October 11, 2022

TLP White

This week, Hacking Healthcare begins by investigating what a recent Biden administration Executive Order means for the future of EU-U.S. transatlantic data flows. We break down what just happened, what to expect in the coming months, and what Health-ISAC members should consider doing about it. Next, we investigate a new report that suggests that American consumers are taking cybersecurity and privacy more seriously and assess what that might mean for the healthcare sector.

Welcome back to *Hacking Healthcare*.

1. **Another Step Toward a New Transatlantic Data Privacy Framework for the EU and U.S.**

   Transatlantic data flows between the European Union and the United States have been marred for many years due to legal challenges that cite the seemingly irreconcilable differences in data privacy and protections required by the EU and the surveillance functions allowed by the United States. Several attempts at creating a legal mechanism to satisfy both parties have fallen apart in EU courtrooms, but the economic need for unimpeded transatlantic data flows means both parties have once again attempted to find a workaround. A recent Biden Executive Order has pushed the effort one step closer to completion, but will this new approach really solve the issues that doomed previous mechanisms?[1]

   To put this in context, let's quickly recap how we got here. Transatlantic data flows between the EU and the United States have made use of several mechanisms in the past, including the International Safe Harbor Principles and the EU-US Privacy Shield. Ultimately, these mechanisms have been struck down in EU court because they failed to provide necessary data privacy protections to keep EU data safe from U.S. government surveillance. The EU and United States have continued to work together to craft replacements that have often been criticized as "papering over the cracks" rather than solving the underlying issues. The EU-US Data Privacy Framework (EU-US DPF) is the latest of these attempts.

In order to make progress on the new framework, the Biden administration signed an Executive Order last week that was meant to address concerns that were brought up in the more recent EU ruling that invalidated the EU-US Privacy Shield.

According to a White House press release, the new Executive Order "bolsters an already rigorous array of privacy and civil liberties safeguards for U.S. signals intelligence activities."[2] The White House specifically points out that the new Executive Order will create a "multi-layer" mechanism for individuals from particular states or "regional economic integration organizations" to "obtain independent and binding review and redress of claims that their personal information" was collected by U.S. signals intelligence.[3] This includes the creation of a new Data Protection Review Court.

As for what comes next, it will now be up to the European Commission to prepare a draft adequacy decision and begin an adoption procedure.[4] While EU officials have said it may take upwards of six months to work through these next steps, should they go smoothly, "data will be able to flow freely and safely between the EU and US companies certified by the Department of Commerce under the new framework. US companies will be able to join the framework by committing to comply with a detailed set of privacy obligations."[5, 6]

Actions and Analysis

Membership required

2. Americans Becoming More Cybersecurity and Privacy Conscious

Those in the cybersecurity and privacy fields have lamented the ambivalence or general lack of awareness and education that the average American has toward cybersecurity and privacy. According to a new report from Consumer Reports and the Aspen Institute, there is evidence to suggest that is changing within the United States and that individuals are increasingly security and privacy conscious.

The nine-page report, released on October 4, stated that "[t]he findings comprise results from a nationally representative survey of 2,103 US adults" taken from this past June.[7] Its overarching finding is that "consumer privacy and security practices have increased over the years as consumers have made changes to update and protect themselves and their personal information or data."[8] Some of the changes noted between 2019 and 2022 are striking:[9]

- Consumers identifying as using strong passwords to access home WiFi or Network jumped 14 percentage points from 74% to 88%.

- Consumers saying they currently use multi-factor authentication (MFA) jumped 27 percentage points from 50% to 77%.

- Consumers saying they will not install apps on a smartphone if they collect too much personal information or do not protect it adequately rose 9 percentage points from 71% to 80%.

However, other security and privacy habits saw significantly less of an uptick:[10]

- Consumers saying they use password managers rose three percentage points from 36% to 39%.

- Consumers saying they use a VPN rose a single percentage point, from 34% to 35%.

Other notable takeaways:[11]

- 48% of consumers said they are either not too confident or not confident at all that personal data, such as Social Security numbers, health history, and financial information, is private and not distributed without their knowledge.

- In terms of who consumers think should be responsible for protecting the online privacy of Americans, there was an eight percentage point uptick from 17% to 25% of those who said consumers should be most responsible and a ten percentage point decline in those holding companies most responsible.

Actions and Analysis

Membership required

Congress

<u>Tuesday, October 10th:</u>
- No relevant hearings

<u>Wednesday, October 11th:</u>
- No relevant hearings

<u>Thursday, October 12th:</u>
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Monday, October 10th:
- 7th eHealth Security Conference (ENISA)

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, 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.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/
[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/
[4] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045
[5] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045
[6] https://www.reuters.com/technology/biden-signs-order-implement-eu-us-data-privacy-framework-2022-10-07/
[7] https://www.consumerreports.org/media-room/press-releases/2022/10/consumer-reports-and-aspen-institute-reveal-consumer-attitudes-towards-cybersecurity-and-online-privacy/
[8] https://consumer-reports-ressh.cloudinary.com/image/upload/v1664551562/Consumer-Cyber-Readiness-Report-Final_edbv9f.pdf
[9] https://consumer-reports-ressh.cloudinary.com/image/upload/v1664551562/Consumer-Cyber-Readiness-Report-Final_edbv9f.pdf
[10] https://consumer-reports-ressh.cloudinary.com/image/upload/v1664551562/Consumer-Cyber-Readiness-Report-Final_edbv9f.pdf
[11] https://consumer-reports-ressh.cloudinary.com/image/upload/v1664551562/Consumer-Cyber-Readiness-Report-Final_edbv9f.pdf