Steptoe

Episode 248: Tomayto, Tomahto: Right to be Forgotten Meets Right to Die

Stewart Baker: [00:00:04] Michael Vatis, my partner in crime and in particular in cybersecurity, your book actually says that he's the man who brought the word "cyber" to government when he was working for Jamie Gorelick at the national security office that she had in the deputy's office at Justice and that he had read, I think, Gibson's book [*Neuromancer*] and started using the phrase. And it took over inside the government and only inside the government so that today when you talk about cyber, you know you're talking to somebody who's come from government because the people who come from Silicon Valley roll their eyes at "cyber" and say, "Oh, God, we stopped talking about that in 1997." We can blame Michael Vatis for this two-culture problem?

John Carlin: [00:00:57] Well, you know I can't reveal sources. He may have been the source for this story that it was Michael Vatis that brought "cyber." Who knows? And one thing was fascinating, just stepping back and doing the book, was realizing the powerful role of movies, fiction, you know whether it's *WarGames* getting President Reagan after seeing the movie for the first time to ask, "Can that happen?" and hearing you know that it could happen and causing the first cyber initiative to William Gibson seeing young kids in the '80s playing video games and thinking, "It looks like they're in a different world, a cyber world," and coining the phrase "cyberspace." I think it's instructive now to look to the movies, to look to science fiction, as we try to think what the next threats are going to be and how we can prepare for them.

Stewart Baker: [00:01:50] [Music] Welcome to Episode 248 of The Cyberlaw Podcast, made possible by but not endorsed by Steptoe & Johnson, as my partners keep reminding me. Thank you for joining us. We're lawyers talking about technology, security, privacy, and government. Today I'm going to be interviewing John Carlin,

former Assistant Attorney General in charge of the National Security Division at Justice and author of a new book, *Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*. And I have made it my ambition to not ask him questions that he's already been asked. So if you've heard him interviewed on a podcast before – and how could you not – check to see how well I did against the questions you've already heard him answer. Okay. And joining me for the News Roundup: Gus Hurwitz from the University of Nebraska; Dr. Megan Reiss from R Street Institute; and Nick Weaver from UC Berkeley. I'm Stewart Baker, formerly with NSA and DHS, the host, the moderator, and the provocateur of today's program. So we oughtta jump in and talk about some real law – and really bad law, too. Illinois has a biometric identity privacy law that the courts have been trying to save from itself, and the Illinois Supreme Court finally said, "No, you can't do that. This law is so bad, it has to be applied as written." At least that's how I read it. Gus, did you take a look at that decision?

Gus Hurwitz: [00:03:18] Yeah, I did. And so the background here is we have this law – a 2008, I believe, law – in Illinois. Biometrics broadly defined can only be collected under certain circumstances. You need to have notice. You need have declaration for how long they'll be kept and what will be used and a bunch of stuff like that. And it also includes really importantly a private right of action which is triggered by violating the terms of the law. So there doesn't need to be a data breach. There doesn't need to be any harm, just you collect someone's fingerprints or their facial scan without telling them or without complying with these various requirements, and you can get sued for a thousand bucks as statutory damages. And over the last couple of years, guess what we've been seeing? A lot of class actions coming up here. A couple other states, Texas for instance, have somewhat similar laws, but none of them are so stupid as to include this private right of action. They require the state attorney general or someone to bring the action, to enforce the law, the violation. And there's been some discussion in recent years about standing requirements, whether or not it's going to be sufficiently tangible damages to survive standing. And the Illinois Supreme Court said in this case brought against Six Flags, a child's biometrics – I forget if it was his fingerprints or face that was scanned –

Stewart Baker: [00:04:47] Fingerprints. Yeah.

Gus Hurwitz: [00:04:49] Yeah. Fingerprints were scanned as just part of the entry process. And his mother brought suit, and the Illinois Supreme Court sustained the suit and the damages on the statutory basis alone.

Stewart Baker: [00:05:05] So if I remember right, I mean there's been a lot of litigation here, and a lot of it was in federal court. And the federal courts do have a standing requirement, right? Because Article 3 requires a case or controversy. But state courts often don't. When the federal courts got this, they said, "Well, you've got to have some injury in order to have standing to have a case or controversy," which is interesting federal doctrine. I'm not even sure it's right in this context, but it's pretty common analysis. And so they solve it. They saved the law from stupid results by invoking standing. And now the Illinois Supreme Court has basically said, "Look, it says you can sue if you're aggrieved. That doesn't to us read like you have to have an injury. You just have to be aggrieved." And God knows in 2019 America being aggrieved ain't that hard.

Gus Hurwitz: [00:06:01] Yeah, and the federalism concerns are really challenging here. There are companies that don't offer services or products. If you're an online company, a platform, you don't enable certain features in the state of Illinois. So we've got companies that are designing and tailoring their products to behave differently in one state versus other states. And unfortunately this could be a blueprint moving forward, as you indicate. Since the *Spokeo* opinion a couple of years ago, there's been a lot of discussion. So *Spokeo*, a US Supreme Court case that really emphasized with a lot of these data and privacy harms, there is a concreteness requirement for harm in order to get into a federal court. So if we're pushing these claims or individuals who are concerned about privacy harms are pushing them to state level statutes, we're going to have 50-some statutes for something that really is a federal issue.

Stewart Baker: [00:07:02] Yeah, or it's just a non-issue. I'm sure that 10 years ago, people might have said, "Oh, my gosh, collecting people's fingerprints? How creepy and

weird!" But now you know we all provide them to our phone company – or at least to Google or Apple – and –

Nick Weaver: [00:07:21] No, you don't to Apple.

Stewart Baker: [00:07:22] Well, okay. So you provide it to your phone. But they are still collecting your biometrics, aren't they?

Nick Weaver: [00:07:29] The phone is collecting the biometrics, but it only stays within the phone. So it's your device is collecting your biometrics. It is not shared, and it is designed not to be shareable.

Stewart Baker: [00:07:42] I'm not sure that's going to protect you from this law. It's interesting. The law also applies to, I think, collecting people's photograph because that's a biometric. It's a dumb overwritten law, which other states mostly haven't followed, and then enforced with this "we will punish you" provision guaranteeing a thousand bucks to anybody who can find a lawyer who's willing to sue, which is not hard because if you add up all those thousand bucks, it turns into real money. To my mind it's an echt example of what's wrong with privacy law. Ten years ago we were worried about this, and now we've gotten a little more used to it. And the idea that we're going to punish, let's say Google to make Nick happier, for collecting fingerprints or for collecting photos to use as part of identifiers strikes me as just nutty. I mean nobody thinks that should be a violation of a law. And now we've got a statute that basically allows anybody who's mad at you to bring this kind of a lawsuit. If you're in the business of collecting even photographs, I think you ought to take another look at this law. And certainly if you're using other kind of biometric identifiers, all this is going to probably mean is a proliferation of notice requirements. But this kid never would have gotten into Six Flags because his parents would have had to agree in writing to his providing his thumbprint to get in. And since they weren't with him, they would have just turned him away at the entry.

Gus Hurwitz: [00:09:22] And I think we can all agree that not getting into Six Flags on demand is a real harm.

Stewart Baker: [00:09:29] [Laughter] You know I've never been to Six Flags. I'm a deprived child.

Megan Reiss: [00:09:33] Me neither.

Stewart Baker: [00:09:34] Yeah. Speaking of deprived children, Vladimir Putin. He's got to be feeling bad 'cause now other people have discovered that doxing folks in power is fun and easy, and they're doing it to him. Megan, tell us about Distributed Denial of Secrets.

Megan Reiss: [00:09:57] DDoS. Of course the name is DDoS. So a competing group was founded contrary to WikiLeaks that is deciding to publish Russian secrets, and they are strategically releasing troves of secrets on Russian oligarchs and members of the Russian elite.

Stewart Baker: [00:10:23] It's not as though they're just targeting the Russians, right?

Megan Reiss: [00:10:25] No, no, no.

Stewart Baker: [00:10:26] They think that WikiLeaks had it right but wasn't crazy enough?

Megan Reiss: [00:10:32] Yes. Well, WikiLeaks never publishes Russian secrets if it could hurt Vladimir Putin in any way. So it's this one weird thing where I'm super torn. I'm like, "This is sweet revenge on the Russians," but because I'm generally opposed to massive troves of documents being released like this, this is not good. But there is that like little bit of me that's like, "Sweet justice."

Stewart Baker: [00:10:57] I think that's right. Now, Nick, I think you got quoted in the story about this.

Megan Reiss: [00:11:00] I noticed that later.

Stewart Baker: [00:11:01] Is Emma Best a friend of yours, one of the co-founders here?

Nick Weaver: [00:11:06] No, I just have interacted with her on Twitter. But one thing that should make you feel better, they are not soliciting nor collecting the data new. What they are doing is taking existing dumps, curating them, and putting them in one place. So they're not responsible for the stuff being out there. They're just responsible for knowing that any cryptographic signatures are valid, adding in formats to make it easier to search, and putting it in one place. So for people like me who might want to look at dumps on whatever, it gives me a one-stop shopping place to find the stuff that's already out there. Because let's say, the Russians do like hacking and doxing each other – we've even turned it into an academic paper.

Stewart Baker: [00:11:56] Yeah. They are second only to the folks in the Persian Gulf who have been – the UAE and Qatar and, for all I know, the Saudis – have been also doxing each other and pulling American PR firms into the mix. So selectively releasing hacked materials is now part of the sort of dark side of PR operations in the United States as far as I can tell. That will not end well. I'm guessing that's going to turn out to be a conspiracy charge. So watch out. Okay. Nick, while the government was shut down, DHS popped up and produced its first emergency order telling government agencies to go check to see whether their DNS [Domain Name System] addresses had been hijacked. How big a deal was that and was it really a threat to the civilian side of US government?

Nick Weaver: [00:13:02] Yes and yes. So what has been happening is everything in our computer security really depends on DNS. That is the name-to-address conversion. And so what attackers would do is compromise the account used to control that, change the

DNS entries to point to the bad guys' systems, and then the bad guy's system can now intercept all Web traffic to the domain, whether or not it's encrypted because they can just get a crypto secret. They can intercept all email to the domain. And so this is a very powerful type of attack, and it's actually hard to catch unless you're specifically looking for it. And probably the best time to have launched this attack against US government computers is, well, when there's this huge shutdown business that is causing half of DHS's staff – and not to mention how many others – to be furloughed.

Stewart Baker: [00:14:00] Right. Because even DHS being on the job – and they did have people on the job – wouldn't have helped because it's somebody in the IT staff of the Interior Department that worries about their DNS, isn't it?

Nick Weaver: [00:14:15] Yes. And also the other thing is there's no real good way for DHS to monitor the health of everybody else's DNS in the government until they actually set up some infrastructure. So responding to this attack in the future can be much more effective if DHS sets up some monitoring things and the like, but until that happens – and that's actual significant work – this attack is quite hard to detect and it is the responsibility of the targeted agencies to detect.

Stewart Baker: [00:14:49] So and it wasn't just aimed at US government sites. It was aimed at pretty much anybody they could hack. What should listeners who are responsible for security be worried about?

Nick Weaver: [00:15:02] Make sure your GoDaddy account is really secure with a unique password. And add in some DNS monitoring where what you do is you look up your own host names on a regular basis off of public DNS servers and make sure nobody is playing games.

Stewart Baker: [00:15:20] Alright. So that's like a script you oughtta run every week. Right? Just double-check and make sure –

Nick Weaver: [00:15:25] Script you oughtta run every minute.

Stewart Baker: [00:15:28] Yeah, I guess that's right.

Nick Weaver: [00:15:29] You're only alert when something changes.

Gus Hurwitz: [00:15:32] Nick, I saw some discussion that with the shutdown, there was a problem with certificates expiring. Apparently this has been an ongoing problem, but there was a large tranche of them that expired during the shutdown because no one was on hand to renew the certificates. Did that exacerbate these DNS concerns at all, or were these standalone issues?

Nick Weaver: [00:15:52] They're standalone, but they're not. The expiring certs are kind of the canary in the coal mine saying, "System abandoned. Easy to hack," because everybody's asleep at the switch. And the other problem is going to be is all the talented people? Boy, it's a great opportunity on LinkedIn for private sector recruiters and/or intelligence recruiters to try to get a whole bunch of assets in the government right now.

Stewart Baker: [00:16:20] Yeah, I think that's right. It was a discouraging time if you were in government. It's one thing to work for a week or two without knowing when you're going to get paid, but that was way longer than most people like to stretch their budget. Right to be forgotten. I feel like the title of this one ought to be "I told you so." Here is a surgeon in Holland who is disciplined for negligence in treating one of her patients. They actually bar her from practice, apparently, for a little bit. She appeals, and they reinstate her, but they continue her on probation. And while that's happening, she goes to Google and says, "I have a right to be forgotten because nobody really needs to know what a crappy surgeon I am as the first thing in the search results." And, God bless them, the Dutch authorities say, "You know actually, we think this is an important thing for people to know," and Google says the same. And some court in the Netherlands says, "Oh, no. That's got to be forgotten. You were listed on a site that talks about doctor blacklist, and people could get the wrong idea from that, that you should be blacklisted. So I'm going to order it withdrawn from Google search terms." And then we're finding out about it now in January of 2019: apparently this decision

came out in July of last year, and they've been arguing all this time over whether the court could publish its opinion. It's a little unclear. But this is such a shocking miscarriage of justice and a demonstration of Baker's Basic Law about privacy, which is that privacy law only protects the privileged in the long run because nobody else cares enough to bring these lawsuits long after the ultimate justification for the policy has disappeared. See *Six Flags*. I don't know, Gus. You can hose me down if you want.

Gus Hurwitz: [00:18:30] No, you just took the wind out of my sail, Stewart. I was going to say this is even worse than just protecting negligence because the underlying information is all still on the Web. It's just not being indexed in this easy to find location. So who is going to figure out "hey, this is a doctor I don't want to go to"? The folks who are more sophisticated, who have some more time to spend doing their research online. So the unsuspecting folks who are less sophisticated or don't have as many resources, they're more likely to get stuck with this incompetent doctor. And who has the ability to go through the litigation and the sophistication to go through and avail themselves of the right to be forgotten? The more sophisticated, resource-rich individuals. So this is all about protecting privilege and making sure that the people who need to have their resources protected have those resources protected.

Stewart Baker: [00:19:26] So I'm on Google's side on that one, but I have to say I am not on their side in this latest YouTube policy. You know there's been a lot of controversy over YouTube, which is sort of the social justice outpost of Google, taking down conservative sites for reasons that are not perfectly clear. They've decided that they're taking too much heat over taking these sites down. Instead, what they're going to start doing is for things that are on the borderline – that is to say that don't violate their guidelines – they're going to just stop recommending them. Their algorithm will say, "Oh, that was a site that might have violated or that somebody reported as possibly violating our terms of service. So even if we decide it doesn't, we can still punish them by making sure that nobody else finds out about their site." That's how I read their policy, and it's pretty close. They say this is for things that don't "quite cross the line – of violating our community guidelines." And we'll start "reducing recommendations," without telling anyone, as far as I can see. There'll be no transparency to this. And if

you've been throttled by YouTube, you probably won't even know it. Now, Nick, I know you're a little more comfortable with this policy, so I'll give you a shot at telling me why I'm wrong.

Nick Weaver: [00:20:51] Okay. The problem is Google's base recommendation is just kind of this machine learning optimization for engagement. And as a result, it actually is optimization for radicalization. No matter what. So if you want running videos, you get to ultra-marathons. If you want Islamic videos, you get to ISIS. You want Hillary Clinton, you get to Pizzagate and QAnon and all that garbage. This is trying to –

Stewart Baker: [00:21:17] Yeah. And if you want Mitt Romney, you apparently end up at Prager University, which is absolutely unthinkable from the people in Silicon Valley!

Nick Weaver: [00:21:25] It's not that. It really is how do you deal with the radicalization effects of the recommendation algorithm? And they're trying to tamp down on it without just going, "You know I'm not even sure if we can do this properly." But it's a real problem, and it still is. So BuzzFeed did a test on blank browsers, and you get all sorts of crazy stuff. You are literally – you'll watch a video on *Star Wars,* and three clicks later, you're at Pizzagate, QAnon about the upcoming arrest of 50,000 Deep Staters who are going to end up in Guantanamo Bay. It's just ludicrous.

Stewart Baker: [00:22:06] So I'm not going to disagree with you that the need to continue engagement, to keep people clicking, to give them stuff that they say, "Whoa, what's that?" and click on it, is a big part of what YouTube wants. They want engagement, and giving somebody something that's just a little further out probably does make sense as an engagement strategy. On the other hand, we're never going to know how this works. Google is basically saying, "Trust us. We'll do the right thing." And I frankly, when it comes to conservative speech, I have zero faith in YouTube's willingness to play it straight.

Nick Weaver: [00:22:43] Except that we have already seen that before. It's a black box machine learning algorithm where even Google doesn't know what's going on, and the results have been catastrophic for everybody but ISIS recruiters.

Stewart Baker: [00:22:58] Well, yeah, it was pretty bad for Prager because they got shut down. Yeah, I hear you. I think this is part of the problem. It makes sense to say, "We don't like the results our algorithm is producing and the social results, and everybody can agree that pushing everybody to the extremes is not such a great idea." On the other hand, the idea of turning over that algorithm to people whose judgment is just so demonstrably distorted by where they live strikes me as equally bad policy. And the question then is: if you don't trust the people who are writing this algorithm, and yet there is only one YouTube, what do you do about it?

Gus Hurwitz: [00:23:45] I'll jump in with the intermediate perspective, which is – I'm, of course, a big "trust the market" kind of guy, and I'd say YouTube currently is not producing good results. There are problems with what they're doing right now, and I think that we absolutely should tell them, "Hey, experiment. Try something different." And we need to give them the space and opportunity to try something different. And if the results are problematic – and the challenge is knowing are the results problematic, but if the results are problematic – then that's when they get punished. I don't think we can say, "Hey, we've got problems right now. We're not going to let you experiment. We're going to come down with a regulatory solution or something else." I think we should embrace the market-based experimental approach.

Stewart Baker: [00:24:30] Hello, Vimeo. Alright. Which is I think sort of the fact that there's so little name recognition for YouTube's principal competitor tells us there's something wrong with the way the market's working here, and I'm not sure what I can say about it. Network effects, first mover advantage, something has made it awfully easy for YouTube to say, "You know we don't really care what you think because you're not going to go anywhere else anyway."

Nick Weaver: [00:24:57] I can say one thing: there is no libertarian solution to a market failure.

Stewart Baker: [00:25:02] Yes. Fair enough. Last topic. I just couldn't resist this because it is a combination of the Chinese use of all of the tools that Silicon Valley and Shenzhen have given them for control with the prospect of yet more Twitter mobbing, but this time in real life. There's an app that's been created in China that tells you if you are near somebody with a really bad social credit score so that you can shame them in person. You know that Twitter is gonna do this next, and those kids from Covington [Catholic High School] will never be able to go anywhere else, with or without their MAGA hats.

Megan Reiss: [00:25:53] When I read this story, I just kept thinking that the creators of it had been watching all the dystopian movies and reading all the dystopian novels but relating to the wrong people in the book.

Stewart Baker: [00:26:06] Yes! It's like the guys who designed that cute little delivery wagon that Amazon says it's going to be using. It's an autonomous vehicle that wanders around your neighborhood to deliver your burritos, and it looks exactly like a *Star Wars* robot. And so yes, it turns out that it's not just cool science fiction that influences designers but dystopian as well. Alright.

Nick Weaver: [00:26:32] Better than the auto security guards that look like Daleks.

Stewart Baker: [00:26:38] Yes! [Laughter].

Megan Reiss: [00:26:38] Yes!

Gus Hurwitz: [00:26:41] Those guys bring me so much joy though.

Stewart Baker: [00:26:45] And I think the Russians like them so much that they put a guy in a suit that looked like one.

Megan Reiss: [00:26:52] I forgot. That was a good one.

Stewart Baker: [00:26:52] So yeah, here's our robot. Okay. Let's go to our interview, which is a little long, so I want to get to it as quickly as I can. Okay. Our interview today is with John Carlin, former Assistant Attorney General for the National Security Division [NSD] at the Justice Department. Old friend and ally. We have worked to similar purpose, John inside the government mostly and me outside the government. And John has written a fine new book, called *Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*, about his time in government and the future. John, it's a pleasure to have you here. I will observe that you've really hit every podcast possible.

John Carlin: [00:27:39] Not yet, Stewart! [Laughter] This was the dream.

Stewart Baker: [00:27:41] [Laughter] This is the hat trick!

John Carlin: [00:27:44] Today's the day!

Stewart Baker: [00:27:46] And so I'm going to try to ask you some questions that – since I've listened to many of the interviews – I'm gonna try to drive you deeper on a few of these topics. It's a great book. People should buy it. People should read it. But even if you don't read it, you should buy it. And what's interesting about it is you were inside while I had just come out and been working cyber at DHS. And so I was deeply invested in the success of the government's efforts against the cyberespionage threat. And so I watched a lot of what you're doing from the outside. And now this is my chance to ask you what was really going on inside. So let me start right there. You spent a lot of time in the book about building the framework for what finally happened at NSD when you were in charge, and part of it, you credit the Bush Administration in its last year or so, is setting up a comprehensive computer security initiative and really proposing a lot of effort and dividing up the world of cybersecurity among NSA and DHS and Justice, FBI. And then the Obama Administration comes in. The president has said it's going to be a

really high priority, but not much happens, at least from the point of view of the Justice Department, until 2014. There's a long lag time there. And I guess my first question is: what's going on? You were career, so you had seen the Justice Department. You were already deep into this stuff. And Justice had a lot to offer, and the FBI had a lot to offer. And yet, it seemed like the administration was pretty slow to figure out what it wanted to do, the Obama Administration.

John Carlin: [00:29:37] Yeah, a couple of things going on. One is a lesson – and the story I tell in the book that occurs again and again with transitions to new administrations, and it seems to particularly occur when it comes to cyber issues, which is there's so much else going on that the work pauses.

Stewart Baker: [00:29:57] Yeah, this is important but not urgent.

John Carlin: [00:29:58] Not urgent. Right. There's some crisis of the day, and they're real. They are real crises, whether it's terrorism or others. I was disappointed to see great people in place, but some of the apparatus that was put in place, I think, to ensure that there was continued attention for a transition from administration to administration now seems to have been taken down in the current administration. When I say that, I mean having someone dedicated within the national security staff who focuses on cyber issues –

Stewart Baker: [00:30:31] This is the job Lisa Monaco had, which no longer exists. Right?

John Carlin: [00:30:34] It is both Lisa Monaco's old job, which no longer exists, and then Rob Joyce's old job in this administration, Michael Daniel before him, that reported to that position, that focused exclusively on cyber. So you got rid of both.

Stewart Baker: [00:30:48] So let me offer a partial defense of this. First, every president gets the White House he deserves because it's all organized around him. And it isn't clear to me that if you have a mission in government, like DHS for cybersecurity

or the FBI for law enforcement, that you're benefited by a lot of attention from the White House staff.

John Carlin: [00:31:15] [Laughter] Spoken as a true member of one of the departments! So I think there's an element of truth to that, but also when it comes to certain areas like improving the defensive readiness of departments – which are not sexy, which are not going to get the attention of cabinet secretaries, which do not get valuable budget dollars or Hill attention because you're not building something new; this is the basic blocking and tackling of cybersecurity, and you're keeping track. In the Obama Administration really occurred towards the end this idea of a sprint towards cybersecurity readiness. I don't think that's occurring right now. There's no one keeping tabs.

Stewart Baker: [00:31:56] There's nobody holding the Cabinet departments' feet to the fire on this issue. Look, I see NSC [National Security Council] and the White House staff as having two principal roles, apart from you know serving the president in whatever capacity the president wants to be served, but they hold the departments' feet to the fire to make them do things that the departments know they should do but don't really want to do, don't want to do on the schedule that's been set. And so NSC nags them and draws up lists of deadlines for them for various things and calls them in to account. So I agree with you. There's not a lot of that happening. And you know we didn't love it when we were in the departments. And the other thing – and the probably more important part of it – is every department, every agency, has stuff that they think is their core job. Right? "This is what I joined government to do. I am going to really excel at this." And then there's stuff that they know they should do, but it isn't their core job and it requires them to coordinate with people in some other agency that they mostly hate. And so they just stay away from that because it's all conflict and no fun, and so things fall between the cracks. And that, I think, you know you need a coordinating agency to make that work.

John Carlin: [00:33:20] I think that's right on both fronts, and I worry currently. And we've seen this story before, which is there isn't you know – the Office of Personnel

Management hack fades in peoples' minds. It was because of that hack that the president tried twice to convene Cabinet meetings, and the attorney general for instance sent me and our chief information officer for the Department of Justice – most Cabinet officers did the same. And it was the third meeting where Lisa Monaco actually, along with the chief of staff to the president, said, "You can bring whoever you want, but as a Cabinet secretary, you have to come and be accountable and understand what is often you may think of as in cyber speak, but it has to be explained to you in a way that you understands so you're setting the risk priority."

Stewart Baker: [00:34:04] So I can fire you if you screw up.

John Carlin: [00:34:07] Yep. That's the hold feet to the fire exercise.

Stewart Baker: [00:34:08] I think that's – but look, this was the Obama Administration, which was notorious for having deputies meetings from 9:00 to 5:00 every day. And so at some point people said, "I'm the deputy secretary. I can't do my job and go to all those damn meetings," and they started sending more and more junior people. I spent a lot of time in meetings in the Bush Administration, but it got a lot worse under Obama. And so you can understand why they would have had to be actually called.

John Carlin: [00:34:39] Yeah. So you know there could be a happy medium somewhere in there, but that solution of having someone drive the un-sexy fix-it, whether it's having centralized servers so you know where your information is or deciding where your data is on the system or making sure that your systems are segmented, it's making sure that that got done. That's exactly where we ended up at the end of the Bush Administration. Right? And similarly, it took a concerted drive from the White House with support of the Director of National Intelligence at the time who made it a real priority to say, "We need concrete items that have to get done, and then we're going to hold you to account whether you've done the task." And to your second point about driving concerted action even when departments don't want to play, one of the things I think we've learned – under this administration there's been enormously

successful work done by the National Security Division by the prosecutors, agents, and intelligence analysts.

Stewart Baker: [00:35:36] And the Treasury Department. And coordinated work with Treasury and Commerce and NSD. It's remarkable.

John Carlin: [00:35:42] Well, actually that's exactly where I was going to say coordinated with Commerce. But when you look at what's occurring with China in particular, there have been these really detailed cases, including catching one of the spymasters when they travel overseas from MSS [Ministry of State Security], prosecuting them, bringing them to the United States for prosecution. An unprecedented success. The creative use of the designation of an "entity" through the Commerce Department, which was part of the strategy that we had put in place before but we hadn't seen executed outside of the world of exports. This is the first time where it really linked to intellectual property. But to your point – and I think this too could be driven better as a strategy, if there was someone pushing it from the White House – where is Treasury when it comes to China? What about the executive order that one Stewart Baker used to call the "April Fools order" because it hadn't been used yet? Well, it still hasn't been used when it comes to Chinese economic espionage.

Stewart Baker: [00:36:39] I'm delighted that actually got enough under the government's skin that you remember it. [Laughter]

John Carlin: [00:36:45] So I think I can tell this now because it comes out in the book. I liked it because it was a push. [Laughter]

Stewart Baker: [00:36:51] [Laughter] I am well aware of that.

John Carlin: [00:36:57] But now it's called for again a little bit to say, "Where's Treasury?" So you have what looks like a concerted strategy. And we have countries as small as Poland taking enormously and unprecedented provocative steps when they catch agents inside their country. There's this beautiful tool of the executive order that

says not only can you sanction the person stealing it but you can go after the recipient of the stolen intellectual property. My clients now in private practice who are victims are saying, "I would come in in a heartbeat if I thought the person who stole it would've paid a real consequence." We haven't seen it used.

Stewart Baker: [00:37:35] Fair enough. Good question. There was an effort to punish the Chinese steel industry for the attacks on, first, the US steel industry and then on the lawyers for the US steel industry, and there was a suggestion that the ITC [International Trade Commission] should actually exclude their products because they were tainted by this unfair practice. And that just sort of disappeared, if I remember right.

John Carlin: [00:38:06] We haven't seen real follow through on that. And that dates back to the first case that we brought in 2014, the People's Liberation Army Unit 61398 case. That, if you recall, targeted not just the steel industry but labor.

Stewart Baker: [00:38:21] Yes, that's right.

John Carlin: [00:38:22] And what they were targeting, the steel workers – the reason they targeted them was because they were encouraging an unfair trade retaliatory suit against China. So I'm not sure there's a good answer. I'd be curious what is. How does the strategy fit in place?

Stewart Baker: [00:38:41] So here's the problem as I see it. The Treasury's always a little anxious about the relationship with China, especially given the amount of US debt that they hold and their sense that they are the keepers of free trade principles for all industries except banks. And so they're always a little conflicted over this, although they've become less conflicted as they've gotten this bigger role in national security. So maybe it's fear of consequences, and that's getting, at least at the secretarial level, a lot of attention.

John Carlin: [00:39:19] I think that sounds plausible and makes sense with where they sit institutionally. I'll say you know one of the stories we tell in the book is about how

getting – the different departments and agencies all for different reasons were cautious about the idea of bringing a case in 2014.

Stewart Baker: [00:39:37] Yes. So I want to hear this a little. At some point – I mean it's tricky for Justice. You're not supposed to get permission to bring prosecutions, if I understand it. And at the same time, it would be crazy for you not to have a united government before you brought the indictment. So you came up with the idea of indicting these guys. Perfectly sensible but novel. And doing something for the first time in government is extraordinarily difficult. My hat is off to you. How did you start that process? Recognizing that the interagency was not going to be your friend, what did you do to prepare the battlefield?

John Carlin: [00:40:23] It's true. People often focus on the policy, but there also were some core just institutional changes that we needed to make and, I think, came from a change somewhat of mindset. You know when I was prosecuting these cases as a line prosecutor, I worked only with the criminal side of the FBI. And there was another squad that did intelligence, and if someone switched squads, they just disappeared.

Stewart Baker: [00:40:47] They just disappeared into the SCIF [sensitive compartmented information facility], and you never saw them again.

John Carlin: [00:40:49] Never saw them again. So when I went over to FBI and realized, "Boy, there's amazing work being done on the intelligence side, and what China in particular is doing when it comes to economic espionage makes the criminal cases that I've been working on pale in comparison. What are we doing about it?" Part of that structural change came, "Well, why aren't we doing anything about it?" And the answer wasn't bad motive. It's that on the intelligence side of the house –

Stewart Baker: [00:41:18] Intelligence guys don't usually bring cases.

John Carlin: [00:41:20] And it's partly they were thinking – and there was a reason for that. Right? It's just the threats have changed. So when it was the Cold War, revealing a

source or method might not be the best strategy for the United States. So instead, like we showed with the Russian illegal case that became the show *The Americans*, you could watch them for 15-20 years as they expend resources here in the United States. You don't disrupt so they don't realize you're watching. And you feed false intelligence.

Stewart Baker: [00:41:44] And it tells you a lot about their tradecraft, and maybe they'll disclose to you somebody else that you could watch. Yeah. But in this case, they were raping and pillaging American companies of their technology in ways that were unrecoverable. Okay.

John Carlin: [00:41:59] So you have to do that shift. And part of that shift then means doing on scale what happened for me, which is making sure that there were prosecutors all across the country and every US Attorney's office who just like they did on terrorism, which was the whole reason the National Security Division was created, are getting access to what's happening on the intelligence side of the house so they can think if they can come up with a creative solution. And in order to do that, you have to train them on how to handle classified information, change the FBI policy to share –

Stewart Baker: [00:42:27] So your first effort was basically to mobilize the institution, and since large chunks of the real heart of the department are out in the US Attorney's offices, you needed those US Attorneys saying, "Hey, I can bring this case," and then coming to Washington to say, "Hey, look at the case that I've got," as opposed to you kind of trying to peddle a case to them.

John Carlin: [00:42:53] Exactly. Unleash the creativity of all these prosecutors across the country. And one thing you appreciate but maybe some listeners don't is it seems like these massive, huge institutions and thousands of people, but some of the key and best changes, they're just a couple of people. So this case, when we started, we had no budget for reorganizing and putting in cyber. It was another period like we are now where the government shutdown was occurring during this period. So you know we stuck guys basically in a supply closet who we flew in from some US Attorney's offices and said, "See if you can access this trove that's been collected and come up with

something new." And then you had to find a US Attorney who was willing to do it, knowing that it had never happened before and was going to take a lot of resources.

Stewart Baker: [00:43:36] And the US Attorney for Pittsburgh basically said, "Yeah, I'll take it on."

John Carlin: [00:43:41] Dave Hickton. He said, "Screw it." And we had talked to a couple other US Attorneys, and for good reasons – resources were tight; they didn't want to do it – and Dave said, "I'm going to give it a shot." And he happened to also be located with some of the best cyber agents in the FBI were out of the Pittsburgh office.

Stewart Baker: [00:43:59] Is that because of Carnegie Mellon and the CERT [Computer Emergency Readiness Team]?

John Carlin: [00:44:01] It's a combination, I think, of Carnegie Mellon, CERT. There's a program out of Pittsburgh, the National Cyber Forensic Training Alliance, or NCFTA, that works with industry that had developed over the years. And all takes is one agent, and there were a couple really good agents who just loved being in Pittsburgh. And we tried to move them, actually. They were so good, we wanted to bring them to headquarters, and they said basically, "It's Pittsburgh, or else I'm out." And so they stayed in Pittsburgh.

Stewart Baker: [00:44:30] Is that still true? You still think that if new cases are going to be pioneered, they're likely to be pioneered out of Pittsburgh?

John Carlin: [00:44:39] I think there's still a cadre of really excellent agents in Pittsburgh. If you look across the book, it's a theme of some of the best cases. They all happen to be out of Pittsburgh. One of the key agents, who I think is phenomenal, just retired – Keith Mularski – and has entered into the private realm, that was behind so many of the great criminal cases – Game Over, Zeus, this epic disruption of a botnet that did everything from taking naked photographs of Miss America – somehow that got more media attention – to using massive ransomware campaigns and theft of funds. So

they took the case, and then you had to convince them that at the end of the day they would be able to bring a case. And then the next step was the intelligence agencies –

Stewart Baker: [00:45:24] Who were probably of mixed views about this. “Yes, we ought to do something because whatever we're doing now isn't working, but not with our intelligence.”

John Carlin: [00:45:36] And even if it's not their –

Stewart Baker: [00:45:39] But for God's sake, the Mandiant report, which basically said, "Hey, look at these guys! And here's pictures of their girlfriends, and here's their blog posts." At that point, it's sort of embarrassing to say, "Oh, yeah, that's all classified."

John Carlin: [00:45:53] We were already well along with the investigation and thinking we'd have a prosecutable case when the Mandiant report hits, and we didn't tell them to hold it. Up to them ultimately, and it's another victim. But I also think of the leadership of – kudos to the leadership of the key agencies at the time: Chris Inglis; Rick Ledgett, who was over at the Director of National Intelligence, who said, "This will make our lives harder. This will improve tradecraft, but we're seeing better than anyone else – we're the ones collecting on it – how much harm," as you put it, "it's doing day in, day out to American companies. And what we're doing now isn't working. So let's give it a shot."

Stewart Baker: [00:46:36] Okay. So now you've got two big chunks lined up more or less for doing this. I'm guessing State Department, traditional National Security Council types think, "We bring a prosecution, God only knows what could happen. But once we've launched, we can't take it back, and we could be diving into a tar pit." So how do you start moving those guys?

John Carlin: [00:47:04] There was a parade of horribles – [Laughter]

Stewart Baker: [00:47:07] [Laughter] I'm sure!

John Carlin: [00:47:07] That were rolled out. So partly it's laying out the facts so that folks get a sense of the amount of damage that's currently being caused. And another change that took time, took good relations of US Attorneys and others in the field talking to the companies that they know so well, was to convince corporate America that you're not going to be in the black forever. And I tell the story of meeting with a general counsel who literally had gamed out, "Okay, for five more years, essentially, we're going to be in the black," –

Stewart Baker: [00:47:43] "And then we're going to be gone."

John Carlin: [00:47:44] "We're going to be gone. And then we'll come complain." And they were frustrated, but they said the interim profits are too great. And so what we started seeing is –

Stewart Baker: [00:47:53] I have always suspected that was Nortel's view, and they took it right off the cliff. They made a lot of money, and then they went belly up because they were totally penetrated.

John Carlin: [00:48:04] And you've seen it, this story, again and again, sector after sector. So it helped that the victims were saying do something and starting to send that demand signal, and that helps move the economic agencies who might otherwise be loath to do something, like Commerce talking to Homeland, who had the responsibility of hearing from –

Stewart Baker: [00:48:28] Who should have been automatically on your side, I would have thought. I mean there's no institutional ox that's gored by bringing the prosecution, and they had to be frustrated by the fact that they weren't gonna be able to protect their way out of the problem. So there had to be other consequences.

John Carlin: [00:48:48] And so then ultimately you also have the arrow in the quiver: it's the Justice Department's prosecution. We find the facts and evidence where they're

going to go, and ultimately it's the Attorney General's decision whether or not to bring the case. So the real question is how are you going to manage the consequences?

Stewart Baker: [00:49:05] "I'm just here to get your advice. I certainly don't want to screw things up unnecessarily, but this case is ours to bring if we choose to." And of course that's a half a bluff, at least, but a nice one to be able to send. You took very early on the position that you were trying to avoid consequences that were unnecessary as opposed to giving State the veto.

John Carlin: [00:49:33] And responsibly. You should do that with a national security case that would cause consequences, like we've done with espionage cases. Arrest someone out of the blue, it might cause harm to American citizens overseas or diplomatic consequences. But it's different than saying may I. It's saying how do you plan for it. Also the Obama Administration at that time, the national security adviser, when we began the case, had really made the theft of intellectual property a priority. It appeared in the president's State of the Union address. He raised it one on one with his counterpart in China to the point where, I think, it became an irritant to the relationship because the president kept raising it with his counterpart. So it was consistent with that strategy, and you could point to that when people talked about –

Stewart Baker: [00:50:24] It was already part of the international dialogue, and this was a pain point that he was happy to raise. Okay. So now at some point you've whittled down the opposition, probably never gotten to the point where people say, "Oh, yeah, okay. We think it's a great idea." At what point do you just say, "Okay. We've heard everything, and we're going to pull the trigger."

John Carlin: [00:50:48] Well, really we did – I think you're right. There were many people towards the end who strongly advocated that that we need to do it and we need to do it. "The time is right. We need to do it now." And I think ultimately we were there. I mean there are some who had their doubts. Doubt about the strategy –

Stewart Baker: [00:51:07] Had enough doubts that if it turned out badly, their memoirs would show that they were right and you were wrong. Okay. It worked out well. For a time it seemed to have a real impact, much bigger impact than many people expected. Whether that's continued? Probably not. So it was, in part, the fact that the president was behind the case, that was as important as the fact of the case.

John Carlin: [00:51:37] I think it was a couple – yeah. I think, absolutely. And then there were a couple other cases that people didn't know about. So one China knew, but the public did not at the time, we were taking a lot of criticism for this is name-and-shame. “You've indicted these five members, but they're never going to see a jail cell.” We actually had arrested a Chinese citizen, Su Bin, who was being held by the Canadians under US process. We were keeping quiet about it to not interfere with the extradition.

Stewart Baker: [00:52:02] He was indirectly tied into this, but it showed that the long arm of US law enforcement was longer than a lot of people thought.

John Carlin: [00:52:09] Yeah. And he was arrested for conspiracy with Chinese intelligence operatives. It just wasn't getting attention, and it was frustrating because a reporter would say, "You'll never arrest someone," and I know we have arrested someone but you can't say it because you don't interfere with the case. So I think that influenced their thinking as well. And then finally, the creation of the new executive order on sanctions and their absolute belief that we were about to use that executive order and sanction some of the recipient companies that caused Xi [Jinping] to come to the table and reach an agreement that changed conduct.

Stewart Baker: [00:52:43] You might impose 25% tariffs on Chinese imports. [Laughter] Okay. So let me ask you a couple of other questions that I was struck by. You talk about how the chief of staff of the Bush Administration, the Bush White House, calls the chief of staff of the Obama campaign in 2008 and says, "You guys are penetrated. You need to know that. You need to take action." And Lisa Monaco, I think, calls their chief foreign affairs person and says the same thing. It's a big deal, and it gets attention from the

campaign. How is it that eight years later the people who got that message managed to have some low-level FBI agent make a couple of calls and get put off by the IT guy at the DNC? What happened to the notion that this is an important thing to tell the campaigns about?

John Carlin: [00:53:47] I was a career official. I didn't know people in either of the campaigns. First time I met someone from the Obama campaign and the McCain campaign was when we went to tell each of them. Back-to-back meetings.

Stewart Baker: [00:54:02] Yeah, yeah! It was a BFD [big freaking deal]. And it was perfectly responsible and something that should have happened. And I don't understand what happened in 2016 when the FBI just let itself be put off and let it go.

John Carlin: [00:54:17] In the first iteration, really our assessment was that they were penetrated, but they were penetrated for more traditional intelligence purposes rather than active measures. No one was going to use the information to cause harm and real concerns. When we learned about it, from the perspective of National Security Division anyway – because we lived so much through the North Korean attack on Sony, we'd seen a nation state use this tradecraft before – that we really needed to get out and do something – make it public and do something in response. It was consistent with what we had at that point already done with China. We had done it with North Korea when it came to Sony, and we had done it with Iran when it came to their distributed denial of service attacks on the financial sector and the Bowman Dam. And we were looking for a Russia case, one to bring. There were some we were working on that ended up being brought later. But here you have this penetration from that perspective. Now I see that there are more complicated counter-arguments, such as, I think there was real concern. What they want to do, in large part, is undermine confidence in democracy. It's democracy that they hate, so if you make it public, do you help in that mission?

Stewart Baker: [00:55:37] Yeah, but you don't even have to make it public. It doesn't look as though anybody in the White House – it's not like they didn't know these people. They knew them all. You would have thought somebody – Lisa Monaco – would have

called the candidate and said to Clinton, "You guys are penetrated, and you need to do something." But it's almost as though nobody thought it was their job, except the FBI, and the FBI thought they could do it in channels.

John Carlin: [00:56:04] Yeah. That's interesting, and some of which I've read about now what happened in the early parts of that case, I don't know that anyone knew early on that –

Stewart Baker: [00:56:14] How bad it was or what it was going to be.

John Carlin: [00:56:15] Yeah. And that they were doing the communication attempts because the FBI wouldn't necessarily tell the White House or the Department of Justice before they go inform a victim. And there were many victims, as you know, throughout Congress, nonprofits, and others.

Stewart Baker: [00:56:33] So this was a big deal in 2008 because it was new and got a lot of attention. By 2016, the FBI has a playbook for telling people you've been penetrated too. And they're saying to the White House, "Yeah, we've got it." And so it just gets handled the way they handle the intrusion into a milk processing plant in the Middle West.

John Carlin: [00:56:57] I wonder about the early stages in terms of notification. Later, when it gets attention, then you have the harder, I think, policy conversations on what to do about it.

Stewart Baker: [00:57:08] Okay. So now I have two personal questions. Michael Vatis, my partner in crime and in particular in cybersecurity, your book actually says that he's the man who brought the word "cyber" to government when he was working for Jamie Gorelick at the national security office that she had in the deputy's office at Justice and that he had read, I think, Gibson's book [*Neuromancer*] and started using the phrase. And it took over inside the government and only inside the government so that today when you talk about cyber, you know you're talking to somebody who's come from

government because the people who come from Silicon Valley roll their eyes at "cyber" and say, "Oh, God, we stopped talking about that in 1997." We can blame Michael Vatis for this two-culture problem?

John Carlin: [00:58:06] Well, you know I can't reveal sources. He may have been the source for this story that it was Michael Vatis that brought "cyber." Who knows? But it's interesting. In the popular imagination, it certainly is "cyber."

Stewart Baker: [00:58:18] No, I think actually that this is one where the Beltway view and the Beltway usage has seeped out into the rest of America, and it's only like Silicon Valley that's sort of deliberately rolls its eyes and says, "You know hackers were originally supposed to be good people who were creative in their use of technology." The same people who say that say you can't call it "cyber."

John Carlin: [00:58:43] We tell some of this story. It's not untrue about the derivation of the word "hacker," but yeah, the popular imagination sure has changed. And one thing was fascinating, just stepping back and doing the book, was realizing the powerful role of movies, fiction, you know whether it's *WarGames* getting President Reagan after seeing the movie for the first time to ask, "Can that happen?" and hearing you know that it could happen and causing the first cyber initiative to William Gibson seeing young kids in the '80s playing video games and thinking, "It looks like they're in a different world, a cyber world," and coining the phrase "cyberspace." I think it's instructive now to look to the movies, to look to science fiction, as we try to think what the next threats are going to be and how we can prepare for them.

Stewart Baker: [00:59:31] The other matter of personal interest: I served on the Robb-Silberman Commission, helped write the report that said, "Everybody's been reorganized for the fight against terrorism, except the Justice Department, which doesn't even have a National Security Division. They've got a piece of the Criminal Division." We said, "There really ought to be a National Security Division," kind of remarkably. And it was a bitter fight. You were in Crim[inal Division], I think, at the time, weren't you? And Crim did not like the idea at all and fought it hard. Only the fact that Judge Silberman is

a master of maneuver on these issues managed to produce the change. But now I think there's almost no one who would say we don't need a National Security Division.

John Carlin: [01:00:18] And great credit in terms of pivoting to hit the cyber threats. And it was one of the core changes we made when I was there was to really focus on counterintelligence and export, not traditional espionage. So cyber threats, export, the use of the tools you have to review foreign investments.

Stewart Baker: [01:00:37] Yeah, you've got CFIUS [Committee on Foreign Investment in the United States]. You're a major hawk on security and CFIUS.

John Carlin: [01:00:43] And I will say – and this is one of the stories I tell – great credit to some of the folks in the Criminal Division, John Lynch, the Computer Crime and Intellectual Property Section. It could have been one of these turf battles that really slowed down the ability to bring the case; instead, they were the ones who taught the national security prosecutors about the Computer Fraud and Abuse Act, about the Electronic Communications Privacy Act. They helped give advice and guidance that in order to bring these cases and share expertise. And similarly, the US Attorney community, whether it was Dave Hickton bringing the case or Jenny Durkan, who was the lead for the subcommittee that was working on computer crime, saying, "This is a good idea, even if it results in more centralization and 'Mother, may I's to Justice." Never, as someone who used to be on the line, the favorite thing for a line prosecutor – and we really couldn't have done it unless those folks believed, too, that this was an important mission and the Justice Department could do more when it came to Russia, North Korea, Iran, China, to nation state threats.

Stewart Baker: [01:01:44] It is a great book. I'm going to ask you now awkward questions about people who came after you. You left at the end of the Obama Administration. The transition to the Trump Administration was characterized by leaks of FISA [Foreign Intelligence Surveillance Act] applications, by ultimately the opening of a counterintelligence investigation naming the president as the subject, by exchanges between the outgoing CIA director and the administration that are poisonous in their

vituperation. And you have not participated in any of the trashing of the new administration. Could we have avoided some of this? Well, let me start. Were you surprised that the president might have been named as a counterintelligence target?

John Carlin: [01:02:46] Without going into too much detail there, I mean it's shocking that the president –

Stewart Baker: [01:02:52] That the question would be asked.

John Carlin: [01:02:52] That the question would need to be asked based on what facts others were seeing.

Stewart Baker: [01:02:59] On the other hand, what do you gain by designating him as a counterintelligence subject? They're not gonna put a FISA tap on his phone, so they didn't need the extra authorities. You kind of wonder why they bothered, except that they were really, really mad that they had just lost their director.

John Carlin: [01:03:14] Well, I'd just be completely guessing from the outside based on public reporting of what happened or not.

Stewart Baker: [01:03:22] Okay. I'm not gonna push you.

John Carlin: [01:03:23] But we'll see. I think it's important in a time where people – Justice Department's been attacked in a way that hasn't been before. The role of an independent Justice Department or FBI. The concept that they don't act at the political direction but they have a degree of independence that's partly cultural and partly legal in terms of how it's protected. I think one of the places where that's really – you've seen that; I'm proud of it – they're doing their mission of protecting us against terrorists and spies is the National Security Division. My successor John Demers. The team that is still in place – that are currently, by the way, working without pay to do this, which also is appalling. And you've been in there. There's just a ton of folks that if you saw what they did day and day, every American would be so proud to call them their own because they

work, they're dedicated on mission, they don't give a darn about politics, and they're out there churning away on really hard problems that require, whether it's tracking down that foreign intelligence operative and getting them to move across country so you can capture them and extradite them, looking at the bits and bytes to figure out what nation states are doing, or hold Russia responsible for something like NotPetya, and that group continues to do their job.

Stewart Baker: [01:04:43] So, John, we could spend all day. I love this stuff. You did a wonderful job running NSD and making it an institution that we can all be proud of. So congratulations. Thanks for the book, *Dawn of the Code War*. It's a terrific read. And it has enough interagency drama that even us inside-the-Beltway fans can enjoy it. So thanks for coming in to talk to us.

John Carlin: [01:05:11] Thank you, Stewart.

Stewart Baker: [01:05:13] Okay. Thanks to John Carlin – also to our Roundup team: Gus Hurwitz, Dr. Megan Reiss, and Nick Weaver – for joining me. This has been Episode 248 of The Cyberlaw Podcast, made possible, but as my partners keep reminding me, definitely not endorsed by Steptoe & Johnson or its clients. Please don't forget: if you suggest an interview guest, we can send you a highly coveted Cyberlaw Podcast mug. Just send those recommendations to CyberlawPodcast@Steptoe.com. Follow me on Twitter, and when I'm really doing everything I should, I will post the stories I'm thinking about covering so that you can comment on them. I didn't do that this week, but about half the time I'll do it. Please rate the show. Leave us a review: iTunes, Google Play, Spotify, Pocket Casts, wherever you go to get your podcasts. It helps to have a review. Show credits: Laurie Paul and Christie Jorge are the producers; Doug Pickett is our audio engineer; Michael Beaver is our intern; I'm Stewart Baker, the host and provocateur. And we hope you'll join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.