April 26, 2019

What's trending on NP Privacy Partner

California lawmakers work to fix some ambiguities in the landmark legislation, Amazon opens its "HIPAA-eligible" environment to certain Alexa skills and more. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

Clarity for the California Consumer Privacy Act? California lawmakers work to fix some ambiguities in the landmark legislation

We've previously discussed the ambiguities throughout California's landmark privacy legislation, the California Consumer Privacy Act (the "CCPA"). The CCPA, passed in June 2018, creates several privacy rights for Californians. However, as the January 1, 2020 effective date looms ahead, many hoped that the California Assembly Privacy and Consumer Protection Committee (the "Committee") would clarify several compliance provisions. Fortunately, this past Tuesday, April 23, the Committee did just that. Significantly, the Committee clarified the following:

- Employees are not "consumers" for purposes of the CCPA, as long as the personal data is collected and used only in the employment context. In the case of contractors, a written agreement must be in place.

- Personal Information does not include all "information that is … capable of being associated" with a particular individual or household, but just information that is "reasonably capable" of being associated.

- Information found in the public record is exempted from the definition of "personal information."

- De-identified data means data that does not identify and is not reasonably linkable, directly or indirectly, to a specific consumer, so long as the business makes no attempt to re-identify the data and takes reasonable measures to: (1) ensure that the data remains de-identified; (2) publicly commit to maintain and use the data in its de-identified form; and (3) require by contract that any recipients of the data maintain the de-identified form. This clarification will likely motivate businesses to maintain data in a de-identified form to limit liability under the CCPA.

- Loyalty programs are exempt from the CCPA's "non-discrimination" restrictions.

These bills now must be considered by the Senate Judiciary Committee before they become law and are incorporated into the CCPA. –*Jenny L. Holmes*

Data Breach

Second try's the charm? Yahoo ups data breach settlement offer to $117.5M.

If approved by the U.S. District Court for the Northern District of California, the $117.5 million settlement agreement proposed by Yahoo on Wednesday will establish the largest common fund ever obtained in a data breach case.

In December 2016, Yahoo announced that login information for over 1 billion of its customer accounts had been stolen in August 2013. However, in October 2017, the company disclosed that an investigation by outside forensic experts revealed that all 3 billion accounts existing at the time had been impacted—making it one of the largest data breaches ever. The stolen information included users' names, e-mail address, telephone numbers, dates of birth, security questions and answers and hashed passwords created using the MD5 algorithm, a process known to be vulnerable to brute force and hash collision attacks.

Victims filed a class action lawsuit alleging that Yahoo did not use appropriate safeguards to protect users' personal information and deliberately failed to notify users that their personal information had been stolen. The suit also captures two smaller data breaches that occurred in 2014 and 2016. The proposed settlement would fund two years of credit monitoring for all class members and reimbursement for out-of-pocket expenses related to identity theft, lost time, paid user costs and small business costs, as well as attorney's fees and costs and expenses, service awards for class representatives and notice and administration costs.

Yahoo and plaintiffs initially agreed to a settlement of $50 million, plus attorney's fees and other expenses, but the proposal was rejected by U.S. District Judge Lucy Koh. In January 2019, Judge Koh ruled that this offer inadequately disclosed the total size of the settlement fund, the scope of non-monetary relief and the size of the settlement class, making it impossible for class members to assess the reasonableness of the offer. The court will hold a hearing on the revised settlement agreement on June 27, 2019. –*Aya M. Hoffman*

Health Care & HIPAA

Amazon opens its "HIPAA-eligible" environment to certain Alexa skills

Earlier this month, Amazon announced that it is opening its "HIPAA-eligible" environment to select Amazon Alexa skills that will transmit and receive identifiable patient information. This allows users of the Alexa virtual assistant to begin using the device for select health-related services.

Amazon defines its HIPAA-eligible services as those that enable HIPAA-regulated covered entities and business associates to process and store identifiable patient information, or HIPAA protected health information, in its Amazon Web Services environment. At this time, Amazon is offering the opportunity to develop a skill for its HIPAA-eligible environment on an invitation-only basis.

The first six HIPAA-eligible Alexa skills focus on an individual's management of their care at home. For example, the Livongo Blood Sugar Lookup skill allows users to ask their Alexa device to provide their latest blood glucose reading. Cigna's Health Today skill allows Cigna enrollees to monitor their wellness program goals and receive health tips. Through the Express Scripts skill, an individual

can track prescription delivery and receive notification through the Alexa device when a prescription is delivered.

Although Amazon's addition of these skills to its HIPAA-eligible environment represents significant progress toward the use of virtual assistants to meet individuals' medical needs, it is important to note that these skills are limited. Amazon is not presenting a framework to allow for skills that capture data in an operating room or emergency room, for example, nor do the six HIPAA-eligible skills allow patients to correspond with clinicians for treatment or diagnosis of medical needs.

For people to use Alexa in these types of environments, not only will Amazon have to deem the relevant skills to be HIPAA-eligible and execute HIPAA business associate agreements with the skill developers, but the facilities and clinicians using Alexa for these services will have to ensure that they have the capability to do so in a manner that complies with the HIPAA requirements governing patient privacy and security. Some key considerations for facilities and clinicians will be to establish protocols to prevent people who are not authorized to access or hear an individual's identifiable information from doing so on the Alexa device, as well as ensure that Alexa captures the data in a way that attributes individual patients' data properly. –*Valerie Breslin Montague*

OCR releases new set of FAQs to address transmission of ePHI to apps

On April 18, 2019, the Department of Health and Human Services Office for Civil Rights (OCR) released new FAQs relating to HIPAA right of access to ePHI. Specifically, the FAQs address applications or other software (collectively "apps") designated by patients to receive ePHI from a covered entity's EHR (electronic health record) system. The FAQs discuss liability for transmission of ePHI and the apps' subsequent use or disclosure of health information, business associate relationships and agreements with apps, and whether a covered entity may refuse to disclose ePHI to an app.

OCR emphasized that once ePHI is disclosed to an app, as directed by a patient, a covered entity will not be liable under HIPAA for uses or disclosures of ePHI by the app so long as the app is not a business associate of the covered entity. A business associate relationship will not exist when the app was not developed for or provided by or on behalf of the covered entity. Subsequently, OCR noted an app's access to a patient's ePHI at the patient's request alone would not trigger a business associate relationship or require a business associate agreement to be put in place for the transmission of ePHI from a covered entity.

OCR provided there would be a business associate relationship between a covered entity and an app developer when the app is one a covered health care provider uses to provide services to individuals involving ePHI. In that case, OCR noted the covered health care provider may be liable under the HIPAA Rules if the covered entity's patient selects that app and that app impermissibly discloses the ePHI it receives.

OCR also provided that under the individual's right of access to their ePHI, a patient may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel. Therefore, a patient could request to a covered entity that their unencrypted ePHI be transmitted to an app as a matter of convenience. OCR noted that the covered entity would not be responsible for unauthorized access to the patient's ePHI while being transmitted to the app. However, OCR recommended that covered entities notify patients of the potential risks of unsecure transmission of ePHI at least the first time the patient makes such a request.

Also based on an individual's right of access to their ePHI, OCR stated that a covered entity may not refuse to disclose ePHI to an app chosen by an individual solely because of concerns about how the app will use or disclose the patient's ePHI. Examples of impermissible refusals provided by OCR included denying disclosure to an app because the app will share the patient's ePHI for research purposes or because the app does not encrypt the patient's data when at rest.

OCR FAQs can be found here. *–Jena M. Grady*

International

EU's new Copyright in the Digital Single Market Directive ratified despite controversy

Last week, the EU's highly controversial Copyright in the Digital Single Market Directive cleared the final hurdle. The European Council ratified the Directive, just weeks after the Directive successfully passed in the European Parliament. Now, with the approval of both the Council and the Parliament, the Directive is poised to go into effect in two years.

The Directive overhauls copyright law in the European Union and has faced massive protests and criticism from digital advocates all over Europe over the contents of Article 13 (renumbered as Article 17 after a recent update). Article 13 of the Directive shifts the responsibility for flagging copyright violations from owners of the copyrighted content to the online platforms themselves. Tech companies and activists alike have stressed that compliance will be nearly impossible even for the tech giants—to say nothing of the smaller outlets—and may change the face of the internet as we know it. Many worry that if platforms are forced to police content, they will opt to ban certain types of content altogether, delivering a huge blow to freedom of expression on the internet. To top it off, the Directive is notoriously unclear: while its language clearly suggests that gifs and memes may become a thing of the past, European lawmakers have insisted that was not the case. Of course, in the U.S., Section 230 of the Communications Decency Act continues to protect online platforms from liability for violations of law committed by its users, but in the EU, when it comes to copyright violations, those protections will cease to exist.

Notably, unlike Regulations (for instance, the GDPR), which become law once they are passed by the central EU institutions, Directives have to be written into each member country's national law. The two-year grace period is rarely strictly enforced so the change may take even longer, buying the Directive's opponents some time to bring a potential legal challenge. *–Karina Puttieva*

For more information, please contact:

- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Aya Hoffman at **ahoffman@nixonpeabody.com** or 585-263-1535
- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
- Jena M. Grady at **jgrady@nixonpeabody.com** or 212-940-3114
- Karina Puttieva at **kputtieva@nixonpeabody.com** or 213-629-6091

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team