June 2nd, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins with a troubling admission from the United Kingdom (UK) government that they conducted a large-scale COVID-19 tracking program to assess their citizens' behavior following vaccination without notifying the individuals whose data was used, raising privacy and ethical concerns. We also explore a new security directive implemented in the United States (US) that is meant to enhance pipeline security following the Colonial Pipeline attack. The directive requires significant mandatory reporting and may have long term implications for other critical infrastructure sectors like healthcare. Welcome back to *Hacking Healthcare*.

1. The UK Government's COVID-19 Tracking Raises Concerns

With many state governments around the world already struggling to overcome vaccine hesitancy among portions of their populations, it could be considered reckless to engage in an activity that undermined public trust. Unfortunately, the UK government appears to have done just that with a secretive COVID-19 tracking program that raises serious ethical and privacy concerns. While the data gleaned from the program may be useful and is allegedly within the parameters of existing laws like the General Data Protection Regulation (GDPR), the exercise raises difficult questions around what is or is not an acceptable activity in the name of 'research' as well as what should or shouldn't be considered permissible as long as data is 'anonymized'.[1]

On May 22nd, the Telegraph reported that "[m]illions of Britons had their movements 'unwittingly tracked' via their mobile phones to see if vaccinated people moved about more after their jabs."[2] This appears to have come to light through a report published by the Scientific Pandemic Influenza Group on Behaviours (SPI-B), which according to the UK government, "provides behavioural science advice aimed at anticipating and helping people adhere to interventions that are recommended by medical or epidemiological experts."[3] Apparently, the researchers used "cell phone mobility data for 10 percent of the British population" and tracked their "CDR [call data records] with corresponding location observations" to compare movement and travel distances between vaccinated and unvaccinated individuals.[4]

In defending the program, government spokesmen announced that "[a]ll the data sets used in this research are set out in the paper which makes clear that the mobile-phone location data used is GDPR compliant and has been provided from a company that collected, cleaned, and anonymised the data."[5] The government also stated its firm belief that the coarse resolution of the data collected made it impossible to identify individuals and that the program had received approval by an Oxford University Ethics committee.[6] Furthermore, the government added that data like this is "is incidental and automatically generated when people use their mobile phones and is part of the general terms and conditions."[7]

Action & Analysis
Included with H-ISAC Membership

2. **Colonial Attack Leads to DHS Pipeline Regulations**

In response to the Colonial Pipeline attack, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) issued a security directive on May 28th with the express purpose of enhancing pipeline cybersecurity. In its press release for the security directive, DHS stated that the directive will "enable [DHS] to better identify, protect against, and respond to threats to critical companies in the pipeline sector."[8] While the security directive appears to only apply to "owners and operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical," all critical infrastructure sectors should take notice.[9]

The security directive requires three "critical" actions from TSA-specified owner/operators:[10]

1. Owners and operators are to "report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA);"
2. Owners and operators are to "designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise;" and
3. Owners and operators are to "review their current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and CISA."

These actions are outlined in more depth within the 6-page security directive, but there are a few notable requirements.

First, the directive states that "information provided to CISA pursuant to this Security Directive will be shared with TSA (and vice versa) and may also be shared with the National Response Center and other agencies as appropriate."[11] That information is to be treated as "sensitive security information subject to the protections of part 1520 of title 49, Code of Federal Regulations."[12]

Second, in terms of reporting, owners and operators must report cybersecurity incidents "involving systems that the Owner/Operator has responsibility to operate and maintain" which includes:[13]

1. Unauthorized access of an Information or Operational Technology system
2. Discovery of malicious software on an Information or Operational Technology system
3. Activity resulting in a denial of service to any Information or Operational Technology system
4. A physical attack against the Owner/Operator's network infrastructure, such as deliberate damage to communication lines
5. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's pipeline systems or facilities, or otherwise has the potential to cause operational disruption that adversely affects the safe and efficient transportation of liquids and gases including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety

Furthermore, owners/operators are required to report the information listed above no later than 12 hours after a cybersecurity incident has been identified. Failure to comply with the new security guidelines would be met with fines.[14]

Action & Analysis
Included with H-ISAC Membership

Congress –

Tuesday, June 1st:
- No relevant hearings

Wednesday, June 2nd:
- No relevant hearings

Thursday, June 3rd:
- No relevant hearings

International Hearings/Meetings –

EU –

Wednesday, June 3rd:
- European Parliament - Committee on the Environment, Public Health and Food Safety

Conferences, Webinars, and Summits –
https://h-isac.org/events/

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

June 2nd, 2021

[1] *Millions 'unwittingly tracked' by phone after vaccination*. The Telegraph. 5/22/2021

[2] *Millions 'unwittingly tracked' by phone after vaccination*. The Telegraph. 5/22/2021

[3] https://www.gov.uk/government/groups/independent-scientific-pandemic-influenza-group-on-behaviours-spi-b

[4] *Millions 'unwittingly tracked' by phone after vaccination*. The Telegraph. 5/22/2021

[5] *Millions 'unwittingly tracked' by phone after vaccination*. The Telegraph. 5/22/2021

[6] *Millions 'unwittingly tracked' by phone after vaccination*. The Telegraph. 5/22/2021

[7] *Millions 'unwittingly tracked' by phone after vaccination*. The Telegraph. 5/22/2021

[8] https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

[9] https://www.documentcloud.org/documents/20791875-security-directive-on-enhancing-pipeline-cybersecurity

[10] https://www.documentcloud.org/documents/20791875-security-directive-on-enhancing-pipeline-cybersecurity

[11] https://www.documentcloud.org/documents/20791875-security-directive-on-enhancing-pipeline-cybersecurity

[12] https://www.documentcloud.org/documents/20791875-security-directive-on-enhancing-pipeline-cybersecurity

[13] https://www.documentcloud.org/documents/20791875-security-directive-on-enhancing-pipeline-cybersecurity

[14] https://www.cyberscoop.com/tsa-cyber-regulations-colonial-pipeline/