Episode 342: Could European Privacy Law Protect American Child Molesters?

December 15, 2020

Overview

Download the 342nd Episode (mp3).

Subscribe to The Cyberlaw Podcast:
Our interview is with Alex Stamos, who lays out a complex debate over child sexual abuse that’s now roiling Brussels. The application of European privacy standards and AI hostility to internet communications providers has called into question the one tool that has reduced online child sex predation. Scanning for sex abuse images works well, and even scanning for signs of “grooming” is surprisingly effective. But they depend on automated monitoring of communications content, something that has come as a surprise to European lawmakers hoping to impose more regulation on American tech platforms. Left unchanged, the new European rules could make it easier to abuse American kids. Alex explains the rushed effort to head off that disaster – and tells us what Ashton Kutcher has to do with it (a lot, it turns out).

Meanwhile, in the news roundup, Michael Weiner breaks down the FTC’s (and the states’) long-awaited antitrust lawsuit against Facebook. Maybe the government will come up with something as the case moves forward, but its monopolization claims don’t strike me as overwhelming. And, Mark MacCarthy points out, the likelihood that the lawsuit will do something good on the privacy front is vanishingly small.

Russia’s SVR, heir of the KGB, is making headlines with a remarkably sophisticated and well-hidden cyberespionage attack on a lot of institutions that we hoped were better at defense than they turned out to be. Nick Weaver lays out the depressing story, and Alex offers a former CISO’s perspective, arguing for a federal breach notification law that goes well beyond personal data and includes disciplined after-action reports that aren’t locked up in post-litigation gag orders. Jamil Jaffer tells us that won’t happen in Congress any time soon.

Jamil also comments on the prospects for the National Defense Authorization Act, chock full of cyber provisions and struggling forward under a veto threat. If you’re not watching the European Parliament tie itself in knots trying to avoid helping child predators, tune in to watch American legislators tie themselves into knots trying to pass an important defense bill without drawing the ire of the President.

The FCC, in an Ajit Pai farewell, has been hammering Chinese telecoms companies. In one week, Jamil reports, the FCC launched proceedings to kick China Telecom out of the US infrastructure, reaffirmed its exclusion of Huawei from the same infrastructure, and adopted a “rip and replace” mandate for US providers who still have Chinese gear in their networks.

Nick and I clash over the latest move by Apple and Google to show their contempt for US counterterrorism efforts – the banning of a location data company whose real crime was selling the data to (gasp!) the Pentagon.

Mark explains the proposals for elaborate new regulation of digital intermediaries now working their way through – where else? – Brussels. I offer some cautious interest in regulation of “gatekeeper” platforms, if only to prevent Brussels and the gatekeepers from combining to slam the Overton window on conservatives’ fingers.

Mark also reports on the Trump administration’s principles for US government use of artificial intelligence, squelching as premature my celebration at the absence of “fairness” and “bias” can’t.

Those who listen to the roundup for the porn news won’t be disappointed, as Mark and I dig into the details of Pornhub’s brush with cancellation at the hands of Visa and Mastercard – and how the site might overcome the attack.

In short hits, Nick and I disagree about Timnit Gebru, the “ethicist” who was let go at Google after threatening to quit and who now is crying racism. I report on the enactment of a modest but useful IoT Cybersecurity law and on the doxxing of the Chinese Communist Party membership rolls as well as the adoption of the most law-enforcement-hostile technology yet to come out of Big Tech – Amazon’s Sidewalk.

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.