Episode 339: The Privacy and Europocrisy Oversight Board

November 23, 2020

Overview

Download the 339th Episode (mp3).
Subscribe to The Cyberlaw Podcast:
This is my favorite story of the episode. David Kris covers a report from the Privacy and Civil Liberties Oversight Board on the enormous value that European governments get in fighting terrorism from the same American surveillance programs that European institutions have been fighting for twenty years to shut down. It's a delightful takedown of European virtue-signaling, and I hope the Biden Administration gives the PCLOB a new name and mission in honor of the report.

But we begin the news roundup with a review of the US-China tech relationship and how it might change under a Biden administration. The Justice Department has issued itself a glowing report card for its contribution to decoupling—the opening of new China-related counterintelligence case every 10 hours. I wonder how long this can go on before China starts arresting American businessmen—and kicks off another round of decoupling.

Speaking of decoupling, the latest legislation aimed at prison labor in China may be getting uncomfortably close to hitting Apple, which is quietly lobbying to water down a bill that most of us expect to pass soon by overwhelming majorities. Megan Stifel and I conclude that the provision that probably scares Apple most is an obligation to make representations about whether the company’s products include parts made with prison labor. That is increasingly difficult to figure out as China has limited audits for such purposes, putting Apple in an increasingly tight spot. Sympathy for Tim Cook is in short supply.

Speaking of legacy burnishing, the Trump White House has issued its own set of guidelines for federal agencies using artificial intelligence. Nick Weaver thinks it’s actually not bad—light touch on most topics—which may be the nicest thing he’s said about a product of this White House in four years. Sticking with AI, Nick comments on the prospect for putting humans in the loop of AI decision making. He thinks that’s a recipe for lousy AI, and that campaigns to get a “Human in the Loop” for lethal systems have already lost the technology fight. At best, we can hope to have our poky old brains “on the loop” in future AI conflicts.

More good news: An IOT security bill that Megan and I both like (Megan more than I) and that Congress has passed and sent to the President for signature. It only sets standards for IOT that the federal government buys, but that’s a good first step.

As a former NSAer, I explain “GCHQ envy” to David, and he provides the latest reason why it must be rampant at the Fort this year, as the agency introduces a new offensive cyber unit to take on organized crime and hostile states.

David also takes on the question whether there’s a legal problem with the US military buying location data from apps companies. Short answer: No. More.

Megan explains a now-patched Facebook Messenger bug that would have allowed hackers to listen in on users. Nick tells us why the FBI needed to hire robots to retrieve sensitive files. Megan gives us some staggering statistics about the prevalence of ransomware. Hint: if you thought COVID-19 was a pandemic, you ain’t seen nothin’ yet. I give a quick summary of the TikTok and WeChat ban litigation, where the government is unlimbering a host of new technical arguments.

I give a shoutout to Sean Joyce, whose principles led him to walk away from what is probably going to be serious money when Airbnb goes public. The company’s leadership let him argue against giving data about individual users to the Chinese government before the users actually move in. But the debate ended when one of the execs opined, “We’re not here to promote American values.” That may not be a good look for Airbnb, but it is for Joyce, who left the company within weeks over the principle.

And, finally, it turns out that the FCC is in its last weeks of Trump legacy burnishing; facing a deadline in January 2020, it had to choose between starting to write regulations about the scope of section 230 and dealing with foreign products in the 5G infrastructure. It chose 5G.

And more.

As always, The Cyberlaw Podcast is open to feedback. Be sure to engage with @stewartbaker on Twitter. Send your questions, comments, and suggestions for topics or interviewees to CyberlawPodcast@steptoe.com. Remember: If your suggested guest appears on the show, we will send you a highly coveted Cyberlaw Podcast mug!

The views expressed in this podcast are those of the speakers and do not reflect the opinions of their institutions, clients, friends, families, or pets.

Practices
Privacy & Cybersecurity

© 2021 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.