December 4, 2018

Hacking Healthcare

TLP White

This week we start by discussing the not entirely far-fetched proposition that bots have First Amendment rights. We also consider a new private sector guide for fighting botnets that aims to shore up technology companies' cybersecurity protections. We then turn to the British government's push to move prescription services online by funding NHS trusts' e-prescription implementation. We end by returning, again, to the issue of encryption and its potential to interfere with legitimate law enforcement efforts.

Welcome back to *Hacking Healthcare*.

Hot Links –

1. ***<u>California Bot Law and Supreme Court Precedent Tee Up Issue of Bots' First Amendment Rights.</u>*** This September, California passed a law requiring bots (software applications that perform automated tasks by communicating with people via the Internet) to disclose their artificial identities.[1] The law, which goes into effect in 2019, was passed in reaction to claims that Russian bots had affected the 2016 presidential election by communicating with people on social media and other platforms.

   In addition to nation-state use of bots for election meddling, businesses regularly use bots to facilitate transactions and orders as well as to market their products and services. Some legal scholars believe that California's bot law could be struck down on First Amendment grounds, because the right to free speech extends to businesses who employ bots.[2] Corporations that have free speech rights, the argument goes, equally have the right to be free from being compelled to say anything at all.[3] Requiring bots to disclose their artificial nature, therefore, could theoretically contravene corporations' free speech right to refrain from speaking.

[1] S.B. 1001 (Cal. 2018), located at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id =201720180SB1001; *see also* https://www.cnet.com/how-to/what-is-a-bot/.

[2] https://www.politico.com/magazine/story/2018/11/27/bots-first-amendment-rights-222689?cid=apn

[3] *See Minersville School District v. Gobitis*, 310 U.S. 586 (1940), located at https://supreme.justia.com/cases/ federal/us/310/586/ (holding that Jehovah Witness students did not have to say the pledge of allegiance before school because they had the right to be free from compelled speech).

We think that any argument in favor of such rights would face compelling counterarguments in court. By merely requiring bots to identify themselves and not censuring them entirely, California's bot law appears to strike an appropriate balance between free speech and consumer protection. In any event, whether the Supreme Court confronts California's law or not, it's clear that consumers will continue to interact with bots for the foreseeable future, whether known to them (as California would have it) or not.

2. ***Industry Group Publishes Best Practices Guide for Fighting Botnets.*** Speaking of bots, the Council to Secure the Digital Economy ("CSDE"), a group of trade associations that represent technology businesses, released an "International Anti-Botnet Guide" on November 29th. The guide sets forth strategies that technology companies can use to help keep their devices, networks, and users secure from botnet threats.[4] As the name suggests, botnets are a string of connected bots that work together to perform tasks. While some of them are useful and even necessary for regular Internet functions, others can be used in ways that allow hackers to gain access to machines and networks through malicious coding, or to bring websites and service offline through DDoS attacks.

   The CSDE guide serves as the industry's attempt to self-regulate to combat cybersecurity vulnerabilities that confront technology companies on a regular basis. It advocates for self-regulation in the industry as opposed to government-imposed requirements, which it believes will "inhibit the security innovation that is key to staying ahead of today's sophisticated threats."[5] The guide presents a set of voluntary best practices that various stakeholders can employ to fight botnet threats.

   Botnets have proven damaging and expensive to the international economy. Some experts estimate that the global cost of cybercrime could hit the trillion dollar mark by 2020.[6] As a result, guides like the CSDE's are important tools to assist companies in remaining vigilant in the fight against cyberattacks.

3. ***Thirteen British NHS Trusts Receive £75m to Improve E-Prescription Management Services.*** In February, England's then-Secretary of State for Health and Social Care Jeremy Hunt announced that the British government would allot £75m to implement an improved electronic prescription and medicine administration system in a number of NHS trusts.[7] England's government hopes that this funding will help decrease the number of medication errors that occur in the country due to poor prescription management on an annual basis (approximately 237 million in 2017).[8]

[4] https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf
[5] https://www.cyberscoop.com/csde-international-anti-botnet-guide/
[6] https://www.darkreading.com/threat-intelligence/anti-botnet-guide-aims-to-tackle-automated-threats/d/d-id/1333371?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple
[7] https://www.digitalhealth.net/2018/02/jeremy-hunt-e-prescribing-acceleration/
[8] https://www.healthcareitnews.com/news/13-nhs-trusts-england-receive-share-%C2%A316m-e-prescribing

England's Department of Health and Social Care has noted that electronic prescription and medicine administration systems are some of the "most challenging… systems to implement in provider organisations."[9] As a result, the government is supporting an open source, open standards-based system that it believes will streamline prescription services for patients across the country. Government funding for this new system has been awarded to thirteen NHS trusts that provide a variety of mental health, community, and acute care services.

4. ***US Deputy Attorney General Stresses Law Enforcement Difficulties with Encryption.*** From our "Yep, we are still debating this" department, we highlight a recent speech at the Georgetown University Law Center's Cybercrime Conference, where Deputy Attorney General Rod Rosenstein warned technology companies and industry groups that sophisticated encryption technologies have the potential to thwart legitimate law enforcement practices. This messaging follows the Department of Justice's ("DOJ") somewhat recent effort to contest end-to-end encryption mechanisms that have been implemented by companies such as WhatsApp and Apple.[10] According to DOJ, end-to-end encryption (a security feature that renders third parties unable to read user messages) can negatively affect law enforcement cases by blocking officers' ability to investigate suspects' actions.

   Government and private sector stakeholders have generally disagreed about what constitutes an appropriate level of commercially available data encryption.[11] While privacy advocates decry the government's alleged desire for a "master key" to enable law enforcement access to user communications, law enforcement agents such as Deputy AG Rosenstein stress their need for back door access due to public safety concerns. In 2016, the federal government tried to force the private sector's hand and require it to weaken encryption protections through an FBI lawsuit against Apple.[12] The FBI eventually withdrew its request and the case was dismissed, because officers found a third party service that gave them access to the information they needed. However, this case added fuel to a longstanding debate that has positioned privacy and security groups against law enforcement agencies in the context of cybersecurity technologies.

Congress –

Tuesday, December 4:
--Hearing to examine the China challenge, focusing on democracy, human rights, and the rule of law (Senate Committee on Foreign Relations' Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy).[13]

[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683430/short-life-working-group-report-on-medication-errors.pdf
[10] https://www.cyberscoop.com/rod-rosenstein-encryption-georgetown-university/
[11] https://www.wired.com/story/rod-rosenstein-encryption-backdoor/
[12] https://www.wired.com/2016/02/apple-fbi-privacy-security/
[13] https://www.senate.gov/committees/hearings_meetings.htm

Wednesday, December 5:
--Hearing on Department of Defense's artificial intelligence structure, investments, and applications (House Committee on Armed Services' Subcommittee on Emerging Threats and Capabilities).[14]
--Hearing to examine the Food and Drug Administration, focusing on leveraging cutting-edge science and protecting public health (Senate Committee on Health, Education, Labor, and Pensions).[15]

Thursday, December 6:
--Joint hearing to explore alternatives to fetal tissue research (House Committee on Oversight and Government Reform's Subcommittee on Healthcare, Benefits, and Administrative Rules and Subcommittee on Government Operations).[16]
--Hearing on RAY BAUM'S Act, a bipartisan foundation for bridging the digital divide (House Committee on Energy and Commerce's Subcommittee on Communications and Technology).[17]

International Hearings/Meetings –

EU – No relevant hearings.

Conferences, Webinars, and Summits –

--Medical Device Security 101 Conference – Orlando, FL (1/21/19-1/22/19)
<https://nhisac.org/events/nhisac-events/medical-device-security-101-conference/>
--FIRST Symposium 2019 – London, UK (3/18/19-3/20/19)
<https://nhisac.org/events/nhisac-events/first-symposium-2019/>
--2019 H-ISAC Spring Summit – Ponte Vedra Beach, FL (5/13/19-5/17/19)
<https://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

Sundries –

--**How to beat back botnets**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/11/29/how-to-beat-back-botnets-433977>
--**The US Leans on Private Firms to Expose Foreign Hackers**
<https://www.wired.com/story/private-firms-do-government-dirty-work/>
--**Congress: Amazon didn't give "sufficient answers" about facial recognition**
<https://arstechnica.com/tech-policy/2018/11/congress-amazon-didnt-give-sufficient-answers-about-facial-recognition/>
--**Feds: AriseBank duped investors out of over $4M in cryptocurrency scam**

[14] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108773
[15] https://www.senate.gov/committees/hearings_meetings.htm
[16] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108783
[17] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108785

<https://arstechnica.com/tech-policy/2018/11/feds-arisebank-duped-investors-out-of-over-4m-in-cryptocurrency-scam/>
--**Mass router hack exposes millions of devices to potent NSA exploit**
<https://arstechnica.com/information-technology/2018/11/mass-router-hack-exposes-millions-of-devices-to-potent-nsa-exploit/>
--**Dell Systems Hacked to Steal Customer Information**
<https://www.bleepingcomputer.com/news/security/dell-systems-hacked-to-steal-customer-information/>
--**Accenture: Russian hackers using Brexit talks to disguise phishing lures**
<https://www.cyberscoop.com/apt28-brexit-phishing-accenture/>

Contact us: follow @HealthISAC, and email at contact@h-isac.org