July 3, 2018

TLP White

We start with consumer groups urging the FTC to look into Google's and Facebook's data consent practices and then take a quick look at the new California privacy law. Then we get an update on new security coming to Wi-Fi networks and take a close look at some of the recommendations from the governments recently released Botnet Report for device manufacturers. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Looking into Google's and Facebook's Data Consent Practices.*** A recent study published by the Norwegian Consumer Council entitled *Deceived by Design*[1], has prompted a number of privacy focused organizations in the US to request that the FTC conduct an investigation into the "misleading and manipulative tactics of the dominant digital platforms in the United States, which steer users to 'consent' to privacy-invasive default settings."[2]

   The letter calls out the four areas identified by the report:

   - Privacy-intrusive default settings;
   - Illusion of choice;
   - Hiding privacy-friendly choices; and
   - Deceptive design choices.

   It is important to note that the report doesn't claim that Facebook and Google don't provide privacy choices; in fact they do, but rather that the settings are designed in such a way as to make them difficult to find or to seem like less desirable options. Take for example the facial recognition feature of Facebook. That option includes an easily identified and highlighted box that urges users to "accept the company scanning their faces for its files."[3] In contrast, the option to decline the feature is tucked away inside a page you can only see by navigating to data settings management.

[1] http://www.consumerwatchdog.org/sites/default/files/2018-06/2018-06-25%20Deceived%20by%20design%20-%20Final.pdf
[2] http://thepublicvoice.org/wp-content/uploads/2018/06/FTC-letter-Deceived-by-Design.pdf
[3] http://fortune.com/2018/06/27/google-facebook-dark-patterns-privacy/

Privacy advocates argue that presenting features in this way drives users to make decisions that benefit the companies because alternatives are not presented equally, nor are the consequences of either choice always made clear.

2. ***California Consumer Privacy Act of 2018.*** As mentioned above, California just passed the California Consumer Privacy Act of 2018.[4] Recognized as the toughest data privacy laws in the US, the Act requires that "companies that store personal information – from major players like Google and Facebook, down to small businesses – will be required to disclose the types of data they collect, as well as allow consumers to opt out of having their data sold."[5] This should sound familiar if you have been following GDPR, and we know you have. There are some differences though. Chief among them is that businesses don't have to identify the actual party that consumer data was sold to, just the category into which they fall. So for example, a business that collects and sells your data must tell you that they sold to a digital advertiser or online retailer, but not which one(s) specifically by name. Many might consider this a distinction without a difference though, since consumers can still choose to not have their data sold or shared at all.

   The law doesn't go into effect until 2020. Between now and then the government will be figuring out how to enforce the law, and we can expect tech, telecommunication, and advertising groups to continue to the fight.

3. **New and Improved Wi-Fi Security on the Horizon.** The Wi-Fi Alliance, which is overseeing the development of the new Wi-Fi Protected Access (WPA) standard, introduced Wi-Fi CERTIFIED WPA3 on June 25th.[6] WPA2, the current widely adopted standard for both personal and enterprise devices, was introduced in 2004, and while it has proven highly effective for most of that time, recent research has shown that it has some serious weaknesses. Late last year, researchers revealed that WPA2 could allow "attackers within range of [a] vulnerable device or access point to intercept passwords, e-mails, and other data presumed to be encrypted, and in some cases, to inject ransomware or other malicious content into a website a client is visiting."[7] Obviously, we don't want that.

   While improvements were made to WPA2 to address some of these concerns, as with any technology, the capability of attackers is always growing and implementing new defensive measures becomes increasingly necessary over time.

   WPA3 introduces a number of new features that not only improve security, but also make it more user-friendly. For starters, it reduces the risk to brute-force dictionary attacks by implementing Simultaneous Authentication of Equals handshake. The short

[4] https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf
[5] https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote
[6] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security
[7] https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/

story on this is that it changes the way devices and routers initiate their connection, making the collection of information needed to conduct the attack far more costly in terms of time; the attacker has to connect to the devices each time they want to guess a password, rather than being able to do it offline. This feature addresses the weakness that led to the widespread KRACK vulnerability.[8] This also includes perfect forward secrecy, meaning that if your password is compromised, old data that may have been collected previously can't be decrypted as well.

WPA3 also introduces Easy Connect, a feature that will make it far simpler to add devices to your network. This is particularly useful for IoT devices, many of which don't have a direct input mechanism for getting them configured.

Finally, WPA3 will make using public Wi-Fi networks much safer by supporting Opportunistic Wireless Encryption, which will ensure that your connection is encrypted right from the moment you connect.

As with previous versions of WPA, the rollout will take time. Some manufacturers, such as Qualcomm, have already committed to implementation, and given the benefits that WPA3 brings to the table, it seems inevitable that others will follow suit. How long it takes to be widely supported is difficult to predict, but when considered in the context of increased focus on the risk of IoT devices, there is reason to believe that adoption may be faster than we have seen in the past.

4. ***The Administration's Botnet Report and Device Manufacturers.*** Back on June 5th, we told you about the Trump Administration's recently released Botnet Report.[9] Now that industry has had a little time to process it, some of the potential implications are beginning to come into focus.

   As a reminder, the report was originally called for in an Executive Order issued in May of 2017.[10] It tasked the Department of Commerce and the Department of Homeland Security to identify actions that would "dramatically reduce threats perpetrated by automated and distributed attacks (e.g. botnets)."

   Of the twenty-four actions called for, five are particularly relevant to device manufacturers, many of whom are focused in whole or in part on medical devices.

   - **Action 1.2. The federal government should leverage industry-developed baselines, where appropriate, in establishing capability baselines for IoT devices in U.S. government environments to meet federal security**

[8] https://www.krackattacks.com/
[9] https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf
[10] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

requirements, promote adoption of industry-led baselines, and accelerate international standardization.

- **<u>Action 1.3.</u> Software development tools and processes to significantly reduce the incident of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry. The federal government should collaborate with industry to encourage further enhancement and application of these practices and to improve marketplace adoption and accountability.**

- **<u>Action 3.2.</u> Home IT and IoT products should be easy to understand and simple to use securely.**

- **<u>Action 4.3.</u> Sector-specific regulatory agencies, where relevant, should work with industry to ensure non-deceptive marketing and foster appropriate sector-specific secure considerations.**

- **<u>Action 5.2.</u> The private sector should establish voluntary labeling schemes for industrial IoT applications, supported by a scalable and cost-effective assessment process, to offer sufficient assurance for critical infrastructure applications of IoT.**

Members should log in for additional information and insight on this topic.

Congress –

<u>Tuesday, July 3</u>:
--No hearings scheduled

<u>Wednesday, July 4</u>:
--No hearings scheduled

<u>Thursday, July 5</u>:
--No hearings scheduled

Conferences, Webinars, and Summits –

--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>

--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/>
--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>
--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/>
--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 Deployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--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 –

-- **Researchers: Last Year's ICOs Had Five Security Vulnerabilities on Average** <https://www.bleepingcomputer.com/news/security/researchers-last-year-s-icos-had-five-security-vulnerabilities-on-average/>

July 3, 2018

-- **First Women-Led Cybersecurity Venture Capital Firm Launches**
<https://www.darkreading.com/cloud/first-women-led-cybersecurity-venture-capital-firm-launches/d/d-id/1332149>
-- **Firefox 61 Released for Windows, Mac, and Linux**
<https://www.bleepingcomputer.com/news/software/firefox-61-released-for-windows-mac-and-linux/>
-- **Firefox is adding 'Have I Been Pwned' alerts**
<https://www.cyberscoop.com/firefox-is-adding-haveibeenpwned-alerts/>
-- **EFF Launches Encryption Initiative for Email Domains Named STARTTLS Everywhere**
<https://www.bleepingcomputer.com/news/security/eff-launches-encryption-initiative-for-email-domains-named-starttls-everywhere/>
-- **Malware in South Korean Cyberattacks Linked to Bithumb Heist**
<https://www.darkreading.com/attacks-breaches/malware-in-south-korean-cyberattacks-linked-to-bithumb-heist/d/d-id/1332144>
-- **'Tick' espionage group is likely trying to hop air gaps, researchers say**
<https://www.cyberscoop.com/tick-espionage-usb-air-gaps-palo-alto-networks/>
-- **Private Sector Cyber-Norm Initiatives: A Summary**
<https://www.lawfareblog.com/private-sector-cyber-norm-initiatives-summary>
-- **Exclusive: Ukraine says Russia hackers laying groundwork for massive strike**
< https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-russia-hackers-laying-groundwork-for-massive-strike-idUSKBN1JM225>

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