May 22, 2018


TLP White

As promised, this week we primarily focus on a roundup of state breach notification laws and related federal proposals. To do so, we begin with the MyFitnessPal breach to set the stage. We also discuss a new approach to improving information sharing between the private sector and the government and conclude with one last GDPR reminder before the highly anticipated EU regulation goes into effect on the 25th. Welcome back to *Hacking Healthcare:*

***Hot Links –***

1. ***Breach Notification: Parsing Through the Patchwork and Proposals Towards a Federal Standard***

   In March, news broke that MyFitnessPal app user names, email addresses, and hashed passwords had been acquired by an unauthorized party in February this year. The app's owner, Under Armour, is now facing a putative class action in California by one of the app's users, claiming that the company should be held accountable for the personal information that was stolen from her and about 150 million other users as a result of the breach.[1] In addition to claiming that her information was compromised, the plaintiff also claims that Under Armour failed to provide consumers with notice of the breach in a timely fashion.

   With breach notification laws now in place in all 50 U.S. states,[2] businesses that experience a security incident have up to 50 pieces of legislation that they must parse in order to understand whether the law has been triggered and what their subsequent obligations are. This is no small undertaking for a company as big as Under Armour, and is tremendously burdensome for smaller companies that are trying to comply.

   Because of this complexity, we thought it would be a good time to reflect on the bigger picture, and to understand the practical effects of the patchwork breach notification regime that we have today. In addition to an overview of state breach notification laws,

[1] https://www.law360.com/cybersecurity-privacy/articles/1044019/under-armour-hit-with-suit-over-myfitnesspal-data-breach

[2] https://www.law360.com/publicpolicy/articles/1029088/breach-notification-expands-to-50-states-with-alabama-law-

we have also reviewed some of the current attempts to harmonize breach notification laws at the federal level and considered the practical impact of moving towards a national breach notification standard.

## I. Overview of State Breach Notification Laws

Most state breach notification laws apply to entities that collect and maintain personally identifiable information ("PII") which at a minimum typically includes names, addresses, identification numbers like a Social Security Number ("SSN"), and biometric information. From here, some states include additional data points in their definition of personal information. For example, California,[3] Illinois,[4] Rhode Island,[5] Alabama,[6] and Arkansas[7] include health information such as medical history and/or health insurance information in the definition of PII.

In addition to variations in the scope of what is considered PII, there is inconsistency with respect to the timing of breach notification. For example, over 30 states – including California,[8] Illinois,[9] and Arkansas[10] – have adopted an "expedient time…without unreasonable delay" notification period while others have adopted a 30,[11] 45,[12] 60,[13] or even a 90-day[14] notification period. Depending on the complexity of the breach and the size of the company, it is not hard to imagine that a business may find itself bumping up against breach notification deadlines before the company has had a chance to get a handle on the basic components of the incident or even risk mitigation to minimize the impact of the security event.

Also, different states require businesses to notify different types of entities, not just the consumer. Several states, for example, require covered entities to notify major credit reporting agencies, state attorneys general, and other government agencies.

With respect to the form of delivery, most states permit similar notification methods such as by mail or email and in some situations, through statewide media. [15] Nonetheless, states often differ in the substance of the notification itself. For example,

---

[3] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82
[4] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
[5] http://webserver.rilin.state.ri.us/Statutes/TITLE11/11-49.3/11-49.3-3.HTM
[6] http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2018RS/PrintFiles/SB318-enr.pdf
[7] https://law.justia.com/codes/arkansas/2017/title-4/subtitle-7/chapter-110/section-4-110-103/
[8] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82
[9] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
[10] https://law.justia.com/codes/arkansas/2017/title-4/subtitle-7/chapter-110/section-4-110-105/
[11] http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String&URL=0500-0599/0501/Sections/0501.171.html
[12] http://codes.ohio.gov/orc/1349.19
[13] http://delcode.delaware.gov/title6/c012b/index.shtml
[14] https://www.cga.ct.gov/current/pub/chap_669.htm
[15] https://law.justia.com/codes/arkansas/2017/title-4/subtitle-7/chapter-110/section-4-110-105/

California requires that notification be in plain language and include clear and conspicuous headers, following a specific form provided by the state. Other states like Arkansas and Illinois do not include such specific language requirements. Some states have distinct requirements for the consumer notification letter as compared to notification provided to the attorney general or other government entity, and may even prohibit the inclusion of some information in one letter that is required in another. Therefore, providing notification for a breach as massive as the MyFitnessPal breach, for example, requires several different notification letters to a variety of entities, not just consumers, to reflect the nuances of each state's content requirements.

So, what does this all mean? Now that we are operating in a world with 50 state breach notification laws, and various (and sometimes conflicting) notification requirements, providing breach notification and conducting the analysis that goes along with it requires a tremendous amount of time and resources. With healthcare being the most targeted industry sector in the first quarter of 2018 for cyberattacks,[16] healthcare organizations are particularly burdened by the variety and inconsistency of breach notification requirements. Healthcare organizations may also have the most to gain from replacing the patchwork of breach notification laws with a national standard at the federal level.

## II. Overview of Three Federal Breach Notification Bills:

Recognizing the need for federal breach notification legislation, the 115th Congress has introduced several breach notification bills since the start of the session. Three bills in particular – (1) the Data Acquisition and Technology Accountability and Security Act ("DATAS"); (2) the Data Accountability and Trust Act ("DATA"); and (3) the Personal Data Notification and Protection Act ("PDNPA") – have generated a lot of buzz so we have decided to provide readers a general overview of these three bills in particular.

The three bills have similar components, including preempting state law and applying to entities that collect and maintain PII. Although the three bills include similar identifiers within their definitions of PII – e.g., name, address, identification numbers such as a Social Security Number, and biometric information – only the DATA includes health information and the PDNPA partially exempts HIPAA covered entities. Also, the DATA and PDNPA require a 30-day consumer notification while the DATAS only requires a consumer notification if there is a risk that the breach resulted in identity theft, fraud, or economic loss. Each bill requires covered entities to notify the major credit reporting agencies if the number of effected individuals exceeds 5,000.

The three bills can be distinguished by the authority granted to federal agencies. For example, the DATAS and PDNPA grant more authority to the Federal Trade Commission

[16] https://healthitsecurity.com/news/cyberattackers-exploiting-weaknesses-in-healthcare-data-security

("FTC") but also provide authority to additional federal agencies while the DATA almost exclusively relies on the FTC.

Overall, although the bills overlap in scope, there are differences worth paying close attention to. NH-ISAC Members should sign in to get a more in-depth analysis of the three bills.

2. ***Information Sharing.*** But enough about breaches and notification. Let's talk about information sharing. Robert K. Knake, former cyber policy director in President Obama's National Security Council and current senior fellow at the Council on Foreign Relations, recently proposed a new approach to information sharing between the private sector and government.[17] According to Knake, "Critical infrastructure companies cannot protect themselves from adversarial nation-states without federal assistance…[and therefore,] [t]he U.S. government should create a classified network to share information on cyber threats with private companies critical to the economy."

   Knake's approach lays out four recommendations, including: (1) revamping security clearance rules by giving the Secretary of the Department of Homeland Security ("DHS") "unambiguous authority" to grant clearances to private facilities and their personnel; (2) accelerating private sector security clearance approvals by quickly clearing cyber intelligence units at critical infrastructure companies identified in Obama's Executive Order 13626[18] (which calls for an improvement to critical infrastructure cybersecurity); (3) calling on the DHS to create a pilot program that builds upon private sector background checks to reduce redundancy and increase efficiency; and (4) asking Congress to permit the DHS to charge and retain fees to cover expanded private sector clearance costs.

   Information sharing, as Members know, is extremely important to mitigating and avoiding cyber threats – especially between the private sector and government to avoid national security issues. Therefore, despite potential reservations surrounding information sharing, approaches like Knake's and other cybersecurity experts should be taken seriously so that the normalized trend towards consistent and effective information sharing can continue to grow.

3. ***GDPR – Ready or not, here it comes!*** After months of wading through confusing regulation and equally confusing guidance, forming your compliance plan, and working through implementation, the General Data Protection Regulation ("GDPR") will officially become effective this Friday, May 25, 2018. If you've already checked off everything on your GDPR to do list, congratulations! And if you have not, there is still a little bit of

[17] https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector?utm_campaign=sharing-classified-cyber-threat-informatin&utm_source=tw&utm_content=051518&utm_medium=social_earned
[18] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

time left (emphasis on *little*). No matter which side of the GDPR readiness spectrum you fall into, the months that follow the GDPR's effective date will be telling for all as we monitor how it is implemented across EU member states. Let the games begin!

***Congress*** –

Tuesday, May 22:
--Hearing to examine the healthcare workforce, focusing on addressing shortages and improving care (Senate Committee on Health, Education, Labor, and Pensions)[19]
--Hearing to examine Internet of Things legislation (House Subcommittee on Digital Commerce and Consumer Protection)[20]

Wednesday, May 23:
--Joint hearing entitled, ""The Federal Information Technology Acquisition Reform Act (FITARA) Scorecard 6.0" (House Subcommittee on Information Technology and House Subcommittee on Government Operations)[21]

Thursday, May 24:
--Hearing to examine cybersecurity, focusing on risks to the financial services industry and its preparedness (Senate Committee on Banking, Housing, and Urban Affairs)[22]

***Conferences and Webinars*** –

--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>
--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>

[19] https://www.senate.gov/committees/committee_hearings.htm
[20] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108341
[21] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108358
[22] https://www.senate.gov/committees/committee_hearings.htm

May 22, 2018

--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>

***Sundries –***

-- **Police Seize Servers of Bulletproof Provider Known For Hosting Malware Ops**
< https://www.bleepingcomputer.com/news/security/police-seize-servers-of-bulletproof-provider-known-for-hosting-malware-ops/>
--**Ex-Trump aide Bannon promoted 'culture war': Cambridge Analytica whistleblower**
<http://feeds.reuters.com/~r/reuters/topNews/~3/1uqngFnad3s/ex-trump-aide-bannon-promoted-culture-war-cambridge-analytica-whistleblower-idUSKCN1IH36S>
--**Cyber attack delays Atlanta mayor's first budget pitch**
<http://feeds.reuters.com/~r/Reuters/domesticNews/~3/o4QgwyIKDWk/cyber-attack-delays-atlanta-mayors-first-budget-pitch-idUSKCN1IG3EG>
--**Trump scraps cyber czar post after first appointee leaves: White House**
http://feeds.reuters.com/~r/reuters/topNews/~3/wNQ6ZVUVRSw/trump-scraps-cyber-czar-post-after-first-appointee-leaves-white-house-idUSKCN1IG3GG>
--**Mark Zuckerberg, Bezos, and Ethically Iffy 'Philanthropy'**
<https://www.wired.com/story/musk-zuckerberg-bezos-and-ethically-iffy-philanthropy>
--**Rollout of Windows 10 April Update Halted for Devices With Intel & Toshiba SSDs**
<https://www.bleepingcomputer.com/news/microsoft/rollout-of-windows-10-april-update-halted-for-devices-with-intel-and-toshiba-ssds/>
--**Latvian national convicted of running 'VirusTotal-for-criminals' malware scanner**
<https://www.cyberscoop.com/scan4you-ruslan-bondars-convicted-malware-scanner/>
--**Hackers Stole Funds from Mexican Banks**
<https://www.darkreading.com/attacks-breaches/hackers-stole-funds-from-mexican-banks/d/d-id/1331821>
--**Google Fixes Issue That Broke Millions of Web-Based Games in Chrome**
<https://www.bleepingcomputer.com/news/google/google-fixes-issue-that-broke-millions-of-web-based-games-in-chrome/>
--**Phishing Spy Campaign Targets Top Mideast Officials**
<https://threatpost.com/phishing-campaign-targeted-top-officials-with-surveillance-ware-tools/131994/>

Contact us: follow @NHISAC and email at contact@nhisac.org