Our interview this week is a deep dive into the mess created by the EU Court of Justice in Schrems II – and some pretty good ideas for how companies might avoid the mess as proposed in a US Government white paper. I interview Brad Wiegmann, Senior Counselor for the National Security Division at the US Department of Justice. We cover a host of arguments and new facts that may help companies navigate the wreckage of Privacy Shield and preserve the standard corporate clauses they’ve relied on for trans-Atlantic data transfers. And, yes, the phrase “hypocritical European imperialism” does cross my lips.

In the news, we can’t let election eve pass without a look at all the election security threats and countermeasures now being deployed. I argue that the election security threat is the second coming of Y2K – a threat that is almost certainly an overhyped bogeyman, but one we can’t afford to ignore. Jamil Jaffer and Pete Jeydel push back. Silicon Valley’s effort to ensure that no one questions the legitimacy of a Biden victory also comes in for some criticism on my end – and is defended by Nate Jones. My candidate for flakiest Silicon Valley technonostrum is banning post-election political ads. That just guarantees that speech about the election will default to the biggest “organic” voices on the internet and to the speech police at each platform.

Confused about all the TikTok and WeChat litigation? The cheat sheet guide is that the US hasn’t won a single case, and it’s gone down hard in three separate opinions, the latest by US District Judge Beetlestone of Philadelphia. This could be Trump Derangement at work, but the fact is that the Chinese platforms have a plausible argument that Congress prohibited IEEPA bans that indirectly regulate distribution of speech. Banning a social platform might seem to fit that exception, but the result is crazy: it implies that TikTok could replay all the Russian election interference memes from 2016, and the government would be helpless to stop it. On appeal, we may see the courts taking a broader view of the equities. Or they may be tempted to say, “Well, Congress screwed this up, let Congress unscrew it.” If Joe Biden wins the election, I can’t imagine an issue he’d most want to keep off his plate.

Nate and I try to sum up what we learned from the social media speech suppression hearing on the Hill. Nate sees no common ground emerging despite wide unhappiness with Silicon Valley’s role in regulating speech. I am more optimistic that a Congress looking to make progress could agree on first steps toward transparency in speech suppression practices on the platforms. The companies themselves seem to have decided that this is table stakes as they strive to avoid worse.

Nate gives us a quick view of the platform speech debate in Europe. My summary: Silicon Valley is already incentivized by EU law to oversuppress; now they’re asking for immunity when they oversuppress, which means, of course, even less speech.

In quick hits, Pete talks about the ransomware threat to US health care. Nate explains the tensions between law enforcement and intelligence in Canada. And Pete tells us why fertility clinics are the latest national security concern for CFIUS.

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