In our 324th episode of the Cyberlaw Podcast, Stewart Baker interviews Bruce Schneier, internationally recognized security technologist, lecturer, and author, including the works *Click Here to Kill Everybody*. Stewart is also joined by Megan Stifel (@MeganStifel), Nate Jones (@n8jones81), and David Kris (@DavidKris).

Our interview is with Bruce Schneier, who has coauthored a paper about how to push security back up the Internet-of-things supply chain. His solution is hard on IOT affordability and hard on big retailers and other middlemen, who will face new liabilities, but we conclude that it’s doable. In fact, the real question is who’ll get there first, a combination of DHS’s CISA and the FTC or the California Secretary of State.

We also discuss:
How it must feel to TikTok as though the shot clock is winding down. Administration initiatives that could hurt or kill its US business are proliferating. Nate Jones, Megan Stifel, and I explore the government’s options. The most surprising, and devastating, of them is a simple ban on TikTok as a threat to national security or the security of Americans. That’s the standard under Executive Order 13873, a brand-new (the regs aren’t yet final) implementation of the well-tested tools under IEEPA. A straightforward application of IEEPA remedies would cut TikTok off from the US market, I argue.

Meanwhile, another little-advertised but equally sweeping rule for government contractors is on its way to implementation. It will deny federal contracts, not just to certain Chinese products but to contractors who themselves use those products.

Not to be outdone by the contracting officers, the Federal Trade Commission and Justice Department are attacking TikTok from a different direction — investigating claims that the company failed to live up to last year’s consent decree on the privacy of children using the app.

And, on top of everything, private sector CISOs are drawing a bead on the app, as Wells Fargo and (briefly) Amazon tell their employees to take the app off their work phones.

It’s no surprise in the face of these developments that TikTok is working overtime to decouple itself in the public’s mind from China, including going so far as to join the rest of Silicon Valley in signaling discomfort with Hong Kong’s new security rules (and ruler). Megan and I question whether this strategy will succeed.

If Chief Justice Roberts were running for office, he couldn’t have produced a better result than the Court’s latest tech decision — upholding most of a law that makes robocalls illegal while striking down the one part of the law that authorizes robocalls — for collection of government debt. David Kris explains.

Nate unpacks a new Florida DBA privacy law prohibiting life, disability and long-term care insurance companies from using genetic tests for coverage purposes. I express skepticism.

Nate also explains the mysteriously quiet launch of the UK-US Bilateral Data Access Agreement. Four years in the making, and neither side wanted to announce that it was in effect — what’s with that, I wonder?

FBI Director Wray gives a compelling speech on the counterintelligence and economic espionage threat from China.

He says the bureau opens a new such case every ten hours. And right on schedule come charges against a professor charged with taking $4M in US grant money to conduct research — for China.

David and I puzzle over the surprisingly lenient sentence handed to a former Yahoo engineer for hacking the personal accounts of more than 6,000 Yahoo Mail users to search to collect sexually explicit images and videos.

I out Reddit as a particularly fanatical convert to SJW orthodoxy in speech suppression, as the service apparently tells its moderators that it’s hate speech to post stories or video showing a person of color as the aggressor in a confrontation.

And Nate closes us out with a bottomless feature on all the problems faced by technological contact tracing.

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

© 2022 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.