Episode 337: Could Kim Jong-un Kill 90% of all Americans Today?

November 9, 2020

Overview

Download the 337th Episode (mp3).
Subscribe to The Cyberlaw Podcast:
This episode’s interview with Dr. Peter Pry of the EMP Commission raises an awkward question: Is it possible that North Korea has already developed nuclear weapons that could cause the deaths of hundreds of millions of Americans by permanently frying the entire electrical infrastructure with a single high-altitude blast? And if he doesn’t, could the sun accomplish pretty much the same thing? The common factor in both scenarios is EMP – electro-magnetic pulse. And we explore the problem in detail, from the capabilities of adversaries to the controversy that has pitted Dr. Pry and the EMP Commission against the power industry and the Energy Department, which are decidedly more confident that the US would withstand a major EMP event. And, for those disinclined to trust those sources, Dr. Pry offers a few tips on how to make it more likely that your systems will survive an EMP.

In the news, that the election turned out not to be hacked and not to be violence-plagued and not to be the subject of serious disinformation. That didn’t stop Twitter and YouTube from overreacting when a leftie hate-object, Steve Bannon, used hyperbole (“heads on pikes”) to express his unhappiness with Dr. Fauci. Really, Twitter’s Trust and Safety operation is so blinkered it can’t be fixed and should be nuked from orbit. Oh, wait, there goes my Twitter account and my YouTube career!

In legal tech news, Michael Weiner explains what’s at stake in the Justice Department’s antitrust lawsuit challenging Visa’s $5.3 billion acquisition of Plaid. I wonder if that means the Department is out of antitrust-litigating ammo. And it might, except you can buy a lot of ammo with $1 billion worth of Silk Road bitcoins, now being claimed by the US. Sultan Meghji says the real question is why it took the US so long to lay claim to the coins.

Just when private companies have come up with plans to comply with California’s privacy law, the voters there change everything. Well, maybe not everything. It looks, Dan Podair suggests, as though compliance with the new CPRA will mostly involve complying with the old CCPA plus a whole bunch more. I’m fascinated by the idea that the initiatives says, “Oh, and by the way, this law can’t be amended except to make it more privacy friendly.”

We bring Michael back to the conversation to brief us on the FTC’s plan to bring antitrust case against Facebook using internal hearing procedure. Michael admits that some might call that a kangaroo court hearing; I suggest that LabMD’s Mike Dougherty be called as an expert witness.

Sultan and I note the ongoing failure of media and rights groups to toxify facial recognition; now it’s being used on “mostly peaceful” protestors who are apparently sweethearts when not punching cops. And it’s hard to argue with using face recognition when it confirms a picture ID left behind in Lafayette Square.

Next, Sultan and I take on Toxification II, the campaign to make people believe that racist artificial Intelligence is a thing. Poorly trained AI is definitely a thing, but that doesn’t make for the same kind of story.

Charles Helleputte analyzes the latest rumor that the EU is planning to prohibit end-to-end crypto. He notes that the EU is also pursuing more infrastructure security and wonders whether the two initiatives can be sustained together.

It turns out that other people on Zoom can, in theory and under the right conditions, guess what you’re typing. It’s one more reason to be careful about webcams and security. I make the sort of cheap joke you’ve come to expect from me.

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