April 12, 2022

TLP White

This week, *Hacking Healthcare* provides an update on the newly developing Trans-Atlantic Data Privacy Framework that would replace the EU-US Privacy Shield that was invalidated in 2020. We will break down what we know of the new agreement, what its chances are of holding up to legal challenge, how long it may take to implement, and what companies should do in the interim. Then we take a look at a recent UK National Cyber Security Centre (NCSC) blog post on the risk associated with using technologies, products and services with ties to Russia, and tie it into a larger discussion around risk management.

Welcome back to *Hacking Healthcare*.

1. **EU-US Privacy Shield Rework**

   From July 2016 to July 2020, the transfer of personal data between the United States and the European Union (EU) was facilitated under the EU-US Privacy Shield. However, legal challenges to the process led to its invalidation. In the time since, companies have been uneasily working around the lack of a formal process, with many concerned that the legal exposure may force them to cease or significantly alter operations. After an anxiety-filled wait, representatives of the United States and EU have announced a preliminary deal for a new version. So, what's changed, and will this iteration, the third such attempt, fare any better in court?

   As a brief background, The EU-US Privacy Shield, and its predecessor, were meant to provide a process for the "lawful transfer of personal data from the EU to the United States, while ensuring a strong set of data protection requirements and safeguards."[1] This was needed because of the more comprehensive data protections within EU law that require such data to retain an adequate level of protection to whatever other jurisdictions it may travel.

   The issue has been that each time the EU and the United States have come up with some form of framework or process, it has been struck down by a determination from

the Court of Justice of the European Union (CJEU) on the grounds that it does not meet those adequacy requirements. As the European Parliament states, the decision to invalidate is "on account of invasive US surveillance programmes."[2]

New Framework

On March 25th, the White House released a fact sheet outlining their commitment to a new "Trans-Atlantic Data Privacy Framework."[3] In it, the White House addressed the noted surveillance issue by stating that the United States is "committed to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, which will ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities."[4]

In particular, the fact sheet outlined how the United States had made commitments to:[5]

- Strengthen the privacy and civil liberties safeguards governing U.S. signals intelligence activities;
- Establish a new redress mechanism with independent and binding authority; and
- Enhance its existing rigorous and layered oversight of signals intelligence activities.

The White House also provided some additional examples of how signals intelligence would be limited, how EU individuals could seek redress, and how additional layers of oversight and civil liberties standards would be adopted.[6] The European Commission's own fact sheet touted the "durable and reliable legal basis" this new agreement in principle is founded on and that it would adequately address the concerns raised in past court rulings.[7]

However, the process is still some way from being complete, and what has been agreed to lacks the technical specifics to determine exactly what the new process will look like. As the European Commission outlines, "The agreement in principle will now be translated into legal documents. The U.S. commitments will be included in an Executive Order that will form the basis of a draft adequacy decision by the Commission to put in place the new Trans-Atlantic Data Privacy Framework."[8] It will likely take many months for both sides to work through their respective next steps, and in the meantime, some individuals and institutions have already questioned the new process, and have indicated their intent to challenge it in court if implemented.[9]

Action & Analysis

2. UK NCSC Warns of Russian Technology, Products, and Services Use

At the end of last month, the United Kingdom's (UK) National Cyber Security Centre (NCSC) published a blog post on the *Use of Russian Technology Products and Services Following the Invasion of Ukraine*.[10] Written by Ian Levy, the NCSC's Technical Director, the post warns of the cybersecurity risks associated with continuing to use Russian technology, products, and services, while importantly cautioning organizations from implementing hurried or unplanned transitions.

Levy outlined his skepticism that the worst predictions of massive offensive cyber operations stemming from the Ukraine conflict will come to pass. However, he cautioned that there are clear risks when "using 'cloud-enabled products' where the supply chain included hostile states, such as Russia," and that those risks may increase during wartime.[11] In Levy's view, while there is no evidence that the "Russian state intends to suborn Russian commercial products and services to cause damage to UK interests," that doesn't mean it isn't prudent to prepare for it.[12]

Some organizations should take this message more seriously according to Levy and the NCSC, including those related to critical national infrastructure, such as Chemicals, Emergency Services, and Health. While Levy acknowledged the limited usefulness of generic advice, he did offer up the following:

- If you are more likely to be a target for the Russian state because of what's going on, then it would be prudent to consider your reliance on all types of Russian technology products or services (including, but not limited to, cloud-enabled products such as anti-malware).

- If you use services that are provided out of Russia (including development and support services), then you should think about how you could insulate yourself from compromise or misuse of these services. This is true whether you contract directly with a Russian entity, or it just so happens that the people who work for a non-Russian company are located in Russia.

Action & Analysis

Congress

Tuesday, April 12th:
- No relevant hearings

Wednesday, April 13th:
- No relevant hearings

Thursday, April 14th:
- No relevant hearings

April 12, 2022

International Hearings/Meetings

- No relevant meetings

EU –

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.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

[2] https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[6] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[7] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087

[8] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087

[9] https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems

[10] https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine

[11] https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine

[12] https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine