Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 1 | JANUARY 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [1] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT
January 2019

EDITOR'S NOTE
Developments

Victoria Prussen Spears*

Welcome to *Pratt's Privacy & Cybersecurity Law Report*! We are excited to ring in the New Year with a host of timely and informative articles from around the nation!

National Cyber Strategy

In our lead article, "White House Releases 'National Cyber Strategy,'" John A. Horn and Bethany L. Rupert, attorneys at King & Spalding LLP, discuss the National Cyber Strategy, which offers a comprehensive set of objectives such as the preservation of a free, open, and secure internet, while also signaling tougher repercussions for nations and criminals that engage in malicious cyber activity.

New Privacy Law in California

Our next article, "Landmark New Privacy Law in California to Challenge Businesses Nationwide," by David C. Keating and David Caplan, attorneys at Alston & Bird LLP, reviews California's sweeping new law that establishes an array of privacy rights for state residents and worries for businesses nationwide.

Revisions to the California Consumer Privacy Act

The California Legislature passed SB 1121 to revise certain sections of the California Consumer Privacy Act – the nation's strictest privacy protection statute which provides Californians with a right to learn what personal information certain businesses collect about them, to stop the sale of their personal information to third parties, and to sue over data breaches if companies fail to adequately protect their information. Natasha G. Kohne, Diana E. Schaffner, Dario J. Frommer, and Jo-Ellyn Sakowitz Klein, attorneys at Akin Gump Strauss Hauer & Feld LLP, discuss the Act and the key

* Victoria Prussen Spears is a researcher, writer, editor, and marketing consultant for Meyerowitz Communications Inc. A graduate of Sarah Lawrence College and Brooklyn Law School, Ms. Spears was an attorney at a leading New York City law firm before joining Meyerowitz Communications. Ms. Spears, who is Editor of *The Banking Law Journal*, *Pratt's Journal of Bankruptcy Law*, *Pratt's Energy Law Report*, *Pratt's Government Contracting Law Report*, and *Pratt's Privacy & Cybersecurity Law Report*, all published by Lexis, can be reached at vpspears@meyerowitzcommunications.com.

changes in their article, "The Significance to Businesses of the California Legislature's Last Minute Revisions to the 2018 California Consumer Privacy Act."

Ohio's Cybersecurity Safe Harbor

Corporate victims of data breaches often become the targets of litigation and governmental enforcement actions, adding costly insult to serious injury. In their article, "Preparing for Ohio's Cybersecurity Safe Harbor Law," Steven G. Stransky and Thomas F. Zych, attorneys at Thompson Hine, discuss a new Ohio law addressing this inequity by providing (limited) protection from private litigation to businesses that suffer a data breach despite their cybersecurity planning and execution.

Data Privacy: Developments in Regulatory Enforcement

In our next article, "Data Privacy: Developments in Regulatory Enforcement," Mark C. Mao and Ronald I. Raether Jr., partners at Troutman Sanders LLP, review developments in privacy regulatory enforcement, noting that the Office of Civil Rights and the Department of Health and Human Services continue to impose the highest fines per consumer through regulatory enforcement.

HIPAA Violations

In her article, "Judge Grants Summary Judgment in Favor of OCR for HIPAA Violations Ordering a Texas Cancer Center to Pay $4.3 Million in Penalties," Marcia L. Augsburger, a partner at King & Spalding LLP, discusses an administrative law judge's ruling that the U.S. Department of Health and Human Services and its Office for Civil Rights properly imposed penalties against MD Anderson Cancer Center for failing to encrypt laptops and USB thumb drives, in violation of the Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rules.

Enjoy the issue and the New Year!

White House Releases "National Cyber Strategy"

John A. Horn and Bethany L. Rupert*

The authors of this article discuss the National Cyber Strategy, which offers a comprehensive set of objectives such as the preservation of a free, open, and secure internet, while also signaling tougher repercussions for nations and criminals that engage in malicious cyber activity.

The White House released its long-awaited National Cyber Strategy[1] (the "Strategy"), offering a comprehensive set of objectives such as the preservation of a free, open, and secure internet, while also signaling tougher repercussions for nations and criminals that engage in malicious cyber activity. The Strategy is similarly ambitious in its expectations for enhanced partnerships between federal agencies and private sector entities and foreign governments. That said, this expansive list of priorities includes few specific actions or steps to implement or accomplish the stated goals, and will require concurrence from private sector businesses and foreign governments that may be reluctant to fully jump into these initiatives. In short, as with many strategic plans, it is a thorough and thoughtful approach but lacks concrete action items and will require significant diplomacy to achieve the anticipated buy-in.

THE FOUR PILLARS

The Strategy is centered around four pillars:

1) protecting against cyber threats by strengthening U.S. government and private information networks, securing critical infrastructure, and enhancing cybercrime enforcement efforts;
2) boosting the digital economy by promoting innovation in the technology sector, guarding intellectual property, and increasing the ranks of our cybersecurity workforce;
3) combating cyber threats and preserving the United States' superiority in safeguarding the internet through taking aggressive actions (thus far unidentified) if necessary; and
4) promoting an open and free internet.

---

* John A. Horn, a partner at King & Spalding LLP and a former Atlanta U.S. Attorney, specializes in government and internal investigations, white collar criminal defense, and crisis management. Bethany L. Rupert is an associate in the Special Matters/Government Investigations Practice Group at the firm focusing on white-collar criminal defense, internal corporate investigations and corporate compliance reviews, and civil litigation. The authors may be reached at jhorn@kslaw.com and brupert@kslaw.com, respectively.

[1] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

The Strategy's most expansive set of objectives are protective in nature, ranging from centralizing and increasing the resiliency of federal agency IT networks, to improving space and maritime cybersecurity, protecting election and other critical infrastructure, and aiding partner nations' cyber enforcement capacity. To combat cybercrime, the Strategy emphasizes "[t]he prompt reporting of cyber incidents to the Federal Government," as well as the implementation of "standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem."[2]

To bolster national defenses against attacks, the Strategy emphasizes that federal cybersecurity efforts will hinge on support from private industry. For example, the Administration expects information technology companies and tech start-ups to work with government agencies and law enforcement to "to confront challenges presented by technological barriers, such as anonymization and encryption technologies,"[3] and to use artificial intelligence and quantum computing to deter cyber threats. The Strategy identifies seven industries with which the government will prioritize building relationships and sharing information: "national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation."[4] Several are singled out for special attention: for example, recognizing that "[i]nformation and communications technology (ICT) underlies every sector in America," the White House plans to work with ICT providers to improve ICT security by sharing classified threats with ICT providers who have been "cleared" for such information.

WILL THERE BE CENTRALIZED FEDERAL REGULATION?

One frequent criticism of current federal cybersecurity policy is the lack of a cohesive national regulatory structure, such that myriad agencies and state regulators have enacted a hodge-podge of security standards and breach notification rules. The Strategy recognizes the increasing number of agencies regulating in this space and pledges to clarify their roles and responsibilities, as well as their "expectations on the private sector related to cybersecurity risk management and incident response."[5] The Strategy further recognizes the importance of reporting cyber incidents to the federal government "by all victims, especially critical infrastructure partners," but offers no details regarding the manner in which this reporting will occur. It is hard to guess exactly what the Administration has in mind here; certainly, the language hints of more

[2] The White House, "National Cyber Strategy of The United States Of America," September 2018, *available at* https://www.whitehouse.gov/wp-content/uploads/2018/09/national-cyber-strategy.pdf, p. 10-11, 15.

[3] *Id.* at p. 10.

[4] *Id.* at p. 8-9.

[5] *Id.* at p. 8.

centralized federal regulation of data security and breach notification, but it is also telling that the document intentionally omits any specific recommendations or plans to achieve this goal.

A DRASTIC SHIFT

The Strategy's most notable and drastic shift from the policies of prior administrations comes in an explicit warning to nation-state and criminal actors alike that more aggressive responsive actions are in store for malicious cyber activity against the U.S. government, businesses, and citizens. The language is once again oblique, stating only that the United States will "develop swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior." Recent public statements by Administration officials have added further details, as National Security Advisor John Bolton confirmed during a press conference[6] that the White House has intentionally "authorized offensive cyber operations . . . not because we want more offensive operations in cyberspace, but precisely to create the structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear." Bolton did not elaborate on the nature of the offensive operations, but he confirmed that the Administration has rescinded Obama-era executive orders restricting the use of retaliatory hacking.

SAFEGUARDING DOMESTIC CRITICAL CYBER INFRASTRUCTURE

Following such widely publicized attacks to public infrastructure such as the Russian hack of the Ukranian power grid, the Strategy recognizes the need to safeguard domestic critical cyber infrastructure. To accomplish this, the White House plans to partner with private industry to "collectively use a risk-management approach to mitigating vulnerabilities to raise the base level of cybersecurity across critical infrastructure."[7] At the same time, the Administration will "develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks."[8] Key to this plan is to share the information learned with the industries identified in the Strategy: "national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation."[9]

---

[6] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administration-seeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/?utm_term=.048b68ae030f.

[7] National Cyber Strategy, *supra* note 2, p. 8.

[8] *Id.*

[9] *Id.* at p. 8-9.

NEW TECHNOLOGIES

The continued development of new technologies also will be an important contributor to both strengthening our cyber defenses and preserving the United States' role as an influencer in global cyber policymaking. Specifically, "[t]he Administration will work across stakeholder groups, including the private sector and civil society, to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies."[10]

Additionally, to promote an open internet, the Administration plans to support and encourage "open, industry-led standards activities based on sound technological principles."[11] The objective of the White House in promoting such developments and standards is to "advance American influence" and ultimately protect the nation from further threats.

CONCLUSION

In sum, much remains to be seen in terms of proposing specific steps to accomplish the many objectives and achieve the broad platitudes in this document. One of the biggest questions moving forward will be the receptiveness of the private sector and foreign governments to the invitations to partner with the White House to solve these challenges. Would-be partners in Silicon Valley and elsewhere have expressed reservations about the government's policies on encryption, and companies often have mixed views about fulsome sharing with the government about cyber threats and incidents. Corporations have a duty to abide by not only the privacy and security laws of the United States, but also those of other countries in which they operate. And as foreign jurisdictions are enacting increasingly strict limitations regarding the transfer of data outside their borders, many of these countries are expressing increasing reservations about U.S. data privacy laws and procedures.

Still, those attitudes may change in the coming months and years as Congress ramps up to consider its own federal legislation on data privacy. In a Senate hearing on September 26th involving some of the nation's largest tech and communications companies, several senators expressed readiness to pass a law similar in effect to the EU's General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act. Sen. Brian Schatz (D-Hawaii)[12] said that, although he understood the concerns of tech and communications companies, such companies should not expect Congress to "replace a progressive California law – however flawed you may think it is – with a nonprogressive federal law." In a second hearing on this topic held on

[10] *Id.* at p. 14.

[11] *Id.* at 25.

[12] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/27/the-cybersecurity-202-senate-hearing-highlights-challenges-of-crafting-national-privacy-law/5babbb8a1b326b7c8a8d16aa/?utm_term=.ff5c40b3368b.

October 10th, senators listened to the viewpoints of privacy advocates, who reinforced the need for a federal law, and stressed that this law should work alongside state laws, rather than preempting them, and that the law should be backed with enforcement authority from the Federal Trade Commission or a new federal agency. Although some legislators have expressed concerns about fashioning the law in this manner, or creating something similar to the California law or the GDPR, there appears to be some agreement that federal privacy legislation is necessary to bring coordination to 50 different state laws that vary significantly. As stated by Committee Chairman Senator John Thune (R-SD),[13] "The question is no longer whether we need a law for consumer data privacy, the question is what shape these laws will take.

[13] https://mashable.com/article/tech-industry-consumer-data-protection-senate-hearing/#iuyFcW9y-JiqR.

Landmark New Privacy Law in California to Challenge Businesses Nationwide

By David C. Keating and David Caplan*

This article reviews California's sweeping new law that establishes an array of privacy rights for state residents and worries for businesses nationwide.

Governor Jerry Brown has signed the landmark California Consumer Privacy Act of 2018 ("CCPA").[1] The CCPA was swiftly devised and passed as part of a deal to avoid a similarly named ballot initiative from being added to the November 2018 ballot by an organization called Californians for Consumer Privacy.

The CCPA is a sweeping new law that establishes an array of new rights for California residents regarding the collection, use, and disclosure of personal information. Effective January 1, 2020,[2] businesses in and outside of California that fall under the law will need to develop policies, procedures, and infrastructure to come into compliance. Because the CCPA was rushed through the legislature to meet the deadline imposed by the backers of the ballot initiative, we anticipate it will be subject to one or more amendments prior to 2020. The CCPA also authorizes the state attorney general to develop regulations "to further the purposes of" the statute.[3] Accordingly, businesses falling under the CCPA should also anticipate some changes to the law before it becomes effective.

The following provides an overview of the new law and concludes with key initial takeaways for business.

COVERED BUSINESSES

The CCPA defines "business" as a for-profit legal entity doing business in California that collects personal information of California residents, or on whose behalf the

* David C. Keating is partner at Alston & Bird LLP and is a co-leader of the firm's Privacy & Data Security Practice focusing his practice on matters involving technology and data. David Caplan is an associate in the firm's Technology and Privacy Group with experience in intellectual property litigation. The authors may be reached at david.keating@alston.com and david.caplan@alston.com, respectively.

[1] CALIFORNIA CONSUMER PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&mkt_tok=eyJpIjoiWTJSbFpUWmxOR014TXpjMyIsInQiOiJvMEpxbWdVbFwvT1hnQ3hWeER4YzZDVzFwQktQc0RvbGJPYlVoUjJ4bEd4WHhDTTlZTFlGXC9Pa0FyVURIYUl5UHp6dzV0b2pQUStXcU1oSFNUS2lTZDRReUJSZTlZaThFelV3aTU4M0o2OEFWTkdMN3YyYjBra2pQQU1BKzJBdVpiIn0%3D.

[2] § 1798.198(a). All citations to the CCPA are to Section 3, Title 1.81.5 of the CCPA, added to Part 4 of Division 3 of the California Civil Code.

[3] § 1798.185(a)(1)-(2), (4), (7).

personal information is collected, and that determines the purpose and means of processing the personal information. A business must meet one of the following thresholds: (a) annual gross revenues in excess of $25 million; (b) annually buys, receives, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more California residents, households, or devices; (c) or derives 50 percent or more of its annual revenues from selling residents' personal information. The term business also includes any entity that controls or is controlled by a business meeting one of the above thresholds and that shares common branding with the same.[4]

Certain businesses are out of scope by virtue of being covered by certain other state or federal privacy laws. For example, businesses in the healthcare industry are not subject to the CCPA to the extent the business collects protected health information under the California Confidentiality of Medical Information Act or the Health Insurance Portability and Accountability Act.[5] The CCPA does not apply to the sale of personal information to or from a consumer reporting agency in connection with a consumer report, to the extent the use of that information is limited by the federal Fair Credit Reporting Act.[6] The CCPA also does not apply to the extent it conflicts with the Gramm-Leach-Bliley Act and its implementing regulations.[7]

PERSONAL INFORMATION UNDER THE CCPA

The CCPA is not limited to information about "consumers," despite the title of the statute. Instead, the law applies to personal information about all California residents, including employees, customers, vendors, and contractors.

The term "personal information" incorporates the usual data types but expands the scope beyond the meaning typically associated with that term in federal and state law. Under the CCPA, personal information includes a full buffet of data types, including probabilistic identifiers that can be used to identify a particular individual or device, characteristics of protected classifications under California or federal law, commercial information, such as records of personal property, products or services purchased, obtained, or *considered*, or other purchasing or consuming histories or tendencies, biometric information, internet or other electronic network activity information (e.g., browsing and search history, and information regarding an individual's interaction with a website, application, or advertisement), geolocation data, audio, electronic, visual, thermal, olfactory or similar information, professional or employment-related

[4] § 1798.140(c).
[5] § 1798.145(c).
[6] § 1798.145(d).
[7] § 1798.145(e).

information, education information, and inferences drawn from any of the foregoing to create profiles reflecting, for example, the individual's preferences, characteristics, and psychological trends.[8]

Going beyond the individual resident, the term also includes information that could reasonably be linked, directly or indirectly, with a particular *household*.[9] Moreover, the definition of unique identifier includes a persistent identifier that can be used to recognize a *family*, or a device that is linked to a family.[10]

THE CCPA EXPANDS CALIFORNIANS' PERSONAL INFORMATION RIGHTS

The CCPA represents a significant expansion of privacy regulation in the United States. The CCPA sets forth a statutory framework that:

1) gives California residents the right to know what categories of personal information a business has collected about them;
2) gives California residents the right to know whether a business has sold or disclosed their personal information and to whom;
3) requires businesses to stop selling a Californian's personal information upon request;
4) gives California residents the right to access their personal information;
5) prevents businesses from denying equal service and price based on the exercise of the above rights; and
6) establishes a private right of action.

RIGHT TO ACCESS

Moving significantly closer to imposing General Data Protection Regulation ("GDPR")- style requirements on businesses that collect personal information of California residents, the statute establishes a new right of access, which requires businesses to disclose on request the categories and specific pieces of personal information the business has collected relating to a requesting resident.[11] If the response is in electronic format, then the information must be in a portable format, echoing the GDPR's new right to data portability.[12] Businesses must comply with these requests up to two times in a 12-month period.[13]

---

[8] *See* § 1798.140(o)(1) for "personal information" generally; see § 1798.140(x) for "unique identifier" (referring to probabilistic identifiers).

[9] § 1798.140(o)(1).

[10] § 1798.140(x).

[11] § 1798.100(d).

[12] *Id.*

[13] *Id.*

RIGHT TO DELETE

The CCPA provides a right to request that a business delete any personal information about a California resident that the business has collected from the individual.[14] A business that receives a verifiable request from a California resident to delete their personal information must delete the individual's personal information from its records and direct any service providers to do the same.[15] This right is subject to a number of exceptions, including, for example, completing a transaction with the individual, detecting security incidents, complying with legal obligations, or use for other internal purposes that align with the expectations of the individual based on the applicable relationship with the business.[16] There is no clear exception for such common business practices as data held in back-up or disaster recovery storage, however, which will make compliance more complicated.

RIGHT TO REQUEST INFORMATION

The CCPA provides the right for a California resident to request information about the categories and specific pieces of personal information that the business has collected.[17] The information businesses are required to disclose includes:

- The categories of personal information it has collected about that individual.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with which the business shares personal information.
- The specific pieces of personal information it has collected about that individual.[18]

A California resident can also request information from a business that sells personal information or that discloses the information for a business purpose, including:

- The categories of personal information that the business sold about the individual.

[14] § 1798.105(a). The California "Eraser" law already establishes a limited right to be forgotten for minors. Cal. Bus. & Prof. Code § 22581.

[15] § 1798.105(c).

[16] § 1798.105(d)(1)-(2), (7)-(8).

[17] § 1798.110(a).

[18] § 1798.110(a).

- The categories of personal information that the business disclosed about the individual for a "business purpose,"[19] which are set out in an exclusive list of use cases focused on use for internal operational purposes related to the original purpose for which the business collected the information or other compatible purposes.[20]

EXPANDED WEBSITE AND PRIVACY NOTICE REQUIREMENTS

The new act requires businesses to expand existing disclosures in their website privacy notices or other California-specific descriptions of privacy rights to include a description of an individual's rights under the CCPA and the information required to be disclosed in response to individual requests for information, including the categories of personal information collected, sold or disclosed for a business purpose as defined in the statute.[21] This information must be updated at least every 12 months.[22]

"DO NOT SELL MY PERSONAL INFORMATION"

The CCPA creates a right for a California resident to direct a business to stop selling his or her personal information to third parties[23] – which was the cornerstone of the original ballot initiative. Notably, the CCPA has an expansive definition of "sell," which includes releasing, disclosing, making available, and transferring an individual's personal information to a third party for monetary or other valuable consideration.[24] As drafted, this captures many common practices such as sharing information with digital commerce fraud detection providers for use to improve those entities' threat databases.

The CCPA requires that businesses notify individuals that their information may be sold and that they have the right to opt out.[25] While this section generally follows an opt-out regime, it requires opt-in consent from minors between the ages of 13 and 16 or from parents in the case of children under 13.[26]

Websites of businesses that sell personal information are required to post a link on their homepage titled "Do Not Sell My Personal Information," which must link to a webpage that allows an individual to opt-out.[27]

---

[19] § 1798.115(a)(2)-(3).
[20] § 1798.140(d).
[21] § 1798.130(a)(5)(A)-(C).
[22] § 1798.130(a)(5).
[23] § 1798.120(a).
[24] § 1798.140(t)(1).
[25] § 1798.120(b).
[26] § 1798.120(d).
[27] § 1798.135(a)(1).

RIGHT TO EQUAL SERVICE

The CCPA prohibits a business from discriminating against a California resident because the individual exercised any of his or her rights under the CCPA.[28] A business cannot deny goods or services to the individual, charge different prices or rates for goods or services, impose penalties, provide a different level or quality of goods or services, or suggest any of the foregoing.[29] That said, a business may charge a different price or provide a different level or quality of goods or services if that difference is reasonably related to the value provided to the individual by the individual's data.[30]

If a business enters an individual into such a financial incentive program, it must obtain prior opt-in consent (revocable at any time) from the individual that clearly describes the material terms of program.[31]

ENFORCEMENT

The CCPA does not provide the same broad private right of action as the ballot measure it replaced, which had essentially deemed any violation of the act an injury in fact. Instead, the CCPA's private right of action focuses on holding businesses accountable directly to California residents for security breaches resulting from a business's failure to implement and maintain reasonable security measures.[32] An individual can recover damages from $100 to $750 per individual per incident or actual damages, whichever is greater.[33] There is some uncertainty regarding the scope of this right to sue in the final approved version of the statute, however, as the threshold extends beyond the traditional definition of a security breach. In addition, the law in several places suggests individuals can bring a claim for violations of "this title." There is some risk, as a result, that individuals may have a right to bring a claim for violations of the statute more broadly.

A California resident wishing to file an action under the CCPA must first follow certain procedures. Prior to initiating any action against a business for statutory damages, the consumer must notify the business in question and allow 30 days to cure the noticed violation.[34] Individuals must also notify the state attorney general and follow certain procedures allowing the attorney general to prosecute the action.[35] The attorney general can pursue enforcement of any violations of the statutory provisions

[28] § 1798.125(a)(1).
[29] § 1798.125(a)(1)(A)-(D).
[30] § 1798.125(a)(2).
[31] § 1798.125(b)(1)-(3).
[32] § 1798.150(a)(1).
[33] § 1798.150(a)(1)(A).
[34] § 1798.150(b)(1).
[35] § 1798.150(b)(2)-(3).

on its own, and businesses may be liable for up to $7,500 per violation in the case of intentional conduct.[36]

KEY INITIAL TAKEAWAYS

Businesses should take time to evaluate the new California law carefully and assess the potential impact to the business. As initial takeaways, businesses should consider the following:

- Review existing privacy disclosures to evaluate potential updates mandated by the CCPA.
- Commence planning to implement the "do not sell" requirement, including cataloguing data sales and reviewing vendor agreements for other types of data sharing that will amount to a sale under the expanded definition in the statute.
- Initial planning for an inventory of data concerning California employees, customers, contractors, mobile app users, website visitors, and other residents to start feasibility planning for fulfillment of access, deletion, and do not sell requests.
- Update vendor privacy language to implement flow-down terms for the new California privacy rights.
- Identify key vendor contracts and evaluate for compliance with California standards.

[36] § 1798.155(b).

The Significance to Businesses of the California Legislature's Last Minute Revisions to the 2018 California Consumer Privacy Act

By Natasha G. Kohne, Diana E. Schaffner, Dario J. Frommer, and Jo-Ellyn Sakowitz Klein*

The California Legislature passed SB 1121 to revise certain sections of the California Consumer Privacy Act – the nation's strictest privacy protection statute which provides Californians with a right to learn what personal information certain businesses collect about them, to stop the sale of their personal information to third parties and to sue over data breaches if companies fail to adequately protect their information. The authors of this article discuss the Act and the key changes.

The California Consumer Privacy Act ("CCPA"), the nation's broadest privacy protection statute, was enacted by the California Legislature in June 2018 as part of a last-minute deal to stop a proposed statewide ballot measure that could have ushered in an even stricter privacy law.

Sponsored by San Francisco real estate magnate Alastair Mctaggart and privacy advocacy groups, the ballot measure was strongly opposed by business groups and tech interests. Racing to beat a statutory deadline for the Mctaggart measure to be placed on the ballot, the Legislature hastily passed the CCPA in June while promising to introduce cleanup legislation after the summer recess.

Efforts to substantively revise the CCPA began nearly immediately after its passage, with the AGO (the chief enforcement agency for the CCPA), business groups, and privacy activists pressing for focused changes. Those efforts coalesced around Senate Bill 1121 in August.

At the beginning of August, Senator Bill Dodd (D-Napa) amended SB 1121 to correct various technical and drafting errors contained in the CCPA.[1] After intense lobbying from business groups, banks, tech interests, and California Attorney General Xavier Becerra, additional substantive amendments were adopted.

* Natasha G. Kohne (nkohne@akingump.com) is a partner at Akin Gump Strauss Hauer & Feld LLP and co-leader of the firm's cybersecurity, privacy, and data protection practice. Diana E. Schaffner (dschaffner@akingump.com) is a counsel in the firm's litigation practice. Dario J. Frommer (dfrommer@akingump.com) is a partner in the firm's California public law and policy practice. Jo-Ellyn Sakowitz Klein (jsklein@akingump.com) is senior counsel at the firm focused on privacy and data security matters.

[1] AB 375 Chapter XX Statutes of 2018.

On August 22, Attorney General Becerra sent a letter to the co-authors of the CCPA outlining five key complaints that he had with the CCPA and asking for corresponding revisions to the CCPA.[2] Becerra opined that:

(1) businesses' and third parties' rights to seek Attorney General Office ("AGO") opinions as to CCPA compliance issues would unduly burden the AGO and could lead to a conflict with its enforcement role;

(2) the civil penalties included in the CCPA are likely unconstitutional, since they purport to amend and modify the California Unfair Competition Law's[3] civil penalty provision as applied to CCPA violations;

(3) consumers should not have to provide notice to the AGO prior to filing and pursuing their private rights of action related to data breaches;

(4) the AGO needs additional time and resources to draft CCPA regulations; and

(5) consumers should be able to bring a private right of action for any violation of the CCPA, not only for violations tied to a data breach.

Various business groups also lobbied for substantive changes to the CCPA, including:

- adding a defense to consumers' private rights of action where a business implemented an information security framework and documented its compliance with the same;
- expanding the Gramm-Leech Bliley Act ("GLBA") exemption;
- expanding the exemption relating to medical information to cover business associates;
- narrowing the definition of "personal information" to apply to information linked or linkable to a specific individual and excluding household information;
- extending the compliance deadline to 12 months after the AGO enacts its final CCPA-related regulations;
- ensuring that the statewide preemption goes into effect immediately; and
- clarifying the definition of "consumer" to exclude employees, contractors and those involved in business-to-business interactions.

On August 31, SB 1121 passed both houses of the California Legislature and approved by the governor on September 23, 2018. The key substantive changes included in SB 1121 are detailed below.

---

[2] X. Becerra Ltr. (Aug. 22, 2018.), *available at* https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical.

[3] Cal. Bus. and Prof. Code.

OVERVIEW OF CHANGES TO CCPA IN SB 1121

The revisions included in SB 1121 fall into two categories: (1) technical or grammatical revisions adopted to fix drafting errors, revise internal inconsistencies, etc.; and (2) substantive revisions that change the enforcement of the CCPA itself. This alert will focus on the latter category. SB 1121 makes the following important changes to the CCPA:

- *Extends Time for the AGO to Adopt Regulations*:[4] The deadline by which the AGO has to adopt CCPA-related regulations was extended by six months from January 1 to July 1, 2020. Attorney General Becerra requested additional time to draft and pass regulations in his August 22 letter.
- *Postpones Enforcement to the Earlier of Six Months from the Date the AGO Adopts its Regulations or July 1, 2020*:[5] In a corresponding change to that noted above, SB 1121 also extends the date on which the AGO can begin enforcing the CCPA by the *earlier* of either six months from the date that the AGO adopts its final CCPA-related regulations or July 1, 2020. Should the AGO adopt its final regulations on July 1, 2020, it appears that businesses may be faced with having to comply with those regulations on the first day that they are promulgated.
- *Makes Statewide Preemption Provision Effective Immediately*:[6] The revisions speed up enforcement of the statewide preemption provision to ensure that it takes effect immediately upon the governor signing SB 1121 into law. This revision is a direct response to local privacy protection efforts, including a ballot initiative set to go before San Francisco voters this November. The San Francisco initiative could result in a "Privacy First Policy" to which the city, its contractors and its permit holders would have to adhere. The Policy is made up of 11 principles that effectively give city residents and certain guests greater control over how their personal information is collected, stored and shared. If the initiative is passed, the city government would have to consider the Policy when drafting and proposing a privacy ordinance containing more detailed rules. SB 1121 would undercut this local effort by ensuring that the CCPA's requirements preempt certain local laws statewide.
- *Removes Various Prerequisites to a Consumer Pursuing a Private Right of Action*:[7] SB 1121 removes Subsection 1798.150(b)(2) and (3) from the CCPA, which required consumers to notify the AGO within 30 days of filing a private right of action and then outlined the potential responses of the AGO to that notice. Some of the AGO responses under Subsection 1798.150(b)(2) appeared to limit consumers' ability to pursue their private rights of action if the AGO

[4] Section 1798.185(a).
[5] Section 1798.185(c).
[6] Section 1798.199.
[7] Section 1798.150(b)(2), (3).

responded in a certain manner. In his August 22 letter, Attorney General Becerra complained of the onus that these provisions would put on the AGO and requested that they be eliminated. Should this revision be adopted, the only prerequisite a consumer will have prior to pursuing a private right of action is providing a business 30 days' notice of an alleged violation and a chance to cure.

- *Modifies the GLBA Exemption*:[8] The revised GLBA exemption eliminates the original requirement that it would apply only if the CCPA was in conflict with the GLBA (it would now apply even if there was no conflict). It also expands its protection to include personal information covered by the California Financial Information Privacy Act.[9] However, SB 1121 adds language explicitly excluding Section 1798.150, which grants a consumer a private right of action, from the exemption. Business groups sought to revise this section in an effort to simplify compliance for companies that have already undertaken significant work and expense to ensure compliance with the GLBA. It is not clear if that goal was entirely achieved, given the exclusion of the private right of action provision from the exemption.
- *Modifies Medical Information Exemptions to Expand Coverage*:[10] While the CCPA included an exemption aimed at limiting its applicability where privacy protection already existed under the California Confidentiality of Medical Information Act ("CMIA")[11] or the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 (together with their implementing regulations, "HIPAA"), the provision was poorly crafted and unduly narrow. SB 1121 overhauls this provision, making important improvements. "Medical information" as defined under and governed by CMIA is exempted. "Protected health information" as defined under HIPAA that is collected by a HIPAA-covered entity (such as a hospital or a health plan) or business associate (such as a vendor providing services for the hospital or a health plan that involve processing protected health information) is also exempted. "Providers of health care" as defined under CMIA and HIPAA-covered entities are exempted to the extent that they maintain patient information in the same manner as medical information or protected health information in accordance with CMIA and HIPAA, as applicable. Questions remain as to whether a company offering a mobile health app that collects information directly from individuals, without the involvement of a licensed health care professional, may take advantage of these exemptions. In addition, SB 1121 adds a new exemption for information

[8] Section 1798.145(e).
[9] Cal. Fin. Code § 4050 *et seq*.
[10] Section 1798.145(c).
[11] Cal. Civ. Code Part § 56 *et seq*.

collected as part of clinical trials, as long as the study was subject to certain human-research, subject-protection requirements.

- *Emphasizes the Broad Definition of Personal Information*:[12] Revisions to the existing definition of "personal information" in SB 1121 emphasize that the term was intended to apply broadly by adding additional language stating that personal information includes the various examples listed in the CCPA if "it identifies, relates to, describes, is capable of being associated with or could be reasonably linked, directly or indirectly, with a particular consumer or household." This reemphasis contrasts with requests from business groups to narrow the definition to exclude household information and to limit the definition to information that is actually linkable to a specific individual.
- *Continues Requirement for Intentional Conduct to Trigger Highest Penalty*:[13] At least one of the various iterations of SB 1121 (as amended on August 24) would have amended the CCPA to permit the AGO to seek the highest civil penalty ($7,500) for any violation of the CCPA, intentional or otherwise. However, the final version of SB 1121 reimposed the original limits in the CCPA, including a $2,500 cap for the amount that the AGO can seek for general violations and a $7,500 cap for the amount that the AGO can seek for intentional violations.

CONCLUSION

The CCPA goes into effect on January 1, 2020. It remains to be seen whether the business community will continue to push for further CCPA amendments when the Legislature returns in December. These efforts may intensify as more businesses nationwide realize the CCPA's far-reaching scope. Indeed, some estimates suggest that as many as 500,000 companies may fall under the statute. With Democrats expected to increase their large majorities in both houses of the Legislature in November, there may be little appetite to scale back CCPA consumer protections. Governor Jerry Brown (D), who was instrumental in brokering the compromise to keep the Mctaggart measure off the ballot, is also set to leave office at the end of his current term. In addition, there is a likelihood that the CCPA may further embolden other state and local governments outside of California to adopt similar measures. Getting ahead of some of these privacy issues now, before they go into full force in California, may provide businesses with the best means of driving policy development in an area that is sure to affect business practices and costs for years to come.

[12] Section 1798.140(o)(1).
[13] Section 1798.155(b).

Preparing for Ohio's Cybersecurity Safe Harbor Law

Steven G. Stransky and Thomas F. Zych*

Corporate victims of data breaches often become the targets of litigation and governmental enforcement actions, adding costly insult to serious injury. The authors of this article discuss a new Ohio law addressing this inequity by providing (limited) protection from private litigation to businesses that suffer a data breach despite their cybersecurity planning and execution.

Cyberattacks are a reality that can impact even the best-prepared business. Unfortunately, corporate victims of data breaches often become the targets of litigation and governmental enforcement actions, adding costly insult to serious injury. The Ohio legislature has addressed this inequity by providing (limited) protection from private litigation to businesses that suffer a data breach despite their cybersecurity planning and execution.

Beginning November 2, 2018, businesses will have the ability to invoke a cybersecurity safe harbor provision pursuant to Ohio law (SB 220) to obtain tort-related liability protection if they suffer a data breach. Businesses can undertake simple measures to efficiently and effectively avail themselves of Ohio's cybersecurity safe harbor.

BACKGROUND ON SB 220

What Does the Cybersecurity Safe Harbor Protect Against?

Pursuant to SB 220, a "covered entity" that has adopted a written cybersecurity program may raise an affirmative defense to any tort action alleging that its "failure to implement reasonable information security controls resulted in a data breach" involving either personal information or restricted information. In other words, this safe harbor will enable businesses that have implemented appropriate cybersecurity programs to counter allegations of tort liability due to a data breach. This often occurs when plaintiffs initiate negligence or privacy-related claims after their personal information is compromised in a data breach. However, the safe harbor does not protect against liability for violating contractual obligations (e.g., contractual provisions governing data protection) or alter any other obligation that a business may have to

* Steven G. Stransky is senior counsel in Thompson Hine's Business Litigation, Privacy & Cybersecurity, and Government Contracts groups, advising clients on national and international privacy and information security issues. Thomas F. Zych is a partner at the firm, chair of the Emerging Technologies Practice, and head of the Privacy & Cybersecurity team, focusing on a range of data protection, intellectual property, consumer protection, social media, competition, and antitrust matters. The authors may be reached at steve.stransky@thompsonhine.com and tom.zych@thompsonhine.com, respectively.

report the data breach to affected individuals, government or regulatory agencies, or any other entity.

Who Can Invoke the Safe Harbor?

SB 220 applies to a "covered entity," which is defined as any type of business, including a nonprofit organization that "accesses, maintains, communicates, or processes" personal or restricted information "in or through one or more systems, networks, or services." SB 220 incorporates the definition of "personal information" from Ohio's data breach notification law, which defines it as an individual's name (i.e., first name or first initial and last name) linked to a Social Security number, driver's license or state identification number, or financial account or credit card data. In contrast, the term "restricted information" means "any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual."

Generally, the definitions of personal and restricted information exclude data that is unreadable (e.g., encrypted or redacted) and would not cause any harm or risk to individuals in the event that either is compromised in a data incident. SB 220 provides safe harbor only to data breaches involving electronic documents and does not provide any liability protection in the event that physical (i.e., hard-copy) documents or records are lost, stolen, or otherwise compromised.

How to Qualify for the Safe Harbor?

In order to invoke the Ohio cybersecurity safe harbor provision, a business must "create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards" to protect personal information (or personal and restricted information) and that "reasonably conforms to an industry recognized cybersecurity framework." The law identifies, among others, the following as acceptable industry recognized cybersecurity frameworks:

- The Framework for Improving Critical Infrastructure Cybersecurity – developed by the National Institute of Standards and Technology ("NIST");
- NIST Special Publication 800-171;
- The Federal Risk and Authorization Management Program Security Assessment Framework;
- ISO/IEC 27000, Information Security Management Systems;
- The Health Insurance Portability and Accountability Act's security rule; and
- The Payment Card Industry Data Security Standard.

The law provides some context to the "reasonably conforms" criterion by stating that the "scale and scope" of a covered entity's cybersecurity program "is appropriate" if it is based on the following: the size and complexity of the covered entity; the nature and

scope of the covered entity's activities; the sensitivity of the information; the cost and availability of tools to improve information security and reduce vulnerabilities; and the resources available to the covered entity.

STRATEGIZE AND LEVERAGE YOUR EXISTING CYBERSECURITY EFFORTS

To effectively and efficiently avail themselves of Ohio's cybersecurity safe harbor, businesses should (1) consolidate their existing cybersecurity measures, (2) identify which of the above-mentioned cyber standards set forth in SB 220 most closely aligns with their current cybersecurity program, and (3) update their cybersecurity practices to satisfy any outstanding requirements.

Consolidate Existing Cybersecurity Measures

SB 220 does not require businesses to establish any particular cybersecurity program, nor does it create new liability for failing to do so. Rather, the purpose of the law is to incentivize businesses to proactively implement cybersecurity measures to protect personal data under their control. Many businesses have already implemented some technical, physical, and administrative data security measures to protect corporate data (e.g., trade secrets, protected health information, intellectual property). For example, businesses routinely use encryption protocols, firewalls and other technical programs to safeguard corporate data, as well as incident response procedures, confidentiality requirements and other administrative security measures. However, these safeguards, plans and policies may have been generated and implemented in a disparate and inconsistent manner. The safe harbor provision requires these policies be reviewed and consolidated under a unified – and written – cybersecurity program.

Identify Where Your Program Aligns

Once a business determines the scope of its existing cybersecurity program, it should compare and contrast it to the acceptable cybersecurity frameworks set forth in SB 220 to identify the framework with which it most closely aligns. Thereafter, it will be better positioned to more narrowly create and implement the remaining elements of the cybersecurity framework needed to satisfy the safe harbor provision. Separately, for businesses that are already subject to an acceptable cybersecurity framework set forth in SB 220, they may simply need to expand their existing cyber program to cover personal information in their possession. For example, businesses that have a medical benefits plan that is subject to HIPAA will have likely implemented several of the cybersecurity measures required by the HIPAA security rule. Similarly, government contractors processing defense-related information will have likely already satisfied NIST 800-171 requirements pursuant to federal acquisition regulations. If these businesses simply expand their security controls from their existing scope (e.g.,

protected health information, covered defense information) to address all personal information, then they would be able to rely upon Ohio's safe harbor law.

Satisfy Outstanding Requirements

Once a business determines the acceptable cybersecurity framework with which it most closely aligns, it should implement any outstanding physical, technical, and administrative measures needed in order to satisfy the framework's remaining requirements. In addition, to ensure that a business can rely upon the safe harbor provision, it will need to establish an internal or external process to continuously monitor its cybersecurity program for compliance purposes.

CONCLUSION

Cyberattacks against the private sector continue to increase in scope and sophistication, and the Ohio law provides a valuable safe harbor to businesses that proactively build a cybersecurity program.

Data Privacy: Developments in Regulatory Enforcement

Mark C. Mao and Ronald I. Raether Jr.*

This article reviews developments in privacy regulatory enforcement, noting that the Office of Civil Rights and the Department of Health and Human Services continue to impose the highest fines per consumer through regulatory enforcement.

Perhaps due in part to the heightened international focus on privacy law, regulators in the United States are taking aggressive stances on privacy practices, many of which have been responsible for the technological growth in the United States these past two decades.

It is important to note that while the Federal Trade Commission ("FTC") and state attorneys general ("AGs") continue to be very active, the Office of Civil Rights ("OCR") and the Department of Health and Human Services ("HHS") continue to impose the highest fines per consumer through regulatory enforcement.

THE FEDERAL TRADE COMMISSION

In re VTech

In January 2018, the FTC entered into a $650,000 settlement with toymaker VTech for allegedly collecting personal information from hundreds of thousands of children without providing direct notice and obtaining their parents' consent, and for allegedly failing to take reasonable steps to secure the data.[1]

In re Prime Sites, Inc.

In February 2018, Prime Site, Inc. settled FTC charges that it violated Children's Online Privacy Protection Act ("COPPA") by collecting information of children under the age of 13 without proper parental consent and that it violated the FTC Act by misrepresenting benefits of an upgraded membership. The FTC alleged that Prime Site collected information of more than 100,000 users who were registered as under age 13, although its privacy policy stated it did not knowingly collect information of children under 13. Prime Site agreed to pay a civil penalty of $500,000, to be suspended upon

* Mark C. Mao is a partner at Troutman Sanders LLP focusing primarily on intellectual property and data privacy. Ronald I. Raether, Jr., is a partner at the firm leading the Cybersecurity, Information Governance and Privacy practice group, and is a member of the firm's Financial Services Litigation group. The authors may be reached at mark.mao@troutman.com and ron.raether@troutman.com, respectively.

[1] Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act, FTC (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

payment of $235,000. Prime Site also agreed to comply with COPPA requirements in the future and to delete information previously collected from children under the age of 13.[2]

In re Sears Holding Management

In February 2018, the FTC approved a petition by Sears Holdings Management Corporation to reopen and modify a 2009 FTC order, whereby Sears settled charges by the FTC that it deceptively failed to disclose the extent of its software's data collection. The 2009 FTC Order required Sears to provide clear and prominent notice of any "Tracking Application" and to obtain express consent before downloading or installing the software. The FTC agreed with Sears' petition that changed conditions justified updating the definition of "Tracking Application," to exclude software that tracks configuration or software or application, information regarding whether the software or application is functioning as represented, or information regarding consumers' use of the software or application itself.[3]

In re PayPal, Inc.

The FTC alleged that Venmo failed to disclose material conditions of external transfers and misled consumers about their privacy controls. Venmo also allegedly violated Gramm-Leach-Bliley Act ("GLBA") by misrepresenting the "bank grade security system" protections. Venmo is now prohibited from making material misrepresentations regarding its services, privacy controls, and security levels. Venmo must also make certain disclosures to consumers, is prohibited from violating GLBA, and must obtain biennial third-party assessments of its compliance with the settlement for 10 years.[4]

In re ReadyTech

In July 2018, the FTC settled with ReadyTech Corporation, which provides online training services, over allegations that ReadyTech violated Section 5 of the FTC Act by falsely claiming it was in the process of certifying compliance with the U.S.-EU Privacy Shield Framework. The FTC alleged that while ReadyTech initiated an application

[2] Press Release, Online Talent Search Company Settles FTC Allegations it Collected Children's Information without Consent and Misled Consumers, FTC (Feb. 5, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/online-talent-search-company-settles-allegations-it-collected.

[3] FTC Approves Sears Holdings Management Corporation Petition to Reopen and Modify Commission Order Concerning Tracking Software, FTC (Feb. 28, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/ftc-approves-sears-holdings-management-corporation-petition.

[4] FTC Gives Final Approval to Settlement with PayPal Related to Allegations Involving its Venmo Peer-to-Peer Payment Service, FTC (May 24, 2018), https://www.ftc.gov/news-events/press-releases/2018/05/ftc-gives-final-approval-settlement-paypal-related-allegations; PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act, FTC (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

with the U.S. Department of Commerce, it did not complete the required steps for certification. As a result of the settlement, ReadyTech is prohibited from misrepresenting its participation in any government or industry sponsored privacy or security program and is also now required to comply with standard reporting and compliance requirements.[5]

In re BLU Products, Inc.

In September 2018, the FTC settled with mobile phone manufacturer, BLU Products, Inc., and its co-owner, over allegations that they made misrepresentations to consumers regarding their data collection and disclosure practices as well as their data security practices. The FTC further alleged that they failed to oversee their service providers and failed to implement appropriate security procedures, which resulted in the third party collecting more information from consumers than was necessary. As part of the settlement, BLU and its co-owner are prohibited from misrepresenting their data privacy and security practices and are required to maintain a comprehensive security program. BLU will undergo third-party assessments of its security programs for 20 years and be subject to record keeping and compliance monitoring requirements.[6]

HIPAA ENFORCEMENT

In re Fresenius Medical Care

In February 2018, the medical care group agreed to pay $3.5 million for five data breaches at five of its locations in 2012. This was one of the largest Office for Civil Rights consent decrees of all time.[7]

In re Filefax, Inc.

In February 2018, Filefax settled charges with OCR over allegations that Filefax violated HIPAA by failing to properly safeguard protected health information ("PHI"). Filefax allegedly allowed an unauthorized individual to transport PHI to a shredding facility, but left the PHI in an unlocked truck and left it unsecured outside Filefax's facility. Although Filefax closed its doors during the OCR investigation, it was still

[5] California Company Settles FTC Charges Related to Privacy Shield Participation, FTC (July 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/california-company-settles-ftc-charges-related-privacy-shield.

[6] FTC Gives Final Approval to Settlement with Phone Maker BLU, FTC (Sept. 10, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu?utm.

[7] Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules, U.S. Dep't Of Health & Human Services (Feb. 1, 2018), https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.

found liable for its failure to comply with the law. Filefax agreed to pay $100,000 and to properly store and dispose of the remaining PHI in compliance with HIPAA.[8]

In re EmblemHealth

In March 2018, EmblemHealth settled charges brought against it by the New York attorney general alleging that Emblem Health violated HIPAA's requirement to safeguard PHI and also violated New York's general business law by including policy holders' Social Security numbers on mailing labels of mail sent to them. EmblemHealth agreed to pay $575,000 and to conduct a comprehensive risk assessment.[9]

In re Virtua Medical Group

In April 2018, Virtua Medical Group entered into a consent decree with the New Jersey attorney general and the New Jersey Division of Consumer Affairs involving allegations that Virtua violated HIPAA and the New Jersey Consumer Fraud Act when the medical records of 1,650 patients were viewable on the internet due to a server misconfiguration by a third-party vendor. Allegedly, the third-party vendor inadvertently changed the web server when updating the software and allowed the FTP site hosting electronic protected health information ("ePHI") to be accessed without a password. While the exposure was a result of the third-party vendor, the New Jersey attorney general and the New Jersey Division of Consumer Affairs held Virtua responsible as the owner of the data and therefore responsible for its protection. Virtua was also alleged to have violated HIPAA by failing to implement security awareness and training, implementing procedures relating to the ePHI maintained on its FTP site, and failing to maintain a written log of each time the FTP Site was accessed. Virtua agreed to pay civil penalties of $417,816, implement remediation measures, and report on such implementation to the Division 180 days after the settlement and every two years thereafter.[10]

In re University of Texas MD Anderson Cancer Center

A U.S. Department of Health and Human Services administrative law judge ("ALJ") granted OCR's motion for summary judgment, finding that MD Anderson violated

---

[8] Consequences for HIPAA violations don't stop when a business closes, U.S. Dep't Of Health & Human Services (Feb. 13, 2018), https://www.hhs.gov/about/news/2018/02/13/consequences-hipaa-violations-dont-stop-when-business-closes.html.

[9] Allison Grande, NY AG Announces EmblemHealth Data Breach Settlement, LAW360 (Mar. 6, 2018), https://www.law360.com/articles/1019179/ny-ag-announces-emblemhealth-data-breach-settlement; A.G. Schneiderman Announces $575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers, New York State Office of The Attorney General (Mar. 6, 2018), https://ag.ny.gov/press-release/ag-schneiderman-announces-575000-settlement-emblemhealth-after-data-breach-exposed.

[10] Virtua Medical Group Agrees to Pay Nearly $418,000, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Medical Treatment Files of Patients, New Jersey Office of The Attorney General (April 4, 2018), https://nj.gov/oag/newsreleases18/pr20180404b.html.

HIPAA and required MD Anderson to pay penalties to OCR in the amount of $4,348,000. OCR investigated MD Anderson following three separate breaches of unencrypted devices. OCR concluded that while MD Anderson had written encryption policies and MD Anderson's own risk assessments noted that lack of device-level encryption posed significant risks of exposure of ePHI, MD Anderson nevertheless failed to timely adopt an enterprise-wide solution and failed to encrypt its devices. The ALJ rejected MD Anderson's arguments that it was not obligated to encrypt the devices and that the ePHI was for research and therefore not subject to HIPAA's nondisclosure requirements.[11]

STATE AG ENFORCEMENT

New York

In January 2018, the New York attorney general and a healthcare provider entered into a $1.15 million deal to end an investigation alleging it risked revealing the HIV status of 2,460 New Yorkers by mailing them information in transparent window envelopes.[12]

California

In March 2018, a major retailer settled charges by the California attorney general alleging that the retailer failed to properly manage disposal of hazardous materials and customer information, giving it an unfair advantage over its rivals. The parties settled for $27.84 million and a permanent injunction against similar violations.[13]

Massachusetts v. Equifax Inc.

In April 2018, a superior court judge denied Equifax's motion to dismiss the Massachusetts attorney general's action against it, holding that the Massachusetts AG plausibly alleged that Equifax's failure to act on a known issue with respect to its data security violated Massachusetts's Standards for the Protection of Personal Information of Residents of the Commonwealth.[14]

---

[11] Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations, U.S. Dep't Of Health & Human Services (June 18, 2018), https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html.

[12] A.G. Schneiderman Announces Settlement With Aetna Over Privacy Breach of New Yorker Members' HIV Status, New York State Office of The Attorney General (Jan. 23, 2018), https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-aetna-over-privacy-breach-new-york-members-hiv.

[13] Mike Mills & Shannon Morrissey, Another Hazardous Waste Enforcement Action Costs a Major Retailer Millions, *California Environmental Law* (Mar. 21, 2018) https://www.californiaenvironmentallawblog.com/environmental-contamination/another-hazardous-waste-enforcement-action-costs-a-major-retailer-millions/.

[14] Kat Greene, Equifax Can't Skip Mass. AG Suit Alleging Security Failures, LAW360 (April 4, 2018), https://www.law360.com/articles/1030065/equifax-can-t-skip-mass-ag-suit-alleging-security-failures.

In re Meitu Inc.

In May 2018, Meitu and the New Jersey attorney general signed a consent order involving allegations that Meitu violated the Children's Online Privacy Protection Act by collecting their personally identifiable information through their photo-editing apps without obtaining verifiable consent from parents or guardians of children under the age of 13. Meitu agreed to pay a penalty of $100,000 and agreed to provide clear and conspicuous notice of its privacy policy with notice of its information collection, use, and disclosure practices; to obtain verifiable consent from parents prior to collection, use, or disclosure; and to comply with COPPA's requirements.[15]

Multi-State Agencies adv. Equifax Inc.

In June 2018, Equifax Inc. entered into a consent decree with multi-state regulatory agencies resulting from the 2017 Equifax data breach. The Order requires Equifax to take a number of compliance measures, including reviewing and improving information security, improving oversight of the audit program, improving oversight and documentation of critical vendors and ensure sufficient controls to safeguard information consistent, improve standards for supporting patch management, and enhance oversight of IT operations relating to disaster recovery. The Equifax Board is required to submit to the Multi- State Regulatory Agencies a list of all remediation projects in response to the 2017 breach and must have independent third-party test controls relating to such projects and provide an update to the Multi-State Regulatory Agencies by December 31, 2018. The Order is effective until it has been suspended, terminated, modified, or set aside by the Multi-State Regulatory Agencies.[16]

In re Unixiz

In August 2018, the New Jersey attorney general settled with Unixiz, the company that owned and operated the online social website "i-Dressup," alleging that it had violated COPPA and state consumer protection statutes, by failing to properly secure information and obtain verifiable parental consent. The investigation was initiated after media outlets began reporting that the website had been breached by an unknown hacker. In addition to injunctive relief, the company also agreed to pay $98,618 in civil penalties.[17]

---

[15] Jeannie O'Sullivan, App Developer Collected Kids' Personal Info, NJ AG Says, LAW360 (May 8, 2018), https://www.law360.com/articles/1041526/app-developer-collected-kids-personal-info-nj-ag-says; NJ Division of Consumer Affairs Announces $100,000 Settlement with App Developer Resolving Investigation Into Alleged Violations of Children's Online Privacy Law, New Jersey Office of The Attorney General (May 8, 2018), https://nj.gov/oag/newsreleases18/pr20180508a.html.

[16] Consent Order, New York State Dep't of Financial Services (June 27, 2018), *available at* https://www.dfs.ny.gov/about/ea/ea180627.pdf.

[17] Operator of Teen Social Website Breached by Hacker Agrees to Close Site and Reform Practices to Settle Allegations it Violated Children's Online Privacy Protection Act, New Jersey Office of The Attorney General, Aug. 3, 2018), https://nj.gov/oag/newsreleases18/pr20180803a.html.

In re LightYear Dealer Technologies LLC

In September 2018, the New Jersey attorney general settled with data management company LightYear Dealer Technologies LLC *dba* DealerBuilt as a result of a data breach that exposed personal information of car dealership customers.

The personal data included names, addresses, social security numbers, driver's license numbers, and bank account information. DealerBuilt agreed to implement and maintain an information security program to be managed by a chief information security officer and to maintain proper encryption protocols for portable devices, among other requirements. DealerBuilt also agreed to pay $80,785, of which $49,420 is for civil penalties; the remainder is for attorneys' fees, investigation costs, and expert fees.[18]

In re Tiny Lab Productions et al.

In September 2018, the New Mexico attorney general filed suit against gaming company Tiny Lab Productions, alleging that it mislabeled its game as not being targeted towards children, in contravention of COPPA. In addition, the attorney general filed suit against one of the mobile application store owners for offering the game, notwithstanding the alleged COPPA violations, in addition to a number of ad tech and ad exchanges, for embedding their SDKs within the game.[19] Although it is far from clear that any of the defendants will ultimately have liability, the case is important for all ad tech companies, ad exchanges, and ecosystem owners to note. It appears that the New Mexico attorney general has decided to take up the mantle formerly undertaken by the New York attorney general, to not only investigate application "backdoors," but to also hold ecosystem owners liable.

OTHER ADMINISTRATIVE ENFORCEMENT EFFORTS

In February 2018, the North American Electric Reliability Corp. ("NERC") reached a settlement with an unnamed power company to resolve two violations alleging failure to protect critical cyber assets. Allegedly, a third-party contractor of the power company improperly copied data to its unprotected network. The data included IP addresses and host names, as well as other critical cyber assets. The data was exposed for 70 days, though there was no evidence anyone other than a researcher, who tipped off

[18] Bill Wichert, Software Co. Settles Auto Dealer Data Breach Claims in NJ LAW360 (Sept. 7, 2018), https://www.law360.com/cybersecurity-privacy/articles/1080689/software-co-settles-auto-dealer-data-breach-claims-in-nj?nl_pk=d100b429-aa27-499d-ad44-acee4f8fe74b&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

[19] Valentino-DeVries et al., How Game Apps That Captivate Kids Have Been Collecting Their Data, *The New York Times* (Sept. 12, 2018), https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html; *see also* Complaint, *State of New Mexico ex rel Hector Balderas, Attorney General v. Tiny Lab Productions et al.*, No. 18-00854 (D. New Mexico filed Sept. 11, 2018).

the NERC, had downloaded the data. The power company self-reported the breach, agreed to a $2.7 million penalty, and to carry out a mitigation plan to improve its security systems.[20]

In re AMP Global Clearing LLC

In February 2018, the U.S. Commodities Futures Trading Commission ("CFTC") settled charges against a futures commission merchant, AMP Global Clearing LLC, for its failure to diligently supervise an IT provider's implementation of its written information security program, resulting in a data breach of customer records and information. The vulnerability existed for 10 months, and an unauthorized actor had even blogged about exploiting the vulnerability. AMP paid $100,000 in penalties and agreed to cease and desist from future violations of the Regulation.[21]

In re Mizuho Securities USA LLC

In July 2018, the SEC settled charges against Mizuho Securities USA LLC for alleged failures to safeguard information, including failing to maintain and enforce policies and procedures aimed at preventing misuse of material nonpublic information. The SEC charged Mizuho for regularly disclosing material nonpublic customer information to other traders and to its hedge fund clients in violation of Section 15(g) of the SEC Act of 1934. The settlement included a penalty of $1.25 million, a censure, and a cease and desist order from committing future violations.[22]

---

[20] Keith Goldberg, Power Co. Fined $2.7M For Exposing Critical Grid Data, LAW360 (Mar. 5, 2018), https://www.law360.com/articles/1018678/power-co-fined-2-7m-for-exposing-critical-grid-data; NERC Full Notice of Penalty Regarding Registered Entity, FERC Docket No. NP18-_-000, North American Electric Reliability Corporation (Feb. 28, 2018), *available at* https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf.

[21] CFTC Brings Cybersecurity Enforcement Action, Hunton Privacy & Information Security Law Blog (Feb. 14, 2018), https://www.huntonprivacyblog.com/2018/02/14/cftc-brings-cybersecurity-enforcement-action/; George Lynch & Daniel R. Stoller, Futures Regulator, Broker Settle Lax Cybersecurity Charges, Bloomberg BNA (Feb. 15, 2018), https://www.bna.com/futures-regulator-broker-n57982088869/.

[22] SEC Charges Mizuho Securities for Failure to Safeguard Customer Information U.S. Securities and Exchange Comm'n (July 23, 2018), *available at* https://www.sec.gov/news/press-release/2018-140.

Judge Grants Summary Judgment in Favor of OCR for HIPAA Violations Ordering a Texas Cancer Center to Pay $4.3 Million in Penalties

Marcia L. Augsburger*

The author of this article discusses an administrative law judge's ruling that the U.S. Department of Health and Human Services and its Office for Civil Rights properly imposed penalties against MD Anderson Cancer Center for failing to encrypt laptops and USB thumb drives, in violation of the Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rules.

The U.S. Department of Health and Human Services ("HHS") and its Office for Civil Rights ("OCR") announced an Administrative Law Judge's ("ALJ") ruling that OCR properly imposed penalties against The University of Texas MD Anderson Cancer Center ("MD Anderson") for failing to encrypt laptops and USB thumb drives, in violation of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy and Security Rules. One reason this decision is significant is that it may resolve an unsettled question: Is the use of encryption mandatory in the Security Rule? HHS's short answer has been "No," but based on the ALJ opinion, its long answer equates to "Yes" – at least when covered entities and business associates decide that encryption is necessary.

BACKGROUND

By way of background, whether encryption is required has long been unclear. For example, on the HHS website in response to the frequently asked question "Is the use of encryption mandatory in the Security Rule?," HHS first states "No," but then qualifies this answer: "The encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI."[1] The regulation adds to the confusion, stating in pertinent part at 45 C.F.R. § 164.312(a)(2):

* Marcia L. Augsburger, a partner in King & Spalding LLP's FDA and Life Sciences and Healthcare practices, handles investigations, complex litigation, and appeals involving fraud and abuse, unfair business practices, contracting and constitutional issues. She may be reached at maugsburger@kslaw.com.

[1] https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html.

A covered entity or business associate must, in accordance with § 164.306:

> (a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
>
> (2) ***Implementation specifications:*** . . .
>
> (iv) ***Encryption and decryption (Addressable).*** Implement a mechanism to encrypt and decrypt electronic protected health information. (Emphasis and italics in original.)

Subsection (2)(iv) seems to mandate encryption. Indeed, it does not contain the more flexible language that subsection (e)(2)(ii) includes regarding transmission of PHI: "***Encryption (Addressable).*** Implement a mechanism to encrypt electronic protected health information *whenever deemed appropriate*." (Emphasis added). However, encryption is "addressable" under both subsections, and therefore not mandatory unless a risk assessment indicates it is reasonable and appropriate.

Adding to the confusion, Commentators and OCR itself have said that because encryption is now easily and inexpensively implemented, it must be considered reasonable and appropriate and therefore required and not simply a safe-harbor.

This was not, however, an argument OCR made in support of its imposition of penalties against MD Anderson. In fact, OCR noted, and the ALJ confirmed, that the regulations governing ePHI do not specifically require encryption. The ALJ added that covered entities have "considerable flexibility" in deciding how to protect ePHI.

THREE INCIDENTS

Nonetheless, the ALJ ruled that OCR properly imposed penalties against MD Anderson for failing to encrypt data on all laptops and other devices. The penalties resulted from an investigation based on three incidents: On April 30, 2012, someone stole a "telework" laptop computer from an MD Anderson clinician's home; on July 13, 2012, a trainee lost, on an employee shuttle bus, a USB thumb drive that her supervisor authorized her to take home; and on or after November 27, 2013, a visiting researcher also lost an USB thumb drive containing ePHI. The laptop contained PHI relating to almost 30,000 individuals and was neither encrypted nor password protected. The trainee's thumb drive was not encrypted and it contained ePHI relating to more than 2200 individuals. The researcher's unencrypted thumb drive contained information relating to about 3600 patients. However, these incidents were not in issue – or at least the penalties did not appear to be based on any determination that the incidents posed an appreciable risk of compromise constituting a breach.

THE OPINION

OCR's imposition of penalties and the ALJ's decision turned on the evidence that MD Anderson recognized the need to encrypt data as early as 2006, determined that all devices should be encrypted, but then failed to promptly encrypt all of them. The ALJ opinion recites that MD Anderson consistently stated that confidential data must be protected against loss or theft; repeatedly announced a policy that both required encryption of confidential data and prohibited unsecured storage of such data; announced in 2008 that it intended to implement the first phase of a media security project that would test and implement encryption of institutional computers, but then delayed encryption and, according to the ALJ, "proceeded with encryption at a snail's pace," putting the process on hold in 2009 due to financial constraints. The opinion further recites that in 2010, citing the theft of a laptop and other incidents, MD Anderson's director of information security proposed restarting efforts to encrypt laptops, but nothing was done until August 2011 and that as of November 2013, more than 10 percent of MD Anderson's computers remained unencrypted. However, these facts were largely unrelated to the penalties, which inexplicably ran from March 24, 2011 through January 25, 2013.

While OCR and the ALJ may have considered MD Anderson's financial and other reasons for delaying encryption as evidence that encryption of all devices was not then reasonable and appropriate, the ALJ did not say so. Moreover, no explanation is provided as to what, if anything, changed on March 24, 2011, and the decision appears to be based largely on the 2006 through 2010 occurrences described above. The ruling is based on the ALJ's opinion that once MD Anderson identified encryption as necessary and appropriate to reduce risk and implemented policies to ensure mobile devices were encrypted, encryption became a "self-imposed" duty subject to enforcement and penalties for non-compliance – even if circumstances changed over time rendering encryption unreasonable.

> These facts establish that Petitioner, a comprehensive cancer center that operates both inpatient and outpatient facilities in the Houston, Texas area, was not only aware of the need to encrypt devices in order to assure that confidential data including ePHI not be improperly disclosed, but it established a policy requiring the encryption and protection of devices containing ePHI. . . . [D]espite this awareness and its own policies, Petitioner made only half-hearted and incomplete efforts at encryption over the ensuing years. As a consequence, the theft of a laptop computer that was not encrypted and the loss of two unencrypted USB thumb drives resulted in the unlawful disclosure of ePHI relating to tens of thousands of Respondent's patients.

However, again, the penalties did not run from the establishment of policies. Moreover, the ALJ suggested encryption was not the only choice, stating: "However, the bottom line is that whatever mechanisms an entity adopts must be effective." Indeed,

the ALJ acknowledged that "[n]othing in th[e] regulations directs the use of specific devices or specific mechanisms by a covered entity."

MD Anderson contended that it was not required by regulation to encrypt its devices because 45 C.F.R. § 164.312(a)(2)(iv) only required that it "implement a mechanism to encrypt and decrypt electronic protected health information." The cancer center argued it met this requirement by adopting and implementing a "mechanism" that included password protection of all computers that accessed potentially confidential information; an encryption requirement for confidential or protected data stored on portable computing devices; and annual employee training event that provided its employees with training about password necessity and integrity, among other relevant topics.

OCR relied on 45 C.F.R. § 164.312(a)(1), which states: "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights . . . ." OCR asserted that MD Anderson violated the regulatory requirements because it failed to ensure that encryption of all laptop computers and USB drives. The ALJ agreed with OCR that the regulations require covered entities to "assure that all systems containing ePHI be inaccessible to unauthorized users."[2] While these statements fall short of saying encryption is required, they express that this was OCR's and the ALJ's position. This is especially apparent from the placement of the ALJ's findings in discussions about encryption, including for example: "[MD Anderson] failed to comply with regulatory requirements because it failed to adopt an effective mechanism to protect its ePHI [and going on to discuss encryption]."

Thus, the ALJ's focus on MD Anderson's acknowledgements between 2006 and 2010 that it should encrypt does not resolve the regulatory ambiguities. Further, the ALJ's internally inconsistent analysis arguably creates more confusion in that on the one hand the ALJ acknowledged that encryption was not necessarily required while on the other, the ALJ penalized for failing to encrypt. Holding that the duty was "self-imposed" does not provide clarification in the context either. If a duty is "self-imposed," an entity may conclude at various times that it is unreasonable to encrypt or to continue encrypting, thus relieving it of its "self-imposed" duty. In fact, MD Anderson was not penalized for failing to encrypt as set forth in its policies. While the opinion does not explain why the penalties ran from March 24, 2011 the opinion suggests that OCR chose March 24, 2011 as the first day of the violations to be "reasonable." And certain statements by the ALJ suggest a conclusion that there were time before March 24, 2011 when MD Anderson was "compliant," which may mean that during that period MD Anderson reasonably concluded encryption was not reasonable and appropriate under the circumstances.

[2] Citing 45 C.F.R. § 164.306(a); 45 C.F.R. § 164.312(a)(1).

For these reasons, the ALJ decision may have no precedential value in terms of guiding future encryption behaviors. At most, but nonetheless significantly, the decision certainly indicates that OCR may take the position that encryption is required if it is reasonable and appropriate under the circumstances or if an entity decides at any time that all devices should be encrypted and they are not at the time a potential breach occurs. This confirms what we knew before.

SUMMARY

To summarize, the ALJ decision instructs that devices containing or accessing ePHI should be encrypted promptly after the entity determines that encryption is a reasonable and appropriate safeguard. It further informs that password protection will not be sufficient if the entity has decided encryption is reasonable and appropriate. The decision does not address situations where entities do not decide to encrypt or whether encryption is reasonable and appropriate in all cases. However, OCR's argument indicates it will likely rely on 45 C.F.R. § 164.312(a)(1) to require encryption where a covered entity or business associate fails to implement available safeguards to limit access only to those who are granted access rights.

RECOMMENDATIONS

Covered entities and business associates first fully and credibly analyze whether encryption of computers, thumb drives and similar devices, including cell phones that access PHI, is reasonable and appropriate, giving at least some consideration to OCR's position that encryption is required in at least some cases. If the entity decides encryption is reasonable and appropriate, staff should make sure that what they propose for implementation is achievable, and then ensure that their stated goals are achieved. If encryption is not reasonable or circumstances make it unreasonable, the reasons for such conclusions should be carefully and accurately documented. If encryption will occur over time or a decision is made not to encrypt, covered entities and business associates should also do everything possible to make sure that all systems containing ePHI are inaccessible to unauthorized users.[3]

[3] The ALJ's full opinion is available at https://www.hhs.gov/sites/default/files/alj-cr5111.pdf.