NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

October 11, 2019

What's trending on NP Privacy Partner

Officials say Facebook's privacy-focused vision will impede criminal investigations, Kaspersky survey finds that internalizing data security measures can reduce costs dramatically and more. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

California court affirms win for Williams-Sonoma regarding gathering personal data at checkout

A California Court of Appeal recently affirmed a lower court ruling in favor of Williams-Sonoma in a case under the Song Beverly Credit Card Act of 1971 (the "Act") challenging the store's practice in soliciting consumer personal information at checkout. Williams-Sonoma Song-Beverly Act Cases, 2019 DJDAR 9435 (Ct. App, 1st Dist. September 30, 2019). The Act makes it illegal, in a credit card transaction, to "request, or require as a condition to accepting the credit card as payment …, the cardholder to provide personal information which the [merchant] causes to be written, or otherwise records, upon the credit card transaction form or otherwise." Civil Code § 1747.08(a)(2). Plaintiffs brought a class action alleging that William-Sonoma broke the law by asking customers for their zip code and other personal information in the middle of processing their credit card at checkout. William-Sonoma countered that the practice of store employees in regard to asking of the information at checkout was not uniform, that providing the information was voluntary, and that signs were prominently posted at checkout advising customers that they did not have to provide the information as a condition to making a purchase. Following a long line of cases under the Act, the court affirmed the lower court's determination that the applicable standard was whether a reasonable person would believe he or she was compelled to provide the information as a condition to completing the transaction based on all the circumstances. It declined to adopt plaintiffs' proffered rule that asking for the information in the middle of processing the transaction was a per se violation. The court also affirmed the lower court's order decertifying the class, based on plaintiffs' failure to establish that the circumstances at checkout were sufficiently uniform so as to constitute a common issue. A California merchant asking for personal information at checkout for marketing purposes may want to review the policies and procedures Williams-Sonoma put in place, as described in the opinion, including employee training, which allowed the company to prevail in this case. – *Karl Belgum*

The 2020 Census and your identity

Over the past several months, the 2020 Census has been a growing concern for many—from the Trump administration's efforts to include a citizenship question to concerns that the process of counting every single person living in the country may not receive the proper funding it needs. However, there is another issue that should be just as alarming. Recently, the U.S. Census Bureau conducted an experiment with previously acquired census data to determine if the information people provide to the Bureau could threaten their privacy. The agency used this information, along with other publicly available records, and discovered that they were able to infer the identities of 52 million Americans. To try to combat this privacy issue, the Bureau is going to use a technique called "differential privacy," which changes certain numbers in the statistics to protect identities, but retains the survey's primary findings. How effective this strategy will be remains to be seen. If the results from the Census are too diluted, it can lead to issues with redistricting and the dilution of minority voting power, possibly violating the Voting Rights Act.

To most people, however, their primary concern will be with their own identity and who will be able to access it with the public information released by the 2020 Census. With people putting more and more of their information on the web via social media or signing up for various other online accounts, it only gets easier for cyber predators to combine all this information, learn identities and other personal information about people, and use it to their detriment.

While bypassing the 2020 Census may not be an option, there are a few simple steps you can take to protect your identity and it mainly has to do with your online profile. Keep your online accounts to a minimum, only sign up for accounts that you will actually use and be beneficial to you, never provide information that was solicited via a suspicious email or other suspicious websites, and keep close track of those online accounts that use or save your credit card information. – *Jenny L. Holmes*

Special thanks to Tevin Hopkins for his contributions to this post.

Cybersecurity

U.S. and U.K. officials say that Facebook's privacy-focused vision for its messaging platforms will impede criminal investigations

Earlier this year, Mark Zuckerberg announced in a written note on Facebook's website that the company would be shifting its platform's focus toward a privacy-focused messaging and social networking service. As a part of this shift, Facebook is working to implement end-to-end encryption into its messaging platforms, which includes Facebook Messenger and Instagram Direct. Recently, however, law enforcement officials in the U.S. and U.K. governments have urged Facebook against putting end-to-end encryption into effect, arguing that it will interfere with their ability to investigate criminal activities.

End-to-end encryption prevents third parties from accessing messages sent between sender and recipient through online messaging services by storing the encryption key only on the participants' devices. Under this system, even Facebook itself could not access the content of conversations that take place on its own messaging platforms because these conversations would not be stored on its servers.

Generally, when an encryption key is stored on a messaging service provider's own servers, law enforcement officials can subpoena the provider to access the messages. However, with end-to-end encryption in place, companies like Facebook cannot provide law enforcement with access to the

encrypted messages. This system is particularly challenging for both the U.S. and U.K., as these countries recently signed a data sharing agreement, the CLOUD Act Agreement, which aims to significantly decrease the amount of time needed to investigate a criminal's online activities. Under this Agreement, both the U.S. and U.K., with proper authorization, can demand electronic data regarding serious crimes directly from technology companies based in either country. With Facebook making the transition to end-to-end encryption, however, law enforcement agencies in both countries will be unable to access encrypted messages.

In his announcement about the company's privacy-focused vision, Zuckerberg addressed the inherent challenges end-to-end encryption would cause law enforcement. He noted, however, that Facebook is working to improve its ability to identify and stop bad actors by examining data relating to areas other than the messages' substance, such as patterns of activity. Zuckerberg also pointed to the importance of private online messaging for those who live under oppressive regimes to freely express themselves. –*Franz Wright*

Special thanks to Christian Albano for his contributions to this post.

Data Breach

Kaspersky survey finds that internalizing data security measures can reduce costs dramatically

Enterprise data breaches have proven to be costly. New research from Kaspersky has found that the cost of these breaches has risen to $1.41 million annually, up from $1.23 million in the previous year. An estimated 4,000 data breaches have already occurred during the first half of 2019, affecting over four billion users' data. Consequently, enterprise organizations invested more in cybersecurity in 2019, with IT security budgets averaging $18.9 million compared to $8.9 million the previous year. Although the cost of each data breach has increased from year to year, Kaspersky's survey, "IT security economics in 2019: how businesses are losing money and saving costs amid cyberattacks," found that enterprises in 2019 have found ways to reduce these costs.

First, companies that have an internal Security Operations Center ("SOC") limited their estimated cyberattack financial damage at $675,000, less than half the average impact of breaches in 2018. Internal SOC's are typically responsible for the ongoing monitoring of security events and responding to incidents. Establishing an internal SOC, however, is no easy task. It includes recruiting analysts, building processes, and purchasing the necessary tools.

Second, the costs of a data breach can be reduced by creating a Data Protection Officer ("DPO") position—34% of all companies that had a dedicated DPO reported no monetary loss. A DPO is typically charged with building and implementing a data protection strategy for an enterprise and managing compliance issues.

The report also indicated that outsourcing security measures to a Managed Service Provider ("MSP") did not reduce financial loss resulting from data breaches. Rather, the survey showed that outsourcing may actually increase the financial impact of a data breach. In fact, the survey indicated that 23% of companies that outsourced their data security reported a financial impact between $100,000 and $249,000, while only 19% of businesses with an internal SOC team reported the same level of loss.

In sum, although these initiatives may seem difficult to justify at first, due to their potential strain on time and budgets, the numbers show that both initiatives are worthwhile investments as it will ensure that an enterprise is prepared for a data breach, allowing for a quick and efficient recovery. –*Justin Smith*

Health Care & HIPAA

Protecting Higher Education Institutions from HIPAA Risks

In a recent webinar, the Nixon Peabody Higher Education team addressed the potential implications of HIPAA on colleges and universities, including in relation to their employer-sponsored health plans, student health clinics, and counseling programs.

Does HIPAA apply to student health centers? Laurie Cohen, Partner (Health Care, Albany)

In providing health care services to students, the college/university will be considered a health care provider under HIPAA (and thus a "covered entity") if it submits claims electronically to a student's health insurer or conducts any other covered transactions electronically.

Although the college/university may be considered a HIPAA-covered entity, the college/university will not, however, be required to comply with the HIPAA Privacy Rule to the extent that the health records maintained by the health center relate only to its students. HIPAA specifically excludes "education records" or "treatment records" from the definition of "protected health information (PHI)."

Instead, such student health records are governed by the Family Educational Rights and Privacy Act (FERPA). Although HIPAA does not apply to student health records, if the college or university meets the definition of a covered entity, HIPAA will apply to any PHI of non-students held by the college or university. To limit the application of HIPAA to specific components/departments, the college or university will want to determine whether to designate itself a "hybrid-covered" entity.

College/university-sponsored health plans are HIPAA-covered entities. Yelena Gray, Partner (Labor & Employment, Chicago)

College and university group health plan sponsors must amend their plan documents for compliance with HIPAA, certify to their plans that the sponsor will adhere to the HIPAA requirements, and establish a firewall between the sponsor's personnel with access to PHI and the sponsor's other workforce.

Colleges and universities must also identify plan vendors that are business associates and enter into business associate agreements with them to ensure maximum protection for plan participants and their covered dependents.

Is the college/university regulated as a HIPAA business associate? Valerie Breslin Montague, Partner (Health Care, Chicago)

Colleges and universities should continually review their operations to determine whether any of their services trigger HIPAA regulation as a business associate arrangement, such as a university providing administrative services to a physician faculty practice plan, where such an arrangement involves access to protected health information. If so, the organization should ensure that it enacts a HIPAA compliance plan and carefully reviews the provisions of all business associate agreements to ensure that the terms governing indemnification, notification, de-identification, and return of data, among others, are acceptable.

Assessing the applicability of HIPAA.

The consequences of noncompliance with HIPAA are significant. Nixon Peabody is able to assist colleges and universities to assess the applicability of HIPAA to its health center operations; its employer-sponsored health plan, as well as other components.

Please reach out to Laurie Cohen, Yelena Gray, or Valerie Montague for additional information. – *Laurie T. Cohen, Yelena F. Gray, Valerie Breslin Montague*

Dental practice learns if you don't have anything that is HIPAA compliant to Yelp don't Yelp at all

On October 2, 2019, the Department of Health and Human Services Office for Civil Rights (OCR) announced Elite Dental Associates - Dallas, P.C. (Elite) had agreed to pay $10,000 to OCR and adopt a corrective action plan to settle possible violations of the HIPAA Privacy Rules.

OCR is a private dental practice in Dallas, Texas, that had a patient submit a review on Elite's Yelp review page. Elite decided to respond to the patient's review by disclosing the patient's last name and details of her treatment plan and insurance. The patient subsequently submitted a complaint to OCR on June 5, 2016, regarding Elite's response.

Once OCR initiated an investigation of the dental practice to review the patient's complaint, OCR determined that Elite improperly disclosed PHI of multiple patients in response to Elite's Yelp reviews without valid HIPAA authorizations; failed to implement policies and procedures with respect to PHI, including releasing PHI on social media/public platforms; and failed to have the minimum content required in its Notice of Privacy Practices as provided by the HIPAA Privacy Rule. Even though Elite had the above significant HIPAA violations, OCR noted that it took into account Elite's size, financial circumstances, and cooperation with OCR's investigation when accepting the $10,000 settlement amount.

OCR Director Roger Severino stated, "Social media is not the place for providers to discuss a patient's care" and that "[d]octors and dentists must think carefully about patient privacy before responding to online review."

To drive this point forward, part of Elite's corrective action plan with OCR includes Elite being required to revise its Notice of Privacy Practices to include a description of the uses and disclosures of PHI for which Elite is required to obtain an individual's authorization and OCR gives examples of posting on Elite's website, social media pages, and/or other public platforms to include in this Notice. Notably, this requirement to provide specific social media examples that require HIPAA authorization goes beyond what is provided in the Notice of Privacy Practices requirements in the HIPAA Privacy Rule. 45 CFR §164.520(b) only requires specific notice of the requirement for authorization for psychotherapy notes and marketing and sale of PHI. For all other uses or disclosures not otherwise permitted by HIPAA, 45 CFR §164.520(b) only requires a general statement that other uses and disclosures not described in the Notice of Privacy Practices will be made only with an individual's written authorization and a statement that the individual may revoke an authorization.

Elite's lesson with OCR is an important lesson for all HIPAA covered entities about the necessity of understanding their responsibilities under HIPAA when posting or responding on any social media platform.

OCR's press release about this settlement can be found here. – *Jena M. Grady*

For more information, please contact:

- Karl Belgum at **kbelgum@nixonpeabody.com** or 415-984-8409
- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Franz Wright at **fwright@nixonpeabody.com** or 585-263-1473
- Justin Smith at **jssmith@nixonpeabody.com** or 401-454-1027
- Laurie Cohen at **lauriecohen@nixonpeabody.com** or 518-427-2708
- Yelena F. Gray at **vfgray@nixonpeabody.com** or 312-977-4158
- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
- Jena M. Grady **at jgrady@nixonpeabody.com** or 212-940-3114

NP PRIVACY PARTNER BLOG

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