May 1, 2018

TLP White

We start this week with news coming out of Congress, including a new privacy bill in the Senate and then we'll discuss a recent House Committee announcement asking for the public's input on ways to reduce cybersecurity vulnerabilities. We then shed some light on a medical transportation service breach and focus on a new report discussing a privacy issue surrounding the Amazon Echo. We also address a major change at the Healthcare and Public Health Sector Coordinating Council and conclude with a discussion about supply chain cybersecurity threats. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Federal Breach Notification.*** Senators Amy Klobuchar (D-MN) and John Kennedy (R-LA) recently introduced bipartisan privacy legislation focused on protecting consumers' online data.[1] The legislation, titled the "Social Media Privacy Protection and Consumer Rights Act of 2018," comes in the wake of Facebook's Cambridge Analytica scandal and Russia's alleged 2016 election interference. According to Senator Klobuchar, "The digital space can't keep operating like the Wild West at the expense of our privacy" and Senator Kennedy said he has "a job to do, and that's protecting the rights and privacy of our citizens."

   The bill would require "operators" of "online platforms" to discuss privacy clearly and transparently as well as give consumers more control over their data. The bill borrows the Children's Online Privacy Protection Act's definition of "operator" – i.e., "any person who operates a website located on the Internet…who collects and maintains personal information from or about the users of or visitors to such website…"[2] and defines "online platform" as, "any public-facing website, web application, or digital application (including a mobile application)… [that] includes a social network, an ad network, a mobile operating system, a search engine, an email service, or an Internet access service.[3]

[1] https://www.klobuchar.senate.gov/public/index.cfm/2018/4/klobuchar-kennedy-introduce-bipartisan-privacy-legislation-to-protect-consumers-online-data
[2] https://www.law.cornell.edu/uscode/text/15/6501
[3] https://www.scribd.com/document/377302061/S-Social-Media-Privacy-Protection-and-Consumer-Rights-Act-of-2018

Specifically, the bill would: (1) require the companies' terms of service to be in plain and digestible language; (2) provide consumers the option to review information that has already been collected and shared; (3) grant consumers greater control and access over their data; (4) permit consumers to opt-out of data tracking and collective practices; (5) compel companies to notify consumers of a privacy violation within 72 hours and to offer remedies to consumers in the event of a privacy violation; and (6) call for companies to install a privacy program.[4]

2. ***Public and Private Efforts to Reduce Healthcare Vulnerabilities.*** Entities in both the public and private sector have ramped up efforts to adapt to advances in technology that impact the healthcare industry.

   HSCA Guidelines. The Healthcare Supply Chain Association ("HSCA") released guidelines for healthcare providers, medical device manufacturers and service providers, drafted to help protect patient health, safety and privacy.[5] The HSCA is a trade organization which advocates on behalf of healthcare group purchasing associations. HSCA collaborates with legislators and regulatory authorities "to ensure fair and efficient procurement practices."[6] Its membership includes healthcare purchasers and supply-chain management organizations.

   House E&C RFI. The House Energy & Commerce Committee ("Committee") is also concerned about the impact of legacy devices on the health care industry. The Committee recently released a request for information ("RFI") asking the public to submit input and feedback regarding legacy technology challenges, opportunities, considerations and suggestions in the health care sector.[7] In the RFI, the Committee notes that "legacy technologies, which are typically more insecure than their modern counterparts, continues to be a root cause of many incidents." Noting the impact of the WannaCry ransomware, the Committee questioned how many other potential "WannaCrys" may be lurking.

   If you or your organization would like to submit your input to the Committee, you may submit feedback to supportedlifetimes@mail.house.gov by May 31, 2018. Submissions will be made publicly available to help advance the public discussion around these issues.

3. ***Breach News:*** According to well-known security researcher Brian Krebs, MEDantex, a Kansas-based medical transcription services company, unintentionally left part of its

[4] https://www.klobuchar.senate.gov/public/index.cfm/2018/4/klobuchar-kennedy-introduce-bipartisan-privacy-legislation-to-protect-consumers-online-data
[5] https://c.ymcdn.com/sites/higpa.site-ym.com/resource/resmgr/HSCA_-_Cybersecurity_Conside.pdf
[6] http://www.supplychainassociation.org/?page=Mission
[7] https://energycommerce.house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf

website open to the public after rebuilding its site after a ransomware attack.[8] The vulnerability came through MEDantex's online patient portal – which was supposed to be password protected – and resulted in a breach of patient data from at least 2,300 providers. MEDantex's founder and chief executive, Sreeram Pydah, said he doesn't "know how [the site] left the documents in the open like that… [and that] [MEDantex is] going to take the site down and try to figure out how this happened."

The vulnerability granted anyone who visited the website access to the site's administration tools, including the ability to add or delete users and access to patients' medical records. Although it is unclear how long the website was open to the public, the breach includes records from 2007 and according to Krebs, the portal may have been accessible as recently as April 10, 2018.

4. ***Tech News. Amazon Echo***. Checkmarx, a security research firm, recently discovered a security risk in the Amazon Echo's activation feature, which allowed the firm to turn the device into a spy tool.[9] The most interesting part, however, is that the firm did not hack into the device in the traditional sense. Instead, the researchers discovered a way to "piggyback" off the device's wake word – e.g., "Hey, Alexa." For those who haven't let Alexa into your lives, just know that a user activates the Echo through a wake word and upon hearing the wake word, the device listens for the user's request and records the relevant data. However, once the device completes its requested task, the device is supposed to stop recording.

   The researchers utilized an attack most commonly associated with mobile devices. An attacker can gain access to a smartphone if a user downloads a malicious app from the smartphone's app store – e.g., Google Play Store. The Checkmarx researchers, adopting the same approach, created an Amazon "skill" that could have been uploaded to Amazon's Skill Store. The researchers designed the skill to act like a calculator – e.g., "Alexa, what's 5 + 5?" – but unbeknownst to an Echo user, the skill also included a function called "shouldEndSession." This function allowed the Echo to remain on and record data even after completing its calculator task. To make matters worse, the skill would also send the recorded data back to the developer.

5. **HPH SCC Re-Vamp.** The Healthcare and Public Sector Coordinating Council ("HPH SCC") recently announced changes to the organization's size and structure. The changes are intended to support the organization's efforts to expand its membership and outreach, as well as to implement policy recommendations from a Health and Human Services task force report ("HHS report").[10]

[8] https://krebsonsecurity.com/2018/04/transcription-service-leaked-medical-records/
[9] https://www.wired.com/story/amazon-echo-alexa-skill-spying
[10] https://insidecybersecurity.com/daily-news/health-sector-group-reorganizes-around-hhs-cyber-task-force-advice-crucial-time

Among the changes to the organization, the HPH SCC has expanded its Joint Cybersecurity Working Group, adding 100 new members since February. The working groups within the HPH SCC are broadly organized around several issue areas and imperatives that appeared in the HHS report, including saleable best practices, securing medical technology and health IT system, supply chain security, expanded information sharing, and workforce development. Some of our very own NH-ISAC members have been actively involved in the efforts through participation in the cybersecurity working groups. The HPH SCC will continue its "scoping process" over the next few weeks as the working groups evaluate the work load and hone in on the focus of their efforts.

Congress –

Tuesday, May 1:
--No relevant hearings

Wednesday, May 2:
--No relevant hearings

Thursday, May 3:
--No relevant hearings

Conferences and Webinars –

<https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>
--Medical Device and Pharmaceutical Security Workshop – London
<https://nhisac.org/events/nhisac-events/security-workshops-london/>
--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17)
<http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>
--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>
--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/>
--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 –

-- **New hacking group targeting healthcare infects MRI, X-ray machine** <http://www.healthcareitnews.com/news/new-hacking-group-targeting-healthcare-infects-mri-x-ray-machine>
--**Scrutinizing a proposal to thread the encryption needle** <https://www.politico.com/newsletters/morning-cybersecurity/2018/04/26/scrutinizing-a-proposal-to-thread-the-encryption-needle-184098>
-- **War Machines: Artificial Intelligence in Conflict** <https://www.lawfareblog.com/war-machines-artificial-intelligence-conflict>
-- **Facebook's Targeted Ads are More Complex Than It Lets On** <https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on>
--**BD Medical Gear Suffers from Wi-Fi Cybersecurity Vulnerabilities** <https://healthitsecurity.com/news/bd-medical-gear-suffers-from-wi-fi-cybersecurity-vulnerabilities>
--**Gmail is Getting a Long-Overdue Upgrade** <https://www.wired.com/story/gmail-is-getting-a-long-overdue-upgrade>
--**Competition is at the Heart of Facebook's Privacy Problem** <https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem>
--**Sentencing delayed for FSB's email-popping hacker pawn** <https://www.cyberscoop.com/karim-baratov-sentence-delayed-fsb-email-hacking/>
--**SEC fines Yahoo remnant Altaba $35 million for failing to disclose breach** <https://www.cyberscoop.com/yahoo-altaba-35-million-sec-fine/>
--**Cops shut down one of the largest DDoS marketplaces in the world** <https://www.cyberscoop.com/webstresser-ddos-europol-arrests/>

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