September 25, 2018

TLP White

We start with a discussion around asserting a negligence claim following a data breach. We also discuss the prevalence of infected websites turning up in search engines results, including whose responsibility it is to deal with the issue. We conclude by shedding some light on proposed data storage legislation in India that has tech lobbyists around the globe up in arms. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Future Harm Falls Short in Negligence Claims.*** A court's recent ruling reminds consumers in Georgia that future harm often does not equate to compensable harm in the aftermath of a security breach. This issue arose in a case titled *Collins, et al. v. Athens Orthopedic Clinic*, regarding a data breach affecting 200,000 current and former patients of the Athens Orthopedic Clinic ("AOC").[1] After a ransomware attack perpetrated through the use of a third-party vendor's log-in credentials and the lengthy investigation that followed it, AOC was unable to afford to pay credit monitoring fees for those patients whose information was involved in the incident.

   Three of the 200,000 patients alleged that their personal information was stolen in the breach and that this exposed them to the threat of identity theft among other harm.[2] The three patients became the plaintiffs in the *Collins* case, arguing that the cost of identity theft protection, credit monitoring and credit freezes for a lifetime constituted sufficient damages to assert a claim under several causes of action, including negligence.

   The lower court granted AOC's motion to dismiss, and the plaintiffs appealed. The issue on appeal was whether the alleged costs (either anticipated or incurred) to protect an individual against the threat of identity theft after a data breach constitutes damages sufficient to state a negligence claim in Georgia. On appeal, the court determined that

[1] https://www.law.com/dailyreportonline/2018/09/18/what-constitutes-negligence-in-company-data-breaches/?slreturn=20180823214306
[2] https://www.law.com/dailyreportonline/2018/09/18/what-constitutes-negligence-in-company-data-breaches/?slreturn=20180823214306

the identity protection costs were insufficient to state a negligence claim where the plaintiff's damages are based on a risk of harm rather than actual, concrete harm.

2. ***Who is responsible for blacklisting infected websites?*** Following scans of more than 6 million websites, researchers at security firm SiteLock observed that people are generally permitted to access websites that have been infected with malware where the website was found through a search engine.[3] Additionally, the researchers revealed that as few as 17% of infected websites are blacklisted by search engines. These observations highlight a breakdown when it comes to blacklisting infected websites.

   The next question becomes, whose responsibility is it? Should search engines bear the responsibility for policing and flagging infected websites? According to a research analyst at SiteLock, search engines are hesitant to blacklist websites absent absolute certainty that the website poses a security risk. This reluctance, the analyst explained, is because flagging a website can eventually lead to substantial damage to the site or the site's reputation.

   Given the reluctance of the search engines, site owners have been left with the responsibility of ensuring that their websites are secure. Of course, this is easier said than done. SiteLock researchers estimate that websites are attacked 58 times a day, on average, noting that bots carry out the majority of attacks. In addition to dealing with attacks, site owners have to keep up with updates that address new vulnerabilities, particularly on open-source content platforms which are frequent targets. Between shielding from attacks and making sure that websites are up to date and up to snuff, site owners have their hands full.

3. ***The Tech Lobby Not Pleased with Data Storage Proposal in India.*** Tech lobbyists are preparing to go to bat in India over proposed data storage legislation that would require tech companies to store user data in India.[4] India's information technology ministry asserts that data localization was necessary to facilitate government investigations and to protect against global data breaches. Over the summer, a government panel recommended that all "critical personal data" should be processed in India, and presented a draft bill on the matter.[5] India is not alone in these sentiments. China and Vietnam have passed similar legislation requiring certain types of data to be stored within the respective country.

---

[3] https://thehill.com/policy/cybersecurity/407172-researchers-users-allowed-to-access-infected-sites-found-through-search?wpisrc=nl_cybersecurity202&wpmm=1

[4] https://www.reuters.com/article/us-india-data/global-tech-firms-gear-up-to-fight-indias-planned-data-law-idUSKCN1LZ19I?feedType=RSS&feedName=topNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtopNews+%28News+%2F+US+%2F+Top+News%29

[5] https://www.reuters.com/article/us-india-data/global-tech-firms-gear-up-to-fight-indias-planned-data-law-idUSKCN1LZ19I?feedType=RSS&feedName=topNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtopNews+%28News+%2F+US+%2F+Top+News%29

The companies opposed to the legislation argue that it will hurt investment as well as the business model of both foreign and domestic firms. Several of the major companies, such as Facebook, Mastercard, and PayPal, have concerns that the proposed legislation will increase compliance and infrastructure costs as well.

Global tech firms are not going to let this legislation pass without a fight. Lobbying groups representing several of the big wigs in global technology have prepared a letter addressed to India's information technology minister, which outlines the potential impact of the proposed legislation on both global and Indian companies. In addition to the letter, lobbyists from Washington and Brussels intend to hold talks with Indian officials.

The data storage legislation isn't the only trick up India's sleeve. The government is also drafting policies that would regulate data stored by cloud computing, e-commerce and payment companies.

Congress –

Tuesday, September 25:
--Hearing to examine health care in rural America, focusing on experiences and costs (Senate Committee on Health, Education, Labor, and Pensions).[6]
--Hearing entitled, "Better Data and Better Outcomes: Reducing Maternal Mortality in the U.S." (House Subcommittee on Health)[7]

Wednesday, September 26:
--Hearing to examine safeguards for consumer data privacy (Senate Committee on Commerce, Science, and Transportation).[8]
--Hearings to examine the cyber operational readiness of the Department of Defense; to be immediately followed by a closed session in SVC-217 (Senate Subcommittee on Personnel & Senate Subcommittee on Cybersecurity).[9]

Thursday, September 27:
--Hearing entitled, "DOE Modernization: The Office of Cybersecurity, Energy Security, and Emergency Response" (House Subcommittee on Energy).[10]

International Hearings/Meetings –

EU –

[6] https://www.senate.gov/committees/hearings_meetings.htm
[7] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108724
[8] https://www.senate.gov/committees/hearings_meetings.htm
[9] https://www.senate.gov/committees/hearings_meetings.htm
[10] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108725

Tuesday, September 25:
--Hearing entitled “Application of the ERN model in European cross-border healthcare cooperation outside the rare diseases area" (EU Commission’s Expert Panel on Health).[11]

Conferences, Webinars, and Summits –

--ICS Security Workshop – Cork, Ireland (9/25) <http://www.cvent.com/events/booz-allen-nh-isac-ics-security-workshop/event-summary-098b4a1a7bca4da78550a3883853b1d6.aspx>
--Health IT Summit – Raleigh, NC (9/27) <https://nhisac.org/events/>
--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/>
--Information Sharing Turns 20: Learn more at Borderless Cyber USA – Washington, DC (10/4) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>
--HSCC Joint Cyber Working Group Meeting – Nashville, TN (10/9-11) <https://nhisac.org/events/nhisac-events/hscc-joint-cyber-working-group-meeting/>
--Biotech/Pharma Security Workshop – Tokyo, Japan (10/17) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-tokyo/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Deployment 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/>
--2018 Heathcare CyberGard Conference – Charlotte, North Carolina (10/25-26) <https://nhisac.org/events/nhisac-events/2018-heathcare-cybergard-conference/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/7-9) <https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--**Equifax fined maximum penalty under 1998 UK data protection law**

[11]https://ec.europa.eu/health/expert_panel/events_en

<https://www.cyberscoop.com/equifax-uk-ico-fine/>
--**US to prioritize attacks against foreign adversaries under new cyber strategy**
<https://thehill.com/policy/cybersecurity/407670-us-to-launch-offensive-attacks-against-foreign-adversaries-under-new/>
--**Critical Security Update Released for Adobe Reader and Acrobat**
<https://www.bleepingcomputer.com/news/security/critical-security-update-released-for-adobe-reader-and-acrobat/>
--**Microsoft Announces Cumulative Updates for .NET Framework for Windows 10**
<https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-cumulative-updates-for-net-framework-for-windows-10/>
--**Wyden: Senators need protection from ongoing Russian hacking campaign**
<https://www.politico.com/story/2018/09/19/russians-hacking-senators-emails-fancy-bear-830642>