CYBERSECURITY

Presented by

CHASE

How To Secure Against the Rise of the Ransomware Economy

The State of Cyberextortion and Why Artificial Intelligence Holds the Key To Prevention

The pervasiveness of ransomware has made big headlines recently, and it's a top cybersecurity concern in 2018 and beyond. Cybersecurity experts describe the proliferation of ransomware attacks in sweeping proportions, and the growing number of attacks reflect a critical threat to industries such as finance, retail, healthcare, the public sector, and more.

An opportunistic and profitable type of malware, ransomware is specifically designed to block access to data on an infected system until payment is received. Ransomware often uses a trojan to gain a foothold on a computer by targeting victims with a malicious payload disguised as a legitimate file. This digital form of extortion is motivated by financial gain and has been successful because it often costs less to pay the ransom than to restore lost data. Unfortunately, payment often leads to continued attacks.

Stuart McClure

Ransomware campaigns can be carried out by cybercriminals with little to no technical skills, or by organized crime syndicates with significantly more experience and funding. In the dark web, the unseen depth of the Internet where criminals operate, ransomware-as-a-service (RaaS) toolkits are marketed and sold, providing nearly anyone the ability to embark on a ransomware campaign. Cybercriminals not only make money through individual attacks, but they also offer their skills and services to provide ransomware to others for a fee.

Ten Things Organizations Need To Know About Ransomware

Ransomware may be damaging, but it can be prevented. Armed with the right intelligence and software, organizations can keep ransomware from holding their data hostage.

1. Ransomware was first reported in 1989
   - Since then, a number of different variants have evolved
2. Ransomware doesn't discriminate when it comes to platforms and devices
   - Any device that can connect to the Internet is at risk
3. Ransomware can be distributed through various channels:
   - Spam email campaigns that contain malicious links or attachments
   - Exploits in vulnerable software
   - Internet traffic re-directs to malicious websites
   - Malicious advertisements (known as 'malvertising')
   - Social engineering (misleading users to break security protocols that introduce malware)
   - Self-propagation (spreading from one infected computer to another)
   - SMS messages
   - Botnets
4. Ransomware often goes undetected
   - Traditional antivirus lacks the ability to identify and remove second-generation malware
5. Organizations need to change from a reactive model to a preventative model
   - Keep software up to date, including operating systems
   - Avoid dangerous web locations
   - Educate staff about phishing emails, infected banners, and social engineering
   - Use artificial intelligence and machine learning cybersecurity tools
6. Organizations should develop a prevention and response plan
   - Prepare in advance of an attack
   - Find and address vulnerabilities
   - Review and test your plan
7. Organizations should identify a prevention and response team
   - Choose an appropriate service level agreement
   - Ensure the team possesses specialized expertise
   - Vet and validate the team's expertise
8. Organizations should perform a compromise assessment
   - Detect current and previously compromised systems
   - Collect evidence and analyze adversary tactics
   - Remediate across the enterprise
9. Organizations should complete a security tools assessment
   - Evaluate existing security tools
   - Execute a gap analysis
   - Remediate findings and outline opportunities for improvement
10. Organizations should respond and future-proof
    - Contain discovered incidents immediately
    - Perform complete remediation activities
    - Carry out sustainable prevention

The Good News

A transformational cybersecurity approach today is changing the industry landscape and provides good news for combating ransomware. The application of artificial intelligence and machine learning provides a new level of malware and ransomware security with prevention rates as high as 99.4 percent.

Only Cylance® offers a pathway to prevention using its award-winning product, CylancePROTECT®, and Cylance Consulting Services, which identify, remediate, prevent, and monitor ransomware as well as other cyberthreats. Cylance's AI, coupled with its expertise, brings cybersecurity to a state of provable prevention.

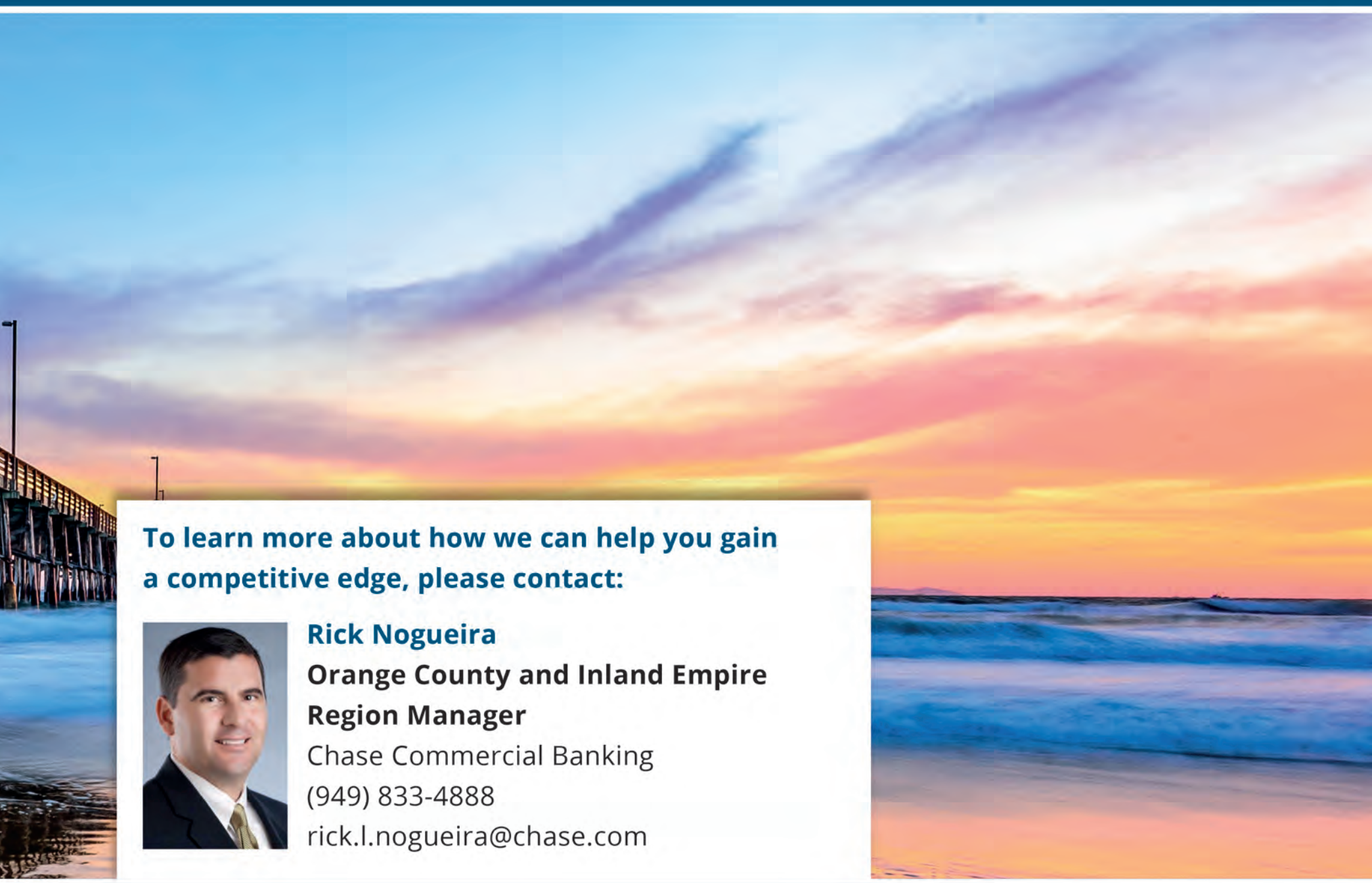
To learn more about how Cylance can help you remediate, or prevent ransomware, visit www.cylance.com/ransomware.

CHASE

Your Business Is Unique.

Are your financial solutions built to match?

We're dedicated to fostering growth in Orange County's communities. Let's start with your business. You can count on our full range of best-in-class products and services to position your business for long-term success, and seamless access to our firmwide network of experts means you'll receive customized financial solutions—along with the latest industry insights—to help meet your growing needs.



To learn more about how we can help you gain a competitive edge, please contact:

Rick Nogueira
Orange County and Inland Empire Region Manager
Chase Commercial Banking
(949) 833-4888
rick.l.nogueira@chase.com

CHASE

Industry-Standards-Based Cybersecurity Services for Small to Medium Sized Enterprises

Cytellix, the Cybersecurity Division of Information Management Resources Inc. (IMRI), located in Aliso Viejo, CA, is an industry-standards-based, managed cybersecurity service provider, specializing in cyber assessments, proactive behavioral analytics, vulnerability identification and situational awareness of an organization's cyber posture. Cytellix created an affordable cloud-based solution for small and medium-sized enterprise (SMEs); one of the largest targets of cyber-attacks. Since 2008, Cytellix has been a trusted provider of cybersecurity services supporting critical cyber command operations for the U. S. Department of Defense including the U. S. Army Netcom Enterprise Command Worldwide, U. S. Missile Defense Agency; Department of Homeland Security and classified agencies within the United States.

Cyber-attacks today target the vulnerable entry points that are considered the "weakest link" with the most significant targets in supply chain and the small and medium enterprise (SMEs). Over 70 percent of all cyber-attacks are targeted towards SMEs and when they are attacked 60 percent of these businesses are forced to close their doors. In the last 12 months, hackers have breached half of all 28 million small businesses in the United States and the Security and Exchange Commission wrote in a recent report; "Small and midsize businesses are not just targets of cybercrime; they are its principal target."

With leadership from CEO Martha Daniel, Cytellix has headed up a collection of standards-based turnkey cyber programs for municipalities, police departments, and local government groups with a focus on IoT monitoring systems, network segmentation, industrial controls, and critical infrastructure in Orange County. Utilizing industry standards, such as the NIST Cybersecurity Framework, GDPR, FFEIC, ISO, and HIPAA, Cytellix provides enterprises with best-in-class, real-time cyber awareness as an affordable turnkey service.

Why Cytellix: Cytellix provides expertise in cybersecurity, risk management, governance, compliance, information assurance, and operations security. We offer affordable enterprise-grade cybersecurity services and premium consulting as a subscription service. We provide industry standards based cyber assessments, gap analysis, security plans, remediation plans and a real time security operations center, the user-friendly portal, contains "Red, Yellow and Green" cyber awareness statuses; cyber policies, and a mobile app to access real-time continuous cyber situational awareness. Cytellix has the only solution in the industry that can detect "known and unknown" threats in any enterprise environment, while providing complete network visibility and threat intelligence. Cytellix experts analyze and investigate the traffic and behavioral analytics of millions of IP addresses for organizations in a wide range of data-rich industries—government, manufacturing, finance, banking, law, higher education, and healthcare.

Cytellix breaks through the crowded cybersecurity market with community engagements. Whether it be webinars, workshop events, or customized guidance, Cytellix is committed to sharing their cybersecurity expertise and improving cyber awareness throughout the county. Cytellix has partnered with Manufacturing Extension Partners, Security and IT Channel Partners, Managed Service Provider's (MSP's), ISO Standard Consultants and International Association of Microsoft Channel Partner's around the USA to provide Cyber Managed Services designed for SME market. Cytellix, recipient of the 2018 Gold American Business Award for Most Innovative Company of the year, helps businesses stay in business.

Trenelle Lyiscott
Cyber Support Manager
949-215-8889 www.cytellix.com

A California Version of GDPR May Be Coming - What You Need to Know About the California Consumer Privacy Act of 2018

By Anne Kelley

People in the U.S. are becoming increasingly aware that their personal data is being shared in ways they never imagined as companies like Facebook, Uber, Safeway and Target are tracking and selling their personal information on a regular basis. Many people feel helpless in stopping companies from sharing their data. A coalition located in Oakland, California, right in Silicon Valley's backyard, believes it is high time for people to have more control over their own personal data. The coalition has authored a proposed California ballot initiative expected to be on the ballot in November of 2018, the California Consumer Privacy Act of 2018. Some are comparing the proposed initiative to the European Union's General Data Protection Regulation, or GDPR, as the initiative's goals are to protect individuals' private information and to give users greater control over how companies use their personal data.

The backlash against the sharing and sale of personal data is increasing due to recent Facebook revelations. In March, Facebook admitted that data on as many as 87 million users was passed to third parties, including British political consulting firm, Cambridge Analytical. Very recently, Facebook confirmed even more data sharing when it acknowledged that it entered into data-sharing partnerships over the last decade with at least 60 device-makers, giving them access to users' data. These agreements included a Chinese company Huawei, which U.S. intelligence officials view as a national security threat. The big problem: neither Facebook users nor the U.S. government had any idea the users' data was being shared so broadly.

On May 25, 2018, Europe's sweeping GDPR went into effect which gives heightened protection to data being gathered on EU citizens. Data protection laws are being proposed in the United States, including legislation in Congress (CONSENT—Consumer Online Notification for Stopping Edge-Provider Network Transgressions) and the California Consumer Privacy Act of 2018.

The California Consumer Privacy Act of 2018 has three central components and gives consumers the right to: (1) "opt out" of data sharing by demanding companies not share or sell their personal data for business purposes; (2) ask companies to disclose what data they have collected and to whom they are disclosing or selling it; and (3) sue or fine companies that are in violation. The initiative also holds businesses accountable if they experience a security breach that discloses consumers' personal information. Google, Facebook and other internet companies have already come out against the initiative.

If voters approve the California Consumer Privacy Act of 2018, it will apply to anyone who goes on the internet in California. Certain companies will be required have a "clear and conspicuous link" on their website's homepage titled "Do Not Share My Personal Data" that would allow users to opt out of having their data sold or shared. Upon request, businesses would also be required to disclose the categories of information they have collected on users and to whom they have sold that data. Companies will also be required to "implement and maintain reasonable security procedures and practices" to ensure that consumers' private information is not exposed in a security breach.

In an age of ever-expanding internet use, security breaches, and increasing questions about data collection and sharing, the California Consumer Privacy Act of 2018 may just be the tip of the iceberg when it comes to regulating how companies collect, store and use individuals' personal data.

Anne Kelley

Anne Kelley is a partner at Newmeyer & Dillion, where she advises clients on cybersecurity related matters, including cyber insurance coverage and data privacy issues. Anne frequently writes and speaks on these topics. For questions on how she can help your business navigate your cybersecurity needs, please contact her at anne.kelley@ndlf.com.

CALLAHAN & BLAINE

Identifying What Constitutes Biometric Information

In April 2018, Facebook CEO Mark Zuckerberg sat before Congress to answer questions about Cambridge Analytica. Mr. Zuckerberg's testimony became front-page news. And rightfully so; Cambridge Analytica obtained the personal data of 87 million Facebook users worldwide, 70 million of those users are from the United States.

For millions of Facebook users, the Cambridge Analytica scandal invoked never thought of questions: Who, besides Facebook, has access to my personal information? Why does Facebook have it? What is Facebook going to do with my personal information? And how did Facebook obtain it in the first place?

For a variety of reasons, these are difficult questions to answer. One reason for this difficulty is that the United States lacks a universal definition of personal information. While most people know to safeguard their bank account information and social security numbers, fewer people understand that personal information extends to biometrics—or measurements related to human characteristics, such as fingerprints, voiceprints, iris scans, and retina scans.

So before answering who has my personal information, why do they have it, what are they going to do with it, and how did they even get it, there is a threshold question to answer: what is personal information?

The GDPR's Definition of Personal Information Includes Biometric Information

In the European Union, the answer to that question is universally defined. The General Data Protection Regulation (GDPR) defines "personal data" as "any information relating to an identified or identifiable natural person." [Art. IV(1)]. The GDPR in turn defines "an identifiable natural person" as 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. [Art. IV(1)]. The GDPR's definition of personal information is very broad; it includes genetic data and biometric information. While such a broad definition invokes questions of its own, whether any type of biometric information is also considered personal information should not be one of them.

Unlike in the European Union, the United States lacks a universal definition. Each state is therefore left to define personal information independently. In 2008, the Illinois Legislature enacted the Biometric Information Privacy Act (BIPA), which defined biometric information specifically.

BIPA's Definition of Biometric Information

BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." [740 ILCS 14/10]. Notably, "biometric information does not include information derived from items excluded under the definition of biometric identifiers" (i.e. photographs). [740 ILCS 14/10].

BIPA's definitions of "biometric identifiers" and "biometric information" therefore create ambiguity whether biometric information includes information derived from digital photographs (i.e. scan of face geometry) notwithstanding BIPA's express exclusion of photographs from its definition of biometric identifier. [740 ILCS 14/10]. This ambiguity now appears resolved following judicial interpretation.

Shutterfly, Facebook, and Google each were named as defendants in separate putative class actions alleging violations of BIPA. These class actions followed a similar framework: (1) BIPA requires, among other things, that a company provide notice before it collects and stores biometric information; but (2) Shutterfly, Facebook, and Google captured and stored biometric information by conducting face scans of the respective plaintiffs from digital photographs without providing the requisite prior notice. [740 ILCS 14/15].

Predictably, Shutterfly, Facebook, and Google each moved to dismiss the respective class actions brought against them, arguing that BIPA does not protect information derived from photographs. All three were unsuccessful, however. *See Norberg v. Shutterfly*, 1:15-cv-05351 (N.D. Ill. June 23, 2015) (by alleging that Shutterfly used the plaintiff's personal face pattern to identify him in a photograph, the plaintiff stated a claim under BIPA); *In re Facebook Biometric Information Privacy Litigation*, 15-cv-03747-JD (N.D. Cal. May 5, 2016) (reasoning that "photographs" are better understood to mean paper photographs, as opposed to digital ones); *Rivera v. Google, Inc.*, 1:16-cv-02714 (N.D. Ill. Feb. 27, 2017) (reasoning that Google creates a set of biology-based measurements ("biometric") used to identify a person ("identifier") and a face template is a "scan of … face geometry," as defined under BIPA).

California's Proposed Definition of Biometric Information

California is poised to avoid the uncertainty surrounding whether face scans of digital photographs constitutes biometric information. The California Consumer Privacy Act, currently waiting whether it obtained enough signatures to appear on the November ballot, defines "biometric data" as "an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid, which can be used, singly or in combination with each other or with other identifying data to establish individual identity." [The California Consumer Privacy Act of 2018 § 1798.106 (a)]. The definition expressly includes, without limitation, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings. [The California Consumer Privacy Act of 2018 § 1798.106 (a)].

While the California Consumer Privacy Act, if passed, would eliminate the ambiguity of whether face scans of digital photographs constitute biometric information, more problems persist. Its broad scope is all but certain to require judicial interpretation to determine, for instance, under what circumstances behavioral characteristics constitute biometric data.

But perhaps the greater problem is the lack of uniformity in the United States as to what constitutes biometric information. As of now, only three states, Washington, Texas, and Illinois have biometric privacy statutes in effect. And only Illinois allows for a private right of action. The lack of uniformity unfairly exposes companies operating in Illinois to lawsuits challenging their biometric collection practices, when regulations in other states are different or altogether nonexistent. And absent uniformity, consumers are left guessing what constitutes biometric information. Without knowing the answer, companies and consumers alike cannot take the appropriate steps to safeguard that information.

Until there is a uniform answer for the threshold inquiry—what is personal information—consumers are hard-pressed to answer who has their personal information, why they have it, what are they going to do with it, and how did they get it in the first place?

Kamran Salour
Kamran Salour is a Senior Trial Attorney with Callahan & Blaine where he represents and defends clients in business disputes. His experience extends to cyber security, privacy, and data protection matters. He is a certified information privacy professional for the U.S. Sector (CIPP/US) and a frequent commentator on biometric privacy law.

California Voters Can Expose Businesses to New Penalties for Data Privacy and Security Violations

In November, voters will decide whether to enact the California Consumer Privacy Act of 2018 (CCPA), which recently qualified as a ballot initiative. Contrary to recent interest, the CCPA would not impose a "European style" or "GDPR-like" data protection framework on companies doing business in California. Nevertheless, the act will impose obligations on many companies to update their privacy policies, strengthen their information security systems, and enhance their process for mapping organizational data flows. Perhaps most significantly, the act would empower plaintiffs to seek statutory damages for violations of new privacy rights and California's existing information security laws.

If the act becomes law, enforcement of four new rights would begin on August 6, 2019:

1. Within 45 days of receiving a consumer's "verifiable request," a covered business must disclose the categories of personal information that it has "collected" about that consumer.
2. Within 45 days of receiving a consumer's "verifiable request," a covered business must disclose the categories of personal information that the business sold, or otherwise shared for a "business purpose," about that consumer, as well as the identities of the third parties who received the information.
3. A consumer would have the right to direct a business not to sell the consumer's personal information (*i.e.*, to "opt out").
4. Businesses would be prohibited from providing a different level or quality of goods or services to consumers who opt out.

A violation of the act would constitute an "injury in fact," meaning consumers would not need to suffer a loss of money or property in order to bring a lawsuit individually or as a class. Consumers may recover statutory damages of $1,000, or actual damages if greater, for each violation. In the case of "knowing and willful violations," consumers may recover up to $3,000, or actual damages if greater, for each violation.

Finally, a business that suffers a data breach, as defined in California's existing information security law (Civil Code § 1798.82) would be deemed to have violated the act, and will be liable for statutory damages if it has failed to implement and maintain reasonable security procedures and practices.

Covered businesses would include any company doing business in California that:

(i) collect consumers' personal information; and
(ii) have annual gross revenues of more than $50 million, or annually sells the personal information of 100,000 or more consumers or devices, or derives 50 percent or more of its annual revenue from selling consumers' personal information.

If the voters pass the act into law, the Attorney General will have six months to adopt regulations that will hopefully provide more concrete guidance including, among other things, a meaningful definition of a consumer's "verifiable request." Covered businesses should be sure to account for any new legal obligations and exposures when conducting risk assessments and be prepared to modify compliance programs accordingly in advance of August 6, 2019 if the act is passed.

Travis Brennan, Shareholder, tbrennan@sycr.com, (949) 725-4271
http://www.sycr.com/Travis-P-Brennan/

Travis Brennan
Travis counsels clients in developing and implementing privacy and data security compliance programs, and guides clients through data breach investigation and response matters. He focuses on data protection issues across a range of industries and is accredited as a Certified Information Privacy Professional with a focus on U.S. private sector law.