THE CYBERLAW PODCAST

Episode 338: Trump's Multiple Re-Entry China Policy Vehicles

November 16, 2020

Overview

Download the 338th Episode (mp3).

Subscribe to The Cyberlaw Podcast:
Another week, another Trump administration initiative to hasten the decoupling from China. As with MIRV warheads, the theory seems to be that the next administration can’t shoot them all down. Brian Egan lays out this week’s initiative, which lifts from obscurity a DoD list of Chinese military companies and excludes them from US capital markets.

Our interview is with Frank Cilluffo and Mark Montgomery. Mark is Senior Fellow at the Foundation for Defense of Democracies and Senior Advisor to the congressionally mandated Cyberspace Solarium Commission. Previously, he served as Policy Director for the Senate Armed Services Committee under Senator John S. McCain—and before that served for 32 years in the US Navy as a nuclear trained surface warfare officer, retiring as a Rear Admiral in 2017. Frank is director of Auburn University’s Director of Auburn University’s McCrary Institute for Cyber and Critical Infrastructure Security. He served on the Cyberspace Solarium Commission and chaired the Homeland Security Advisory Council’s subcommittee on economic security. We talk about the unexpected rise of the industrial supply chain as a national security issue. Both Frank and Mark were moving forces in two separate reports highlighting the issue, as was I. So, if we seem suspiciously agreed on important issues, it’s because we are. Still, as an introduction to one of the surprise hot issues of the year, it’s not to be missed.

After our interview of a Justice Department official on how to read Schrems II narrowly, it was only a matter of time. Charles Helleputte reviews the EDPB’s effort to give more authoritative and less comfortable advice to US companies that want to keep relying on the standard contractual clauses. Still, the Justice Department take on the topic manages to squeak through without a direct hit from the privacy bureaucrats. Still, the EDPB (and the EDPS even more) makes clear that anyone following the DOJ’s lead is in for an uphill fight. For those who want more of Charles’s thinking on the topic, see this short piece.

Zoom has been allowed to settle an FTC proceeding for deceptive conduct (claiming that its crypto was end to end when it wasn’t, and more). Mark MacCarthy gives us details. I rant about the FTC’s failure to ask any serious national security questions about a company that deserves some. Brian brings us up to speed on TikTok. Only one of the Trump administration penalties remains unenjoined. My $50 bet with Nick Weaver that CFIUS will overcome judicial skepticism that EEEPA could not is hanging by a thread. Casey Stengel makes a brief appearance to explain how TikTok might win.

Brian also reminds us that export control policymaking is even slower and less functional on the other side of the Atlantic, as Europe tries, mostly ineffectively, to adopt stricter limits on exports of surveillance tech.

Mark and I admire the new Aussie critical-infrastructure cybersecurity initiative, mostly for its clarity if not for its political appeal.

Charles explains and I decry the enthusiasm of European courts for telling Americans what they can say and read on line. Apparently, we aren’t allowed to post on Facebook that political censorship is what members of a fascist party tend to advocate; but don’t worry about our liability; we can’t pronounce the plaintiff’s name. Faschy McFarschface, though, that I can pronounce.

So, in retrospect, how did we do in policing all the new cyberish threats to the 2020 election? Brian gives the government credit for preventing foreign interference. I question the whole narrative of foreign interference (other than the hack and dump operation against the DNC) in 2016 and 2020, noting how conveniently it serves Democratic messaging (Hillary only lost because of the Russians! Ignore Trump’s corruption allegations because it’s more Russian interference!). Mark and I wonder that Silicon Valley thinks it’s accomplishing with its extended bans on political advertising after the election. They’re going to find out it’s almost always election season somewhere (see, e.g., Georgia). DHS’s CISA produced a detailed rumor control site that may have corrected one too many of the President’s tweets. Chris Krebs, familiar to Cyberlaw Podcast listeners, may be on the chopping block. That would be a shame for DHS and CISA; for Chris it's probably a badge of honor. Frank Cilluffo and Mark Montgomery weigh in with praise for Chris as well.

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.