January 5th, 2021

TLP White

Welcome to 2021! This week, *Hacking Healthcare* begins by breaking down the United States (US) National Institute of Standards and Technology's (NIST) newly published final guidance on securing Picture Archiving and Communication System (PACS). Next, we evaluate what the European Commission's approval of Google's Fitbit acquisition means for healthcare data privacy and security as technology companies continue to enter the space. Finally, we examine how Singapore's successful digital contact-tracing effort is quickly becoming a cautionary data privacy tale. Welcome back to *Hacking Healthcare*.

1. **NIST Publishes Final SP 1800-24: Securing Picture Archiving and Communication System (PACS)**

   On December 21st, NIST published the final version of *SP 1800-24: Securing Picture Archiving and Communication System (PACS)*.[1] As NIST notes, PACS is "nearly ubiquitous in healthcare environments," and is "defined by the Food and Drug Administration (FDA) as a Class II device that "provides one or more capabilities relating to the acceptance, transfer, display, storage, and digital processing of medical images."[2] As such, PACS often connects to various systems in an healthcare delivery organization's (HDO) environment, such as clinical information systems and medical devices.

   The newly finalized document comes in recognition that these kinds of connections in highly complex HDO environments can "introduce or expose opportunities that allow malicious actors to compromise the confidentiality, integrity, and availability of a PACS ecosystem."[3]

   The freely available 386-page publication includes an *executive summary*, sections on *approach*, *architecture*, *security characteristics*, and *how-to guides*.[4] As a whole, NIST believes the guidance contained within will help "HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk and protect patient privacy while maintaining the performance and usability of PACS."[5]

   Action & Analysis
   H-ISAC Membership Required

2. Google-Fitbit: Regulators at Odds Over Healthcare Data Usage

Google's growing presence in the healthcare space created significant concern among regulators and privacy advocates when their parent company, Alphabet, announced their intention to acquire Fitbit in 2019. Google's intended move came as consumer interest over healthcare-related wearables grew significantly in recent years, with Fitbit becoming one of the more notable brands.

The announcement of the acquisition was quickly followed by concerns from Fitbit owners that Google would suddenly have "access to their most intimate health information – from the number of steps they take each day to their breathing patterns, sleep quality or menstrual cycles."[6] While Fitbit attempted to assure its more than 28 million users that their data would not be sold or used for advertising, skepticism remained. This prompted various regulators to promise to investigate before signing off and led to some privacy conscious individuals requesting their Fitbit accounts and data be immediately deleted.[7]

Google's attempted acquisition of Fitbit made notable progress recently, with the European Commission finally granting its approval on December 17th.[8] This clears the way for Google to make a significant entry into the EU's "market for wearables and the nascent digital health space."[9] However, approval was subject to conditions meant to outline specifically how "Google can use the data collected for ad purposes, how interoperability between competing wearables and Android will be safeguarded and how users can continue to share health and fitness data, if they choose to."[10]

The approval and its conditions came after the European Commission led an "in-depth" investigation into the potential negative impact on competitiveness in this space, including considering data privacy and usage issues. With regards to data, The European Commission ultimately concluded that Google will have to: [11]

- Ensure they adhere to GDPR;
- Avoid using health and wellness data for Google Ads (including data collected from sensors like GPS location);
- "Maintain a technical separation of the relevant Fitbit's user data that… will be stored in a data silo"; and
- Give users in the European Economic Area the ability to grant or deny the use of health and wellness data stored in their Google Account or Fitbit Account by other Google services.

These conditions will run for a minimum of ten years, with the European Commission having the option to extend them up to ten more years. Furthermore, the European Commission requires that a trustee "will monitor the implementation of the

commitments," and that trustee will be given extensive "competences, including access to Google's records, personnel, facilities or technical information."[12]

However, outside the EU, not all regulators are onboard with this move. The Australian Competition and Consumer Commission (ACCC) announced shortly after the EU decision that it has not given its approval to Google's proposal and will continue its investigation. The ACCC currently expects a final decision will likely come by late March.[13] The ACCC Chairman has cast some doubt on its fate by saying, "we are not satisfied that a long term behavioural undertaking of this type in such a complex and dynamic industry could be effectively monitored and enforced in Australia."[14] While in the United States, there have been calls for the Justice Department and FTC to conduct their own investigation of Google.[15]

Action & Analysis
H-ISAC Membership Required

3. Singapore Gives Law Enforcement Access to Contact Tracing Data

For a time, it was hoped that digital contact tracing efforts could act as a technological solution to managing COVID-19. It was hoped that if properly implemented, it could allow the world to return to some semblance of normalcy until an effective vaccine had been distributed. In theory, taking a tried and tested medical practice and bringing it into the 21st century with mobile apps capable of logging all kinds of useful data for health authorities was an excellent idea. In practice, various hurdles related to adoption, legality, and technological limitations stymied much of its potential.

One of the more significant pushbacks that digital contact-tracing efforts faced came from privacy advocates. It was their position that this kind of system was ripe for abuse by governments unchecked by effective controls and oversight, or by criminals and other unsavory actors if such a program was improperly secured. This week, some of those fears seem more justified as the government of Singapore confirmed that law enforcement may access COVID-19 contact tracing data that is collected by their TraceTogether app.[16]

This likely came as a surprise to many as the government had previously made various assurances that this would never be the case.[17] In an effort to be "transparent", the government has gone from statements emphatically denying that anyone but "a very limited, restricted team of contact tracers" would have access, to acknowledging that "TraceTogether data may be used in circumstances where citizen safety and security is or has been affected."[18]

While the Minister-in-Charge of the Smart Nation Initiative and Minister for Foreign Affairs has said that token handed out by the government does not contain GPS functionality and therefore is not a tracking device, it's unclear if that remains true for the 2 million citizens who use to mobile app on their smartphone.[19] The government has

claimed that law enforcement has only accessed this data once so far and that it intends dismantle the app once COVID-19 has passed.[20]

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, January 5th:
- No relevant hearings

Wednesday, January 6th:
- No relevant hearings

Thursday, January 7th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

Thursday, January 7th:
- European Parliament – Committee on the Environment, Public Health, and Food Safety

Sundries –

Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again
https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

Conferences, Webinars, and Summits –

https://h-isac.org/events/

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

[1] https://csrc.nist.gov/publications/detail/sp/1800-24/final
[2] https://csrc.nist.gov/publications/detail/sp/1800-24/final
[3] https://csrc.nist.gov/publications/detail/sp/1800-24/final
[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf
[5] https://csrc.nist.gov/publications/detail/sp/1800-24/final
[6] https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data
[7] https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data
[8] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484
[9] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484
[10] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484
[11] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484
[12] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484
[13] https://thehill.com/policy/technology/531278-google-fitbit-deal-creates-rift-among-foreign-regulators

[14] https://thehill.com/policy/technology/531278-google-fitbit-deal-creates-rift-among-foreign-regulators
[15] https://thehill.com/policy/technology/531278-google-fitbit-deal-creates-rift-among-foreign-regulators
[16] https://www.bbc.com/news/world-asia-55541001
[17] https://www.zdnet.com/article/singapore-police-can-access-covid-19-contact-tracing-data-for-criminal-investigations/
[18] https://www.zdnet.com/article/singapore-police-can-access-covid-19-contact-tracing-data-for-criminal-investigations/
[19] https://www.zdnet.com/article/singapore-police-can-access-covid-19-contact-tracing-data-for-criminal-investigations/
[20] https://www.bbc.com/news/world-asia-55541001