September 11, 2018

Hacking Healthcare

TLP White

We start with a look at Australia and the development of a Consumer Data Right. We also discuss NIST's plans to create a privacy framework. We conclude by shedding some light on what went down at the 2018 Five Country Ministerial. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Australian Consumer Data Right.*** The GDPR isn't the only international privacy regime for organizations to consider. Australia's proposed Consumer Data Right ("CDR") is poised to come into effect on July 1, 2019, introducing an additional layer of international complexity to privacy compliance.

   The CDR was created to establish greater data access rights for consumers, permitting consumers to obtain some of the data that is held about them by a third party as well as enabling some of that data to be shared with accredited parties for select purposes.[1] According to the Australian treasury website, the Australian government decided to create a CDR "to give Australians greater control over their data, empowering customers to choose to share their data with trusted recipients only for the purposes that they have authorized."[2]

   Initially, the CDR will be implemented in the banking, energy, and telecommunications sectors, with plans for it to be rolled out to the entire Australian economy on a sector-by-sector basis. Additional guidance will be needed to help flesh out the CDR, including providing clarity regarding a broad definition of personal information as well as guidance around providing consent, such as what would be required for a consumer to provide their consent to disclose their personal information.

   The CDR was open for comment through September 7th, 2018. The Australian Competition & Consumer Commission ("ACCC") is scheduled to release a Rules Framework this week, which is supposed to describe how the ACCC proposes to address particular issues in the CDR Rules.[3]

[1] https://www.lexology.com/library/detail.aspx?g=a958300f-6509-49a9-a833-2c93e401aa46

[2] https://treasury.gov.au/consumer-data-right/

[3] https://www.accc.gov.au/focus-areas/consumer-data-right/rules-framework

2. ***NIST Privacy Framework.*** The National Institute of Standards and Technology ("NIST") has started to assemble the troops for another round of framework creation. NIST announced that it is starting to gather public feedback to help create a voluntary privacy framework designed to help companies protect personal information. The U.S. Department of Commerce is leading the charge, with the goal of developing a voluntary privacy framework as an enterprise risk management tool.[4]

   The privacy framework will focus on privacy risks that stem from how organizations collect, store, use, and share information to meet their mission or business goals. The privacy framework will also be designed to address information collected when customers interact with products and services and related concerns around internet connected devices. As explained by NIST Senior Privacy Policy Advisory Naomi Lefkovitz, the framework is envisioned to "provide a catalog of privacy outcomes and approaches for organizations of all kinds to: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services." To that end, businesses can discuss and resolve privacy issues using a common set of principles and understanding.

   As envisioned, the privacy framework will follow a similar creative process to that which led to the development of the 2014 Cybersecurity Framework, a mix of public meetings and feedback mechanisms that leveraged expertise from industry, civil society groups, and academic institutions. The first public workshop is scheduled for October 16, 2018 in Austin, Texas, and will be co-located with International Association of Privacy Professionals *Privacy. Security. Risk.* event. During the workshop, interested stakeholders can learn more about the process for developing the NIST Privacy Framework, ask questions directly of NIST leadership on the framework effort, and hear panels of experts discuss privacy related issues.

3. ***Encryption and the 2018 Five Country Ministerial*** The Five Country Ministerial, an annual gathering of senior security officials from Australia, Canada, New Zealand, the United Kingdom, and the United States, was held recently to discuss ways to deepen collaboration on public safety issues and to jointly confront persistent and emerging homeland security threats.[5] During the event, the senior security officials discussed a range of homeland security issues, including enhancing aviation security and border security, countering emerging threats such as those posed by weaponized or nefarious drones, confronting human trafficking, enhancing counterterrorism, mitigating cyber threats, and protecting critical infrastructure.

   The Official Communique released following the event included specific discussion around the topic of encryption. The leaders collectively agreed "that there is an urgent

[4] https://www.nist.gov/sites/default/files/documents/2018/09/04/privacyframeworkfactsheet-sept2018.pdf

[5] https://www.dhs.gov/news/2018/08/24/secretary-nielsen-travel-australia-five-country-ministerial

> need for law enforcement to gain targeted access to data, subject to strict safeguards, legal limitations, and respective domestic consultations."[6] The participating countries agreed to a Statement of Principles on Access to Evidence and Encryption, a document that sets forth a framework for discussion with industry on resolving challenges to lawful access posed by encryption in a manner that respects human rights and fundamental freedoms.[7] Specifically, the principles address mutual responsibility, the importance of the rule of law and due process, and freedom of choice for lawful access solutions.

Congress –

Tuesday, September 11:
--No relevant hearings.

Wednesday, September 12:
--No relevant hearings.

Thursday, September 13:
--Hearing entitled, "The Role of the Interagency Program Office in VA Electronic Health Record Modernization" (House Subcommittee on Technology Modernization).[8]

Conferences, Webinars, and Summits –

--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--H-ISAC Radio discussion (9/24): Cloud Security – Member-to-member discussions; link will be sent in member email.
--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/>

[6] https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018

[7] https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption

[8] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108639

September 11, 2018

--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/>
--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>
--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 –

--**'We simply haven't done enough': Facebook and Twitter execs testify on foreign influence campaigns**
<https://www.cyberscoop.com/foreign-influence-campaigns-facebook-twitter-sheryl-sandberg-jack-dorsey-congress/>
--**NSA official: Foreign hackers have ‘pummeled’ U.S. by stealing IP**
<https://www.cyberscoop.com/george-barnes-nsa-us-china-ip-theft/>
--**Cisco Releases 16 Security Alerts Rated Critical and High**
<https://www.bleepingcomputer.com/news/security/cisco-releases-16-security-alerts-rated-critical-and-high/>
--**USA Is the Top Country for Hosting Malicious Domains According to Report**
<https://www.bleepingcomputer.com/news/security/usa-is-the-top-country-for-hosting-malicious-domains-according-to-report/>
-- **WhatsApp: Mobile Phishing's Newest Attack Target**
<https://www.darkreading.com/endpoint/whatsapp-mobile-phishings-newest-attack-target/a/d-id/1332652>

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