September 8th, 2022

TLP White

This week, Hacking Healthcare begins by examining a recent FTC action related to the Biden administration executive order on reproductive health that targets a data broker over the sale of identifiable location data. We consider how the FTC has begun to engage with data privacy and security issues more actively and how this case may illuminate a broader discussion on the anonymization or deidentification of sensitive data. Next, we look at how a cyberattack last July has led one country to sever all diplomatic ties with another and why the U.S. government's response seems notable. Welcome back to *Hacking Healthcare*.

1. **FTC Takes Action Related to Post-Roe Biden Executive Order Raises Anonymization Questions**

   With the overturning of Roe v. Wade, the Biden administration engaged in activities designed to blunt the effects of the U.S. Supreme Court decision. Several of these efforts were outlined in an executive order that included encouraging the Federal Trade Commission (FTC) to take steps to protect consumer privacy and address deceptive or fraudulent practices. A recent FTC action to sue an organization over the selling of location data that could link individuals to visits to abortion clinics may offer a glimpse into how the FTC plans to follow through, while simultaneously asking questions about anonymization.

   As a brief reminder, in response to the overturning of Row v. Wade, President Biden signed an executive order *on Protecting Access to Reproductive Healthcare Services*. This executive order was designed to "defend reproductive rights," by: Safeguarding access to reproductive health care services, including abortion and contraception; Protecting the privacy of patients and their access to accurate information; Promoting the safety and security of patients, providers, and clinics; and Coordinating the implementation of Federal efforts to protect reproductive rights and access to health care.

   For their part, the FTC was asked "to consider taking steps to protect consumers' privacy when seeking information about and provision of reproductive health care services," and aid in "[considering] options to address deceptive or fraudulent practices, including online, and protect access to accurate information."[i] This particular FTC action would appear to tie directly back to this ask.

In a filing to the U.S. District Court for the District of Idaho made on August 29th, the FTC alleges that Kochava violated the FTC Act by "acquiring consumers' precise geolocation data and selling the data in a format that allows entities to track the consumers' movements to and from sensitive locations."[ii] The filing describes the relative ease by which tens of millions of unique IDs with sensitive location data could be acquired by nearly anyone with a personal email address who stated that it was for "business" uses.[iii]

The FTC alleges that this data could be used to identify people and track them to sensitive locations such as healthcare or abortion clinics. The filing states that it is possible to use the geolocation data and the unique identifier for each ID to identify the user or owner of the device. Furthermore, with enough of the geolocated data one could likely identify device ownership by tracking where a device is at night when the owner is likely asleep or, where the device is during the day to determine the device owners place of employment. Additionally, the FTC filing alleges that "Kochava employs no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations."[iv]

The FTC maintains that this practice could cause consumers harm and qualifies as a violation of the FTC Act for unfair or deceptive acts or practices. The case is ongoing.

Action & Analysis

Included with H-ISAC Membership

2. **Albania Severs Diplomatic Relations with Iran Over Cyberattack**

On Wednesday, the government of Albania severed all diplomatic relations with Iran over a cyberattack it believes they carried out back in July. The Albanian response is among the most significant public government reactions to a cyber incident, and it comes at a time when numerous other national governments have suffered debilitating cyberattacks. The response raises questions about what cyber actions cross the line, what is an appropriate response for a government, and should attacks against critical infrastructure sectors, like healthcare, be treated more seriously.

For context, the Albanian government suffered a cyberattack in July that Albanian Prime Minister Rama described as one that "threatened to paralyse public services, erase digital systems and hack into state records, steal government intranet electronic communication and stir chaos and insecurity in the country."[v]

With support from the United States, Albania has spent weeks investigating and remediating the incident. In doing so, they allege to have found evidence to confidently attribute the "orchestration" and "sponsorship" of the attack to the Iranian government. Albania has since ordered the removal of Iranian diplomats and embassy staff, while officially calling an end to diplomatic relations with that country. The prime minister of Albania is quoted as saying that "This extreme response ... is fully proportionate to the gravity and risk of the cyberattack."[vi]

The White House released a statement echoing Albania's concerns and called it an "unprecedented cyber incident" that "[disregarded] norms of responsible peacetime State behavior in cyberspace, which includes a norm on refraining from damaging critical infrastructure that provides services to the public."[vii] They also promised to hold Iran accountable for actions that "threaten the security of a U.S. ally and set a troubling precedent for cyberspace."[viii]

Action & Analysis
Included with H-ISAC Membership

Congress -

Tuesday, September 6th:
- No relevant hearings

Wednesday, September 7th:
- No relevant hearings

Thursday, September 8th:
- No relevant hearings

International Hearings/Meetings -

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits

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

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

About the Author
Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

[i] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/
[ii] https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf
[iii] https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf
[iv] https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf
[v] https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/
[vi] https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/
[vii] https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/
[viii] https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/