

LAWFARE

The Cyberlaw Podcast: Challenging Edward Snowden

Stewart Baker

October 4, 2019

In this episode I cross swords with John Samples of the Cato Institute on Silicon Valley's efforts to disadvantage conservative speech and what to do about it. I accuse him of Panglossian libertarianism; he challenges me to identify any way in which bringing government into the dispute will make things better. I say government is already in it, citing TikTok's People's Republic of China-friendly "community standards" and Silicon Valley's obeisance to European standards on hate speech and terror incitement. Disagreeing on how deep the Valley's bias runs, we agree to put our money where our mouths are: I bet John \$50 that Donald J. Trump will be suspended or banned from Twitter by the end of the year in which he leaves office.

There's a lot of news in the Roundup. David Kris explains the background of the first CLOUD Act agreement that may be signed this year with the UK.

Nate Jones and I ask, "What is the president's beef with CrowdStrike, anyway?" And find a certain amount of common ground on the answer.

This Week in Counterattacks in the War on Terror: David and I recount the origins and ironies of Congress's willingness to end the NSA 215 phone surveillance program. We also take time to critique the *New York Times*'s wide-eyed hook-line-and-sinker ingestion of an EFF attack on the FBI's use of National Security Letters.

Edward Snowden's got a new book out, and the Justice Department wants to make sure he never collects his royalties. Nate explains. I'm just relieved that I will be able to read it without having to shoplift it. And it seems to be an episode for challenges, as I offer Snowden a chance to be interviewed on the podcast—anytime, anywhere, Ed!

Matthew Heiman explains the latest NotPetya travail for FedEx: A shareholder suit alleging that the company failed to disclose how much damage the malware caused to its ongoing business.

Evan Abrams gives a hint about the contents of Treasury's 300-page opus incorporating Congress's overhaul of CFIUS into the CFR.

I credit David for inspiring my piece questioning how long end-to-end commercial encryption is going to last, and we note that even the *New York Times* seems to be questioning whether Silicon Valley's latest enthusiasm is actually good for the world.

Matthew tells us that China may have a new tool in the trade war—or at least to keep companies toeing the party line: The government is assigning social credit scores to businesses.

Finally, Matthew outlines France's OG take on international law and cyber conflict. France opens up some distance between its views and those of the United States, but everyone will get a chance to talk at even greater length on the topic, as the U.N. gears up two different bodies to engage in yet another round of cyber-norm-building.