full assembly and then potentially on to the Senate.
AB 846	This bill would authorize customer loyalty programs even if a consumer opts-out of their personal information being sold.	On 5/8/19, the bill passed the assembly appropriations committee. It has been ordered to a

Amd No.	Analysis	Status
		third reading as of 5/9/19 and will move to a vote by the full assembly and then potentially on to the Senate.
AB 1564	Currently, the CCPA requires that businesses make available to consumers two or more methods to submit access requests, including, at a minimum, a toll-free number and a web address. This bill would instead require only that business make available a toll-free number *or* an email address, or if the business maintains a website, a method to submit requests via the website.	On 5/13/19, the bill was read a third time in assembly, passed, and ordered to the Senate.
AB 1416	This bill would clarify that the CCPA does not restrict an entity's ability to comply with any rules or regulations and permits the use of data to prevent fraud or illegal activity.	On 5/7/19, the bill was ordered to a third reading.
AB 1035	Currently, the law requires individuals be notified of a breach "in the most expedient time possible." This bill would require disclosure of a breach be provided in the most expedient time possible, but in no case more than 45 days following a data breach. It would also define "reasonable security procedures and practices" to include a cybersecurity program that reasonably conforms to specified standards published by the National Institute of Standards and Technology (NIST).	On 5/9/19, the bill was read a third time in assembly, passed, and ordered to the Senate.
AB 1281	This bill would require any business that uses facial recognition technology, as defined, to disclose that usage in a physical sign at the entrance of every location that uses the technology.	On 4/25/19, the bill was read a third time in assembly, passed, and ordered to the Senate. On 5/8/19, the bill was referred to committee (judicial and appropriations)

Impact on Business

Arguably, the proposed amendment with the biggest impact to business would have been SB 561, which as we previously reported would have expanded the private right of action to any (even technical) violations of the CCPA. While it appears there will be no expansion of the private right of action this year, many legal scholars and commentators believe the CCPA may still ultimately see an expanded right of action. We will just have to wait and see.

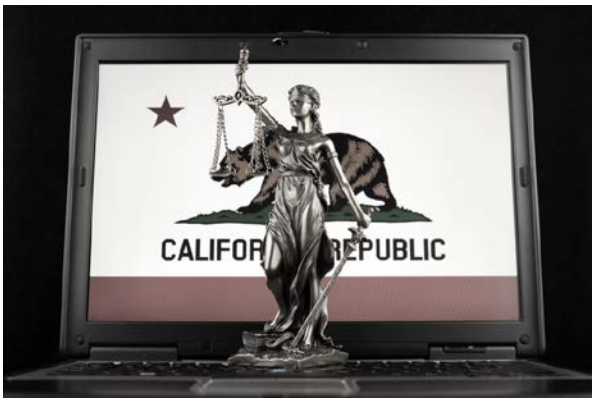
The majority of the proposed active amendments at this time appear to be poised to narrow or provide some needed clarity to provisions of the CCPA. For example, if AB 873 passes, it will focus the definition of personal information to information that is linked directly, or indirectly, to a particular consumer and may eliminate some of the confusion surrounding how to apply the CCPA to

"households." Ultimately, the CCPA will likely see several changes of the course of the next few months. The legislative session ends in September and in the meantime, we will continue to closely monitor the developments.

Elaine F. Harwell is a Senior Counsel with Procopio and a member of its Privacy and Cybersecurity Practice Group. She is an experienced business litigation attorney and a trained privacy professional. Her practice is focused on representing clients in cybersecurity and data privacy matters, including litigating claims involving privacy issues, helping clients manage emerging risks and conduct privacy risk assessments, and advising on regulatory issues. Elaine has also been involved in numerous trials as well as arbitration proceedings related to contract and general business disputes, complex unfair competition and business practice claims, and professional liability. She has earned the ANSI-accredited Certified Information Privacy Professional/United States (CIPP/US) credential through the International Association of Privacy Professionals (IAPP).

EXPANDED PRIVATE RIGHT OF ACTION PROPOSED FOR CALIFORNIA CONSUMER PRIVACY ACT

By Procopio Senior Counsel Elaine F. Harwell



When California quickly passed the landmark California Consumer Privacy Act (CCPA) last June, policymakers across the state made clear that they did not anticipate the new law--the most sweeping privacy legislation in the United States--would be implemented unchanged. What was unknown was what those changes might be, and whether they would reduce or increase burdens on businesses operating in the state.

Now, almost eight months later, the second set of proposed changes to the CCPA have been put forward that, while narrow in scope, could if enacted have a significant impact on California businesses through an expanded enforcement mechanism.

What Has Been Proposed

State Senator Hannah-Beth Jackson introduced legislation on February 25, 2019, to further amend the CCPA in a move supported by California Attorney General Xavier Becerra. According to Senator Jackson, Senate Bill 561 is intended to further strengthen the CCPA. If passed, the risk to businesses for noncompliance with the CCPA will dramatically increase. As currently drafted, SB 561 will:

- Expand the private right of action to any consumer whose "rights under [the CCPA] are violated." As currently drafted, the CCPA limits the private right of action to where consumers' non-encrypted or non-redacted personal information has been subject to a data breach as a result of the business' violation of the duty to implement and maintain reasonable security procedures.
- Remove the right to cure any alleged violation within 30-days after being notified.

The proposed changes to enforcement are notable. Consumers, without any demonstration of harm, would have the ability to file suit for any alleged violation of their rights under the CCPA. Additionally, if the proposed bill

passes as drafted, businesses would no longer have the opportunity to cure the violation within 30 days before a private lawsuit suit could be filed or before the Attorney General could initiate an action.

Notably, SB 561 also removes the onerous requirement that the Office of the Attorney General provide, at taxpayers' expense, legal opinions directly to any business or private party with individual legal counsel on CCPA compliance. Instead, the Attorney General will be given the option to "publish materials" that provide general guidance on how to comply with the CCPA.

Where We Stand Now

Passed and signed into law in 2018, the CCPA is scheduled to become effective January 1, 2020, with enforcement delayed until July 1, 2020. It is currently the most comprehensive privacy legislation in the U.S., with extensive new compliance requirements and liabilities for businesses. In short, the first-of-its kind legislation grants California residents a number of new rights with respect to the collection of their personal information by businesses.

Those new rights include, among others, the right to be informed about the categories of information a business collects and the purposes for which it is collected and sold, the right to access their information in a portable format, the right to request deletion of personal information, the right to opt-out of the sale of their personal information, and the right to be free from discrimination for exercising rights under the Act with respect to pricing and service. Businesses are required to respond to consumer requests for this information, free of charge, and within 45 days in an electronic format that can be transferred to another business.

Additionally, the CCPA creates specific transparency requirements relating to collecting and selling personal information. Businesses must disclose the new rights to California consumers in public-facing privacy notices and if "selling" personal information as defined by the act, businesses have additional obligations that include providing a "clear and conspicuous" link on the business' homepage titled "Do Not Sell My Personal Information."

Looking Ahead

Given the intricacies and detailed obligations for complying with the CCPA, the proposed amendments in SB 561 must be taken very seriously. This is especially true since SB 561 removes the opportunity to cure an alleged

violation. Thus, a well-intentioned business that makes an innocent compliance mistake will no longer have a chance to resolve the issue before enforcement actions or lawsuits are filed. Even more problematic is the fact that the CCPA is still riddled with drafting inconsistencies and ambiguities that make compliance a daunting task.

That said, further amendment by lawmakers and some clarification is anticipated from the Attorney General before the CCPA goes into effect in 2020. Additionally, even though aspects of the law may change before it becomes effective, there are many things that a business can do now to prepare for the upcoming changes, including identifying what personal information a business has, where it resides, where it came from, and where it is going. Conducting a thorough inventory and mapping of personal data is an important first step to complying with the CCPA (and other data protection laws) no matter the specifics of the law. Procopio's Privacy and Cybersecurity practice group members can assist with those and other privacy-related efforts.

Elaine F. Harwell is a Senior Counsel in Procopio's Privacy and Cybersecurity Practice Group. Elaine is a business litigation attorney and a trained privacy professional. Her practice is focused on representing clients in cybersecurity and data privacy matters, including litigating claims involving privacy issues, helping clients manage emerging risks and conduct privacy risk assessments, and advising on regulatory issues. Elaine has also been involved in numerous trials as well as arbitration proceedings related to contract and general business disputes, complex unfair competition and business practice claims, and professional liability. She has earned the ANSI-accredited Certified Information Privacy Professional/United States (CIPP/US) credential through the International Association of Privacy Professionals (IAPP). Elaine is also a frequent speaker and writer on legal issues surrounding privacy and data governance.

Scott Takaoka

Vice President, Client Executive

425 Market Street, 28th floor

San Francisco, CA 94104

Mobile +1.302.0289

scott.takaoka@aon.com

Responsibilities

Scott Takaoka is Vice President, Cyber Solutions Group at Aon. Based out of the firm's San Francisco office, he is responsible for developing and growing the firm's relationships with enterprise clients, helping them identify, characterize and proactively manage their cyber risk and increasing their resilience to cyber events.

Scott is a part the Aon Cyber Solutions Group, comprised of cyber liability insurance brokers, cyber security consultants, digital forensic/incident response practitioners and cyber risk analysts, providing a comprehensive solution portfolio to assist clients with their cyber risk management challenges. With this holistic approach, Aon helps its clients understand and characterize their current levels of cyber risk, then provides risk transfer and risk mitigation solutions should their current risk levels exceed their appetite for such risks.

Experience

Prior to joining the Aon Cyber Solutions Group, Scott spent 3 years a Vice President, Business Development for an application security and GRC consulting firm, focused on organizational threat modeling, security program development/outsourcing, and penetration testing of applications, network, IoT devices. Scott helped his client design and implement risk based application security programs that focused on balancing business impact from exploits of vulnerabilities with cost of remediation. He helped clients develop risk frameworks to measure security program impacts, and communicate risk to non-technical stakeholders outside of IT and security organizations.

Before that, Scott spent 4 years as Vice President of Business Development for a SaaS based application vulnerability scanning company, where he was responsible for joint solution development and strategic alliances. Scott led an initiative to develop risk based metrics program to help guide clients on remediation decisions based in business impact instead of technical risk.

Previously, Scott spent 17 years in both hardware and software based technology companies in a variety of business development, product management and sales positions.

Education

Scott earned Bachelor of Arts Degrees in Political Science and Rhetoric from the University of California, Davis.

John Shin, CISSP, QSA, CISM

Managing Director, RSI Security

John Shin is currently a managing director at RSI Security. RSI is a cybersecurity-focused technology company that helps private and public sector organizations in highly regulated industries to effectively manage risk. RSI provides cyber-engineering, assessment, advisory services as well as technical testing to amp up client's security posture while mitigating business risk.

Qualified security assessor for Payment Card Industry, Certified Information Systems Security Professional, Certified information security management, and principal author on multiple Internet privacy and security technology papers such Dominant Cyber Offensive Engagement and Supporting Technology and Reconnaissance & Data Exfiltration for U.S. Air Force Research Laboratory. Mr. Shin has 18 years of leadership, management, and Information security experience. Previously, at Abraxas Corporation, He was a director responsible for cybersecurity programs and solutions used by the National Security community such as FBI, CIA, NSA, DISA etc. Mr. Shin held various management positions for VeriFone's global security solution and Genoptix. John Shin holds B.A from the University of California, San Diego and an MBA from Rady School of Management. John is currently a member of board for Entrepreneurs Organization, a global non-profit organization exclusively for entrepreneurs.