September 1st, 2022

Hacking Healthcare

TLP White

This week, Hacking Healthcare begins by examining the Federal Trade Commission's proposed rulemaking on harmful commercial surveillance and lax data security. We briefly explain why healthcare sector members might want to engage with the FTC's process, despite its potential completion being many years from now. Then, we break down some takeaways from a recent ransomware attack that put a French hospital out of commission, including what to make of the prevalence of healthcare sector attacks, as well as posing questions about the role of government.

Welcome back to *Hacking Healthcare*.

1. FTC Announces Rulemaking on Commercial Surveillance and Lax Data Security Practices

On August 11, the Federal Trade Commission (FTC) announced that it is "exploring rules to crack down on harmful commercial surveillance and lax data security practices."[1] Citing the enormous scale by which personal information is collected and used, alongside the heightened risks and harms associated with data breaches and data misuse, the FTC released an Advance Notice of Proposed Rulemaking (ANPR) to seek public comment "on whether new rules are needed to protect people's privacy and information."[2] However, this particular rulemaking process, its potential impacts on the healthcare sector, and its overall goals are not quite as straightforward as they might seem.

FTC Chair Lina Khan remarked that the growing digitization of the economy and business models that often incentivize companies to collect sensitive user data may mean that "potentially unlawful practices may be prevalent."[3] Khan described this initial step toward a rulemaking as a way to "begin building a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices and what those rules should potentially look like."[4]

The ANPR was subsequently published on August 22 in the Federal Register, which goes into far greater detail as to why the FTC feels this approach is needed, what specifically it is interested in getting feedback on, and how organizations can engage.[5]

Reasons for Rulemaking: While the FTC has previously used existing authorities under the FTC Act to take enforcement actions against organizations that have committed privacy and data security violations, including when health-related data has been shared with third parties, the FTC stated that its past work suggests that enforcement of the FTC Act alone may not be enough to protect consumers.[6]

Issue Under Consideration: The ANPR contains more than 90 questions that fit broadly into a number of categories, including Data Security, the Collection, Use, Retention, and Transfer of Consumer Data, Automated Decision-Making Systems, and the scale and harm of commercial surveillance practices or lax security measures.

Specific questions include:

- Which measures do companies use to protect consumer data?
- Should the Commission commence rulemaking on data security?
- Should new rules require businesses to implement administrative, technical, and physical data security measures, including encryption techniques, to protect the security, confidentiality, or integrity of covered data?
- To what extent, if at all, should the Commission require firms to certify that their data practices meet clear security standards?

Engagement: Organizations interested in engaging with the FTC on this matter are able to submit written comments on the Federal Register website by October 21.[7] Furthermore, the FTC will hold a public forum on Thursday, September 8, 2022, from 2 p.m. until 7:30 p.m. Eastern time. The public forum will be available virtually.

Action & Analysis
*Membership required**

2. French Hospital Diverts Patients Following Cyber Attack

In what feels like is becoming an increasingly common occurrence, another major hospital has been hit by a crippling malware attack that has impacted operational capabilities and put patients at risk. While the increase in incidents like this highlights the need for healthcare delivery organizations to better resource cybersecurity and resiliency, the incidents also raise questions about what the appropriate government response is to these sorts of reckless and potentially deadly attacks.

On August 21, it was reported that a major hospital in France, the Centre Hospitalier Sud Francilien (CHSF), was hit by a ransomware attack that left it struggling to provide emergency services and forced it to transfer and divert patients to other facilities. The attack also forced the rescheduling of surgeries and other procedures reliant on technology.[8] The attack crippled the hospital's entire network, including storage systems for medical imaging as well as IT systems linked to patient admissions. Consequently, staff were left handling patient data manually.[9]

Reports have since come out that have attributed the attack to the LockBit ransomware group, whose demand of $10M for the decryption key was allegedly refused by the hospital.[10, 11] CHSF reportedly contacted the French national cybersecurity agency, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), shortly after the incident, and the agency has been helping with the response. Additional government action was taken by the Paris prosecutor's office, which opened an investigation that is being led by the national gendarmerie.[12]

Action & Analysis
Membership required

Congress

Tuesday, August 30th:
- No relevant hearings

Wednesday, August 31st:
- No relevant hearings

Thursday, September 1st:
- 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.

[1] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices?source=email

[2] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices?source=email

[3] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices?source=email

[4] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices?source=email

[5] https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

[6] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices?source=email

[7] https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

[8] https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/

[9] https://therecord.media/lockbit-ransomware-group-implicated-in-crippling-attack-on-french-hospital/

[10] https://therecord.media/lockbit-ransomware-group-implicated-in-crippling-attack-on-french-hospital/

[11] https://www.france24.com/en/europe/20220823-cyber-attackers-disrupt-services-at-french-hospital-demand-10-million-ransom

[12] https://therecord.media/lockbit-ransomware-group-implicated-in-crippling-attack-on-french-hospital/