July 17, 2018

TLP White

We start with the latest in exercise data shenanigans and then learn some lessons from the CISO of Equifax. We conclude today with a look at a law in Illinois dealing with biometric data and who owes who what when it is collected. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Polar Fitness App Revelations.*** You might recall a story from earlier this year regarding a company called Strava, whose fitness tracking app was found to be revealing the location of its users, including those on sensitive military and government installations.[1] Now we find ourselves in a similar situation with Polar. This time, the information exposure might be more significant, since it appears to show every "exercise a person has performed since 2014 on a single map, allowing potential snoops to gather scores of valuable information on potentially high-ranking people."[2]

   In fact, a group of researchers looking into the matter were ultimately able to identify 6,460 unique users. Those users were shown to have performed over 650,000 exercises at their homes and more than 200 sensitive locations. Example users included "…a nuclear airbase officer, an intelligence officer at a U.S. Air Force base; Western military members in Afghanistan and Iraq; and employees at the NSA and FBI." Yikes.

   All very interesting and concerning, but we'll let the good folks at Polar describe why we think this is an important issue: "It is important to understand that Polar has not leaked any data, and there has been no breach of private data."[3] You may have noticed that we have been seeing more of this in recent history. While actual breaches are occurring (sensitive information is being taken without authorization), there is increasing awareness of how data that is simply available publicly, or with very little effort, is creating risk for individuals and organizations alike.

---

[1] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[2] https://www.scmagazine.com/polar-fitness-app-found-to-reveal-movements-of-military-personnel-government-agents/article/779853/

[3] https://www.polar.com/us-en/legal/faq/public_and_private_training_data_statement

For their part, Polar is "…analyzing the best options that will allow Polar customers to continue using the Explore feature while taking additional measures to remind customers to avoid publicly sharing GPS files of sensitive locations."[4]

2. ***From the "Live and Learn" Department: Equifax.*** We all know that teachable moments can come from adversity, and it's fair to say that Equifax has had their fair share of it. The good news is that as Equifax continues to recover and rebuild, we can all watch and learn.

   Recently they brought on a new CISO in the form of Jamil Farshchi, who spent time rebuilding the cybersecurity program post-breach at Home Depot.[5]

   Jamil is implementing a three-phase approach grounded in the idea of "shared fate" for all parts of the organization, which starts with culture change. "The number one thing, by far, is driving the culture change. It's not just my top priority, but it also tends to be the most difficult aspect of the turnaround initiative."

   Farshchi highlights two things in his approach: he reports directly to the CEO, and "every single person's incentive plan..." has a security component. Reporting to the CEO is not something most CISOs experience, and yet we see time and again that following a major security incident, CISOs are elevated within the organization. It tends to suggest that proactively empowering CISOs before an incident may well be worth org chart reshuffling because it will not only raise C-Suite awareness, but a good CISO will help his or her leadership counterparts understand how to achieve business success in a secure way. This in turn drives accountability down through the rest of the organization. As Farshchi says, "[s]ecurity isn't just security's job. Everyone needs to feel it through and through or we won't be successful otherwise."

   The third major part of Equifax's approach involves the creation of a "fusion center." If you spent any time in government or interfacing with it in this area, you might not have the greatest opinion of the idea. However, as Farshchi describes, it makes sense when done right: "you marry up your physical security and all of the activities, visibility and detection capabilities on that side with the cyber team itself. What we're doing is taking it one step further and we're injecting the IT operational folks in as well." His hope is that by bringing all these cross-functional stakeholders together, visibility into risk will be greater and the ability to mitigate it will become more effective and timely.

3. ***Meanwhile in Illinois…the Future of Biometrics Privacy and Security?*** In the never-ending race with adversaries who are after your data, the drive to implement more security identity and authentication mechanisms has brought about the age of

[4] https://www.polar.com/us-en/legal/faq/public_and_private_training_data_statement
[5] https://www.cyberscoop.com/jamil-farshchi-equifax-ciso-apache-struts/

biometrics. Whether your face, your fingerprints, or yes even the way you walk[6], these innovations can and will continue to change the way we interface with the technology around us.

But just as attackers will go after usernames, password, birthdates, government IDs, and any other form of identifying information they can get their hands on, so too will they go after biometric data. The most famous case for this was the Office of Personnel Management (OPM) breach in 2015. Among the highly sensitive data of 21.5 million current and former federal government employees were over 5 million digital fingerprints (including yours truly). Of course, unlike a password, those fingerprints can't really be changed, meaning the risk to those 5 million people will stay with them their entire lives. And therein lies part of the reason that some argue special consideration needs to be given to it.

Which leads us to the state of Illinois and their Biometric Information Privacy Act (BIPA). One of only a handful of laws like it, and the only one that allows plaintiffs to sue. Under the statue, "companies are prohibited from scooping up biometric information unless they first notify individuals in writing about the specific purpose and length of time for which their data will be collected, stored and used and obtain a written release form these individuals."[7]

In this case, the plaintiff is arguing that a theme park failed to receive written consent regarding their collection of her son's fingerprints for purchasing a season pass. The initial court ruling was that since there was no harm, the plaintiff wasn't an "aggrieved person" and therefore not entitled to any recompense.

Several major privacy and policy organizations took issue with this including the Electronic Privacy Information Center, the Electronic Frontier Foundation, the American Civil Liberties Union, the Center for Democracy and Technology and several others. The reason they care is because of the potential long-term ramifications, certainly in Illinois, but possibly beyond.

In a pair of amicus briefs, these organizations argue that not holding the plaintiff as an "aggrieved person" would "significantly undermine the private enforcement mechanism of the statute…leaving no means to hold wrongdoers accountable for their violations of the BIPA's notice and consent requirements."

As noted above, biometric information stays with a user forever, and if not properly handled by those collecting it, can pose a serious lifetime risk to the compromised user's identity. If users aren't empowered to know how the information is being collected,

[6] https://ieeexplore.ieee.org/document/8275035/

[7] https://www.law360.com/cybersecurity-privacy/articles/1060789/biometric-privacy-suits-don-t-need-actual-harm-ill-court-told

used, and destroyed, then they can't make informed decisions on whether they want to share it or not. To be fair, the high court's decision in Illinois will have a limited impact outside of Illinois in the near term. But it's fair to say that this decision could easily reverberate in other states, or even at the national level given that biometrics are increasingly being used, and the attention governments are giving to privacy and security at the moment.

Congress –

Tuesday, July 17:
--Hearing to examine reducing health care costs, focusing on eliminating excess health care spending and improving quality and value for patients (Senate Health, Education, Labor, and Pensions Committee).[8]

Wednesday, July 18:
--Hearing entitled, "Powering America: The Role of Energy Storage in the Nation's Electricity System" (House Subcommittee on Energy).[9]
--Hearing to examine oversight of the Federal Trade Commission (House Subcommittee on Commerce and Consumer Protection).[10]
--Joint Hearing entitled, "2020 Census: Information Technology Preparations" (House Subcommittees on Government Operations & Information Technology).[11]

Thursday, July 19:
--Hearing entitled, "China's Threat to American Government and Private Sector Research and Innovation Leadership" (House Permanent Select Committee on Intelligence).[12]

Conferences, Webinars, and Summits –

--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--NH-ISAC & Boston Scientific Medical Device Security Workshop – Maple Grove, MN (7/24) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-maplegrove-mn/>
--NH-ISAC Blended Threats Exercise Series – MN (7/25) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--CSS-Healthcare System Management of Medical Devices – TBD (7/26) <https://nhisac.org/events/nhisac-events/css-2/>

[8] https://www.senate.gov/committees/hearings_meetings.htm
[9] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108567
[10] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108560
[11] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108569
[12] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108561

--Basic Best Practices in Cybersecurity – Abilene, TX (7/31) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas-2/>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Information Sharing Turns 20: Learn more at Borderless Cyber USA– Washington, DC (8/9) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>
--NH-ISAC Blended Threats Exercise Series – CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--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/>
--Biotech/Pharma Security Workshop at Amgen – Tokyo, Japan (8/29) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-at-amgen-tokyo/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/>
--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC & Cleveland Clinic Medical Device Security Workshop – Breachwood, OH (10/17-18) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-cleveland-clinic-beachwood-oh/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Demployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Is It Smart to Install a Smart Lock?**

July 17, 2018

<https://www.wsj.com/articles/is-it-smart-to-install-a-smart-lock-1531331694?mod=rss_Technology>
-- **Year-old router bug exploited to steal sensitive DOD drone, tank documents**
<https://arstechnica.com/information-technology/2018/07/year-old-router-bug-exploited-to-steal-sensitive-dod-drone-tank-documents/>
-- **Engineer Found Guilty of Stealing Navy Secrets via Dropbox Account**
<https://www.bleepingcomputer.com/news/legal/engineer-found-guilty-of-stealing-navy-secrets-via-dropbox-account/>
-- **Notorious 'Hijack Factory' Shunned from Web**
<https://krebsonsecurity.com/2018/07/notorious-hijack-factory-shunned-from-web/>
-- **Google Enables "Site Isolation" Feature for 99% of Chrome Desktop Users**
<https://www.bleepingcomputer.com/news/security/google-enables-site-isolation-feature-for-99-percent-of-chrome-desktop-users/>
-- **Banks Suffer an Average of 3.8 Data Leak Incidents Per Week**
<https://www.darkreading.com/endpoint/privacy/banks-suffer-an-average-of-38-data-leak-incidents-per-week/d/d-id/1332275>
-- **Microsoft Is Updating People and Maps Apps for Windows 10 With New Features**
<https://www.bleepingcomputer.com/news/microsoft/microsoft-is-updating-people-and-maps-apps-for-windows-10-with-new-features/>
-- **Chinese Censorship Bug Caused iPhone Crashes when Receiving Taiwan Flag Emoji**
<https://www.bleepingcomputer.com/news/security/chinese-censorship-bug-caused-iphone-crashes-when-receiving-taiwan-flag-emoji/>
-- **Voting machine vendors under pressure**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/07/12/voting-machine-vendors-under-pressure-277054>

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