Steptoe

# Episode 243: Tech World Turned Upside Down Down Under

**Stewart Baker:** [00:00:03] Welcome to Episode 243 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government. Today I'll be interviewing Representative Jim Langevin of Rhode Island. He's likely to be the chair of a pretty important subcommittee, the House Armed Services Emerging Threats Committee, which does SOCOM and DARPA and Cyber Command oversight. Plus he's got a certain amount of technological affinity himself because he's quadriplegic in a wheelchair that he occasionally turns into a Segway, so we'll cover that in our interview. For the News Roundup I'm really excited to have Denise Howell with us. Denise is the host of the long-running – maybe the longest-running legal podcast – This Week in Law. It's disappointing, Denise, that you're the host of a podcast that has 200 more episodes than The Cyberlaw Podcast and you are still younger and better looking than I am.

**Denise Howell:** [00:01:17] That's just not possible, Stewart.

**Stewart Baker:** [00:01:18] [Laughter]

**Denise Howell:** [00:01:19] I'm not willing to accept that at all. Thank you so much for having me on. I'm thrilled to be here.

**Stewart Baker:** [00:01:24] No, it's great. I love your program. I listen to it regularly. It's more of a stroll. If we are rushing through these stories, you stroll through them and take your time with them and produce a lot of useful insights that we barely have time to touch on. And so I'm really looking forward. Well, maybe we'll do a little more strolling in this episode than we usually do. So thanks for coming.

**Denise Howell:** [00:01:52] It's my usual gait, but listeners tell me they speed it up so they can get through it all in time.

**Stewart Baker:** [00:01:57] You know I do that on all podcasts. I think you actually listen better if you run it up to at least 1.25x, and I've done it as fast as 1.5x. You can absorb it all. And it drives my wife crazy when she gets in the car and I'm listening to it at that speed because she thinks that everybody sounds like chipmunks. I think it's just like you know more efficient and just as likely to give you the information you need.

**Denise Howell:** [00:02:27] We may just have to embrace it and do an Alvin and The Chipmunks Christmas thing here on your show today.

**Stewart Baker:** [00:02:33] It's a deal.

**Gus Hurwitz:** [00:02:36] I'm just hoping that my students aren't listening because I'm imagining my student evals now saying, "Please talk faster. You can do your hour-long class in 35 minutes."

**Stewart Baker:** [00:02:46] That was Gus Hurwitz, Associate Professor of Law at the University of Nebraska. And he introduced us to the fact that today is the 25th anniversary of the introduction of *Doom*, which is responsible for at least half of the people on this podcast getting into tech.

**Gus Hurwitz:** [00:03:04] I promise not to sing happy birthday, but I might challenge everyone to a deathmatch.

**Stewart Baker:** [00:03:07] If you do, you're gonna have to sing it as Alvin. Okay. Also joining us, Nate Jones, formerly with the Justice Department, National Security Council counterterrorism office, now with Culper Partners. Nate, welcome.

**Nate Jones:** [00:03:21] Thank you for having me, Stewart.

**Stewart Baker:** [00:03:22] And last, but surely not least, the irrepressible Nick Weaver from UC Berkeley, the man who holds our feet to the tech fire when we start waxing legal and depart from the reality of tech. So, Nick, it's great to have you as well.

**Nick Weaver:** [00:03:44] Thank you.

**Stewart Baker:** [00:03:45] Okay. So speaking of waxing legal and holding our feet to the fire, I think we ought to take a quick trip Down Under. And once again, Denise, I have to say you have bumpers. You have little musical interludes that tell people what they're going to. I've never figured out how to do bumpers for our show. So I'm just gonna say imagine we're going Down Under to talk about the Australian Parliament's controversial encryption bill. Nick, do you want to kick this off?

**Nick Weaver:** [00:04:17] Yes. The devil's in the details. So the real question is going to be what is the meaning of “significant structural weakness” or whatever that language is. So let's use concrete examples. iMessage can accommodate the Australian request in a nanosecond. I've written about it. You just basically create a hidden extra account. The problem is you have systems like Signal which can't without introducing significant structural weaknesses, the sort of weaknesses where you get a secret in the hands of the Chinese and the Chinese are able to wiretap everything. And that's a real problem. So we don't know the devils in the details. And that has this huge impact.

**Stewart Baker:** [00:05:09] So the language, the bill says that the Australian Government can come to tech providers, pretty much all of them, and serve them an order saying, "We want you to find a way to give us access to the communications of your system." They cannot ask for the introduction of a systemic weakness, and that is defined as a "weakness that affects a class of technology. It does not include a weakness that is selectively introduced to one or more target technologies connected to a particular person." So you can see what they're getting at. They're saying, "Don't create a hole for everybody. We want a whole for Nick Weaver."

**Nick Weaver:** [00:05:52] The problem is in doing that, there's no effective way to do that without introducing holes for everybody in most cases. So iMessage, the reason why iMessage can qualify is it has a hole, that it does support the addition of silent accounts because there's no key transparency, but there is no such way to introduce, say, a vulnerability into Signal without doing that. So Signal, it's the same code for everybody, so you can't do a customized install for Bob because Signal's actually not in charge of distributing the code, and Signal, you can't introduce a custom intercept for Bob because Bob would see it with the key transparency. So the question is will those arguments fly or not in the Australian court.

**Stewart Baker:** [00:06:52] So there's actually, this isn't a court, or at least not at first instance. It's basically an argument you make back to the government when they ask you to do something. They do have the ability to ask for voluntary measures that would make it possible to selectively create a hole for a particular –

**Nick Weaver:** [00:07:15] [Laughter] Unless you're Skype being bought out by Microsoft for the benefit of [FISA Section] 702 collection, that's not going to happen.

**Stewart Baker:** [00:07:23] So let me ask Denise, you're out there in Silicon Valley. Do you share Nick's view that the companies there are just going to say, "We're not interested in changing our technology to help the Australians?"

**Denise Howell:** [00:07:38] Oh, absolutely, and I'm not even sure that Australian companies who are subject to this law are capable of altering their technology in the way that this law wants them to. I guess, as you say, the devil is in the details, and we're going to see what happens. It seems like the bill itself is an exercise in public relations and opinion control. I mean they're trying to build in some safeguards that are trying to address – or at least you know begin to be a response to – what Nick has raised here, for example. And again I think it's going to be interesting to see how this plays out and how it winds up working because there are two kinds of requests that can be made. There's this technical assistance request and also a technical capability request, and it

seems like the technical capability one is the more – it has the most teeth, has the most ability to –

**Stewart Baker:** [00:08:36] To require actual changes in the way the technologies work, and yeah, I think you're right.

**Denise Howell:** [00:08:39] Exactly. And in that case, there's some sort of an appeal process where you can dispute a technical capability notice where there's going to be a judge and "a person with technical expertise" to judge whether the proposed backdoor is reasonable and proportionate or is one of these impermissible systemic weaknesses that the bill says it won't require companies to do. So in some sense it's going to be taken on a case by case basis. And this language seems to be addressing the arguments of people who would say, "Well, you simply can't do this. You're going to compromise everyone's system." "No, no, no, no. We just want to compromise on particular access to particular people." It seems like if this is how we're going to make sure we do it, I'm with Nick. I'm not sure that you'll ever – if these appeals are to actually have substance and validity, I'm not sure you'd get through that process.

**Stewart Baker:** [00:09:45] I'm less sure that the tech guys can navigate that. The standard ultimately, if I'm reading this right, is you have to demonstrate a material risk that the introduction of this hole will allow otherwise secure information held by someone other than the party you're targeting to be accessed. So they say it's a systemic weakness if you add something that will or is likely to jeopardize the security of information held by another person. And that means a material risk that the information will be accessed by an unauthorized third party. So you have to have a pretty good reason to believe some third party will have access to this. Let me ask a very concrete question to Nick: The Ray Ozzie solution? The Ozzie solution is basically to say we're already updating the phone and the computer.

**Nick Weaver:** [00:10:45] No. [Laughter]

**Stewart Baker:** [00:10:46] No? But why is that not sufficient if you can target your updates?

**Nick Weaver:** [00:10:53] That is actually not Ray Ozzie's solution. What Ray Ozzie and Stefan Savage are about is the "Going Dark" device problem, not the "Going Dark" communication problem. And the "Going Dark" device problem is actually a lot easier to solve because the first thing you can do is make it so that you have to get the device in hand, which eliminates so much of the systemic risk.

**Stewart Baker:** [00:11:21] Right.

**Nick Weaver:** [00:11:21] But if you are doing for communication, which is what the Australian bill seems targeted as much as anything, you always run the risk of basically having some sort of magic number infrastructure that if the Chinese get a hold of, they can compromise. And we've seen this happen on multiple occasions. So Google's lawful intercept mechanism was compromised by the Chinese. The lawful intercept mechanism –

**Stewart Baker:** [00:11:50] Can I stop you there? I don't think that's true. There are reports that Google's intercept list was browsed – or at least the Chinese who broke into Google in 2009 tried to get access to that list, and somebody trying to get access who wasn't really authorized was caught in their logs. But that's not the same as their mechanism being compromised or maybe even the access compromised.

**Nick Weaver:** [00:12:23] But we don't know. That's part of the issue. And we do know that the lawful access mechanism in the Greek cell phone system was compromised by parties unknown.

**Stewart Baker:** [00:12:34] That's true.

**Nick Weaver:** [00:12:35] And so whenever you build these mechanisms, they're such attractive targets too. A bit of bribery. Hell, how much could you get with a million dollars to spread around?

**Stewart Baker:** [00:12:47] Come on, now. Nick, everybody has a mechanism for updating their software, their devices, and every one of those update mechanisms could be compromised and would be a disaster for the user. And yet we keep adding those capabilities in because we believe that on balance the security gains from that are worth the security risks.

**Nick Weaver:** [00:13:14] And if we want to compromise the update mechanism, you are attacking the computer equivalent of vaccines, and yes, we have seen the update mechanisms compromised too. That was the whole thing behind NotPetya.

**Stewart Baker:** [00:13:27] So I think you've put your finger on something though, which is device access, where there's a pretty plausible argument that when all is said and done, if you have the device in hand and you say to Apple, "Get me in using the update," that Apple is going to have to argue, "But there's a material risk that otherwise secret information held by a third party will be compromised by our doing that." I think that's a hard row to hoe for them. Isn't it?

**Nick Weaver:** [00:13:57] Except that for Apple they've designed the phone so that in order to update the phone you have to unlock the phone first.

**Stewart Baker:** [00:14:06] I think that's the interesting question. I'll ask Denise, do you think that Silicon Valley is going to double down and say, "Not only are we not going to make it easier, we're going to do everything we can to make it impossible to comply with the Australian law," and then say, "Yeah, nanny nanny, boo boo, sucks to be you," when the Aussies come to us?

**Denise Howell:** [00:14:25] I think so, and I hope so. I do think to the extent they can do it, I think companies like Apple will say, "Well, we're not subject to this law, and we think

it's a bad idea. We think it's a bad idea for a number of reasons." We've been talking about this in terms of a law that applies in Australia, but we can't really think about this law without thinking more globally than that. I mean you've already brought in how are US and other companies' devices going to be able to operate in Australia under this law. Will Australian companies be able to export their technology to other countries, say GDPR-governed countries, that this may come head to head with and conflict with? I think that GDPR actually comes in in a couple of ways. One, we could get into whether or not a device that complies with this law complies with the GDPR, but the other sort of more insidious way I think the GDPR provides an example of what may happen with technology companies is sort of the opposite of what you're saying, Stewart. Some may dig in and say, "Nanny nanny, boo boo," [laughter] as you so eloquently put it. Others, particularly ones operating in Australia, may say, "Oh, well, as many companies have done – we've seen the dominoes fall with the GDPR as far as 'Oh, we've got to comply, and we've got to comply now,' and we don't want to have to hash through whether our compliance is sufficient or not. We're just going to be very, very proactive about it and do what the government wants before they even come to us with one of these notices. We'll just make sure we have these capabilities in place." And I'm concerned that we may see that kind of approach happen from companies in Australia who just don't want to have to get into a dispute about whether they're doing what they're supposed to be doing.

**Stewart Baker:** [00:16:21] Nick, I cut you off. Last thoughts on this topic?

**Nick Weaver:** [00:16:25] It's going to be an amusing cluster.

**Stewart Baker:** [00:16:29] [Laughter] Yes. That's for sure. And look, we know quite well that the Aussies were encouraged by the other English-speaking countries, the Five Eyes countries, to go down this road in a variety of multilateral meetings with principles adopted that are pretty consistent with what the Aussies are doing here, which means that my guess is that New Zealand and the UK and maybe Canada are all watching this, thinking, "Well, if the roof doesn't fall in, maybe in a year we'll try the same thing." Alright. The Marriott hack, not only is it like the second biggest in terms of records

compromised, individuals compromised, it's developing an interesting reputation as not just a commercial hack. Gus, can you bring us up to date?

**Gus Hurwitz:** [00:17:21] Yeah. So this is one of those stories that just keeps on getting more and more interesting but also one of those stories that we seem to know less and less about. So there's a Reuters report out a couple of days ago that relies on three unnamed sources investigating the Marriott hack that suggest the Chinese government was somehow implicated or involved in the attack. We know very little about the details other than those assertions. There are some tools apparently that are attributable to Chinese government actors that have been found on Marriott systems, but it's really hard to know what to make from that.

**Stewart Baker:** [00:18:04] It's kind of a soft attribution. Nobody is saying, "We got 'em dead to rights." They're saying, "That's what it looks like to us, but we're still working on it." It's almost as though they're waiting for the US government to say, "Yep, it was the Chinese."

**Gus Hurwitz:** [00:18:19] Yeah, but I think the bigger story here is it appears that almost everyone has compromised Marriott systems.

**Stewart Baker:** [00:18:26] [Laughter]

**Gus Hurwitz:** [00:18:27] So there are reports going back several years of commercial compromises of their systems, of the Russians in their systems. Now we have reports of the Chinese in their systems. One of the major compromises appears to be the result of one of their cybersecurity contractors actually opening a malicious payload, thinking that they were investigating that, and that's what compromised their systems. So it seems that everyone has over the last few years gotten into Marriott, which leads me to the question: What the heck is going on with the hotel chains and their cybersecurity? The only surprising thing perhaps is that LabMD wasn't a hotel chain. If you think Wyndham, LabMD, and Marriott as three of these big cybersecurity cases, what's going on with hotels and their security? And I think there's actually a really important question here.

Hotels are very large, very customer-oriented, franchise-based operations, and I think that they have very difficult security requirements that they're trying to balance. I tend to be on the side of let's not default to blaming the actors and saying, "Oh, you guys were just really bad, incompetent actors," without understanding was there some actual business decision or calculus here. And I wonder whether or not there is a particular difficulty in securing large, franchise-based, consumer-focused operations that poses some unique security challenges that we should be studying and thinking about, at least in the legal context, if not the technical context.

**Stewart Baker:** [00:20:10] A lot of people, when you check in, you expect your history to be available to the people who are checking you in. But they're really a different company owned by different individuals than the last Starwood Resort you stayed in. I think the other issue here that emerged was Starwood had done its own roll up of other hotel chains, and every time you acquire another company with its own IT system, you're basically infecting yourself with anything that has gone wrong with their system in the last five years.

**Gus Hurwitz:** [00:20:46] Yeah. And this is both on the customer service and the business valuation and also frankly on the antitrust side a really important calculation and aspect of these businesses and how we think about liability that's not really well appreciated and understood. So looking at an industry that I know particularly well, if you look at the cable industry, one of the reasons that the cable industry has such a terrible track record on customer support is because when you think about any of the large cable networks today, they're actually an agglomeration of several hundred or several thousand independent MSOs [multiple system operators] – cable operations – each of which over the last five, 10, 15 years has been folded into an existing system. And it's really hard to integrate all those different systems in a way that at the back office level, at the technical level, works seamlessly, and that's led to a lot of difficulties operationally. And when you're looking at all of the mergers that we've seen with what has become Starwood and then Marriott, that's a really hard thing to do right. And it leads to both inheriting challenging liability – that's the story of Verizon and Yahoo – and

also inheriting and trying to integrate complex technical systems in ways that can create vulnerabilities.

**Stewart Baker:** [00:22:12] Well, and one last observation here: If you're wondering how it was there was all this passport information in their files, I think you can thank the Europeans because when you check into hotels in large parts of continental Europe, there is a requirement that they get your passport, copy the number, something of the sort, and record that so the police can come by and look at the passports of everybody who's checked into the hotel. So, Denise, if you thought the GDPR was going to prevent the creation of security holes on behalf of law enforcement, I think the experience with passport collection suggests the GDPR is pretty friendly to governments that want to get access. It's just companies that it screws over.

**Denise Howell:** [00:22:59] Yeah. That's a good point, Stewart.

**Stewart Baker:** [00:23:02] Okay. So we've beaten up the Europeans. We've beaten up the Chinese. We've beaten up the Aussies. How about the Saudis, the Italians, and the Israelis? Nate, how do all those folks end up in one scandal?

**Nate Jones:** [00:23:17] [Laughter] You know I think most of your listeners are probably familiar with the background of this case, but for those who are not: Jamal Khashoggi was a US permanent resident and *Washington Post* columnist. On October 2, [2018,] he walked into the Saudi consulate in Turkey, where he was met by a 17-man team of Saudis who were sent in from Riyadh and promptly murdered, dismembered, and disposed of [Khashoggi]. Since that time, the world has been fixated on a couple of questions. The first was whether the Saudi government and the Crown Prince Mohammad Bin Salman, or MBS, played a role in the assassination. Recently, a CIA assessment affirmed what many suspected from the outset. It assessed with high confidence that the Crown Prince MBS in fact ordered the assassination of Mr. Khashoggi. And that seems to have resolved that first question in the minds of most people, with the exception of President Trump and Jared Kushner. And a quick tangent on that: This story again keeps raising or keeps alive the broader concerns about Mr.

Kushner's coziness with his Telegram or Signal pen pal, MBS. But the reason this is relevant to your question, Stewart, is the question that's left open is the question of why, and that's still subject to a lot of speculation. And one narrative that's been emerging for some time and was, I think articulated pretty well by David Ignatius in *The Washington Post* last week, has two parts. The first is that the Saudi government and MBS in particular have been very proactive at trying to shape their public image. A lot of this of course stems from the fear that flowed from the Arab Spring, and autocrats around the world began to worry that that threatened their hold on power in their countries. And it's further complicated by MBS's controversial way in which he ascended to his position as crown prince and his worries about that slipping away. But where this intersects with those countries and with technology is the way in which the Saudi government has invested in developing technological capabilities to, first off, identify and silence dissenters, those who are fomenting narratives on social media and other platforms that they dislike and don't agree with. And the second is to figure out how to use their platforms, including on social media, to advance their own preferred narrative about the government and regional politics and the like. And with respect to the former, MBS has apparently focused part of his effort on developing a powerful set of surveillance tools by partnering with technology companies in Italy, in the United Arab Emirates, and in Israel, of all places. And the Israeli one in particular would require a government license to export it to Saudi Arabia, which has among other things, prompted some litigation there by a close friend and ally of Jamal Khashoggi. And –

**Stewart Baker:** [00:26:21] He's suing the company that developed the hacking capabilities in Tel Aviv –

**Nate Jones:** [00:26:29] Right.

**Stewart Baker:** [00:26:30] Because he says they – so this is a Saudi dissident going to Tel Aviv to vindicate his human rights. This is a different world than the one we grew up in.

**Nate Jones:** [00:26:40] Very different. And yeah, he claims that his communications were compromised by this and that it played some role in the murder and assassination of Mr. Khashoggi. We haven't, as far as I've seen, seen any direct evidence that it played a role, although his recent criticism of MBS in particular and the Saudi government do fit in this narrative of him being an inconvenient nuisance for the government and that having potentially played a role in his assassination. And you know I think the one interesting thing about this story is it raises the prospects of some potentially low-tech methods that are being deployed. And Nick I think referred to this at the outset when we're talking about the Australian legislation and that is there were some reports in October that the Saudis were grooming a Twitter employee to help with getting access to user profiles. So they're taking out all the stops, it seems here, and trying to use the tools at their disposal to crack down on dissent and, as I said, to push their own narrative. And to me, this raises a few interesting things. First is: Even if it didn't play a role in the assassination of Mr. Khashoggi, the Saudi government faces real threats and has been a critical source for US intelligence on its counterterrorism efforts, and so there are valid reasons why governments, including the Saudis, need these kinds of capabilities. But – and this is a big but – it highlights how these tools, even if they can be used for good, can result in significant harm or abuse when they're not governed by a system of rule of law to protect against those kinds of things. And then thirdly, I think it highlights once again the challenges that the tech industry is facing, this time largely companies outside of the US. But the questions that they're facing about their responsibility to prevent abuses and misuses of their products and answer questions about how they're going to partner with governments around the world and under what conditions. And so I think that's a struggle that's going to continue for the tech industry more broadly and including companies outside of the US.

**Nick Weaver:** [00:29:01] Although these companies in particular are a very interesting case. So the Israeli company is the NSO Group. Their malcode has been used to hack dissidents in UAE, Saudi dissidents in Canada, really evil stuff. And they're really in the Wernher von Braun school of rocketry. They don't care that the stuff is being used to target dissidents as much as it is to target terrorists. The other thing that I think is missed is that CIA leak blew a huge amount of US SIGINT [signals intelligence]

collection on the Saudis, that the details on the leak told the world that the US has metadata but not content on the communication between MBS and his aides. That says a huge amount, and we probably lost that capability by now already.

**Stewart Baker:** [00:30:11] I think you're right. My reaction to Nate's kind of sideswipe of the president is aligned with that. There was so much enthusiasm for showing that the president was not telling the truth when he wasn't sure MBS did it that somebody inside the agency and lots of people outside it or maybe at the intelligence committees leaked a whole bunch of stuff that was designed to embarrass the president for about 48 hours and will cost us capabilities for years.

**Nate Jones:** [00:30:46] Yeah, and I would definitely agree with that. On Nick's first point, you know I think it's a valid point about these companies having a different outlook on the world. But I do think that getting caught up in these kinds of high-profile cases and having a light shone on their practices can result in some pressure on them. But I think that it will be interesting to see how that plays out and how much longer they can get away with those kinds of things.

**Nick Weaver:** [00:31:13] They've gotten away with it for years. So we caught the NSO Group like two years ago, and they're still selling to Middle Eastern repressive dictators for use of targeting dissidents.

**Stewart Baker:** [00:31:25] So I'm going to ask you on the next show, Nick, to give me a list of more than five countries that you think it would be safe for them to sell this stuff to – Denmark does not count – because I guarantee you there are people who would say that selling it to the United States government is selling it to a repressive regime. There's nobody who can't be portrayed and may not be capable of doing things in their national interests that the rest of the world isn't very comfortable with.

**Nick Weaver:** [00:31:53] Except that the key is do they get caught. So like Bill and the Citizen Lab folks, they don't actually care about the crooks. And so when the stuff is used against crooks, it actually doesn't show up on the radar of groups like Citizen Lab.

There's plenty you can sell to, and in fact one of the problems that you face in law enforcement in using the same tools that are used by these Middle Eastern idiots is your stuff gets compromised when they screw up.

**Denise Howell:** [00:32:27] In this world that we're living in, where we're seeing this kind of example of how governments can do things to other governments, I'm wondering what you all think of how the state of play shifts if this law that we were previously discussing in Australia doesn't rock a lot of boats, as you said Stewart, and other countries follow suit thinking it's a good idea and we wind up with a private sector of communication technologies that we know have either are compromised or are compromisable. Since most governments look to the private sector at least for some of their technology, doesn't that just aggravate the situation?

**Stewart Baker:** [00:33:11] Yeah. I think it means less and less can we just say there is one technology for the world, and more and more it's a question of which technology in which country you're going to use. I remember one time before – well, I'll leave that story because it's probably still classified.

**Denise Howell:** [00:33:33] [Laughter]

**Stewart Baker:** [00:33:33] Let's finish off with two quick stories. EMP [electromagnetic pulse]: There's a report out saying that EMP would be a disaster, like all of our nuclear power plants would melt down, just the way the Japanese plant did, after about two days without power. And Nick, you've been kind of an EMP skeptic not because it wouldn't work but because it might work too well and lead to worse consequences.

**Nick Weaver:** [00:34:09] Yeah. Basically, to generate a significant EMP takes a nuclear weapon. You drop a nuclear weapon in the ionosphere over the US to cause an EMP, we're going to give you 50 megatons by return post. However, the EMP FUDsters [fear, uncertainty, doubt] are good for something in that the same damage can be caused by the sun. If you ever feel like you want something to worry about, look up the Wikipedia page for the Carrington Event. If the sun did that today, we'd be looking at somewhere

between $600 billion and $3 trillion worth of damage to the US economy. And anything that defends against EMP defends against solar storms.

**Stewart Baker:** [00:34:54] So we should be doing it even though – is it really true that only a nuclear weapon can generate an electromagnetic pulse? I thought you could come up with something much smaller that would produce a more geographically limited pulse.

**Gus Hurwitz:** [00:35:09] You've been watching too much *Ocean's Eleven*, Stewart.

**Stewart Baker:** [00:35:14] [Laughter]

**Nick Weaver:** [00:35:14] There are designs for flux compression generators which turn explosive into an electrical pulse. That would only be good for a very small area, and if you want to cause a blackout and can get 500 pounds of explosives to the target, just blow up the frackin' substation. It's easier.

**Stewart Baker:** [00:35:33] Okay. Last, Huawei's CFO – and the daughter of the founder of Huawei – was detained in Canada, is now fighting extradition to the United States on charges for export control violations. Quick poll of the panel: Does this mean that the 90-day tariff truce is probably the only relief we're going to get? Is this going to really so poison the relationship that the trade negotiations can't succeed? Gus, you got a view on that?

**Gus Hurwitz:** [00:36:10] I'm crying myself to sleep every night.

**Stewart Baker:** [00:36:11] [Laughter] How about you, Nate?

**Nate Jones:** [00:36:14] I think it's going to be a significant hiccup that you know I think they'll have to find a way to work around, and ultimately they will because resolving this trade dispute will over the long term prove too important.

**Stewart Baker:** [00:36:26] Denise?

**Denise Howell:** [00:36:27] Yeah, I agree with that, that both companies are too practical to wind up not doing business with each other for very long or having it too painful to do business with each other very long, but I keep thinking that everything comes back to backdoored phones here.

**Stewart Baker:** [00:36:45] [Laughter] Yes, in some ways it does. Nick, last word on that?

**Nick Weaver:** [00:36:48] A great and glorious Charlie Foxtrot, and I think going to be a trend to accelerate the balkanization of the technology industry, and also if I was a C-level executive of a major US tech company, I'd probably cancel that Chinese vacation.

**Gus Hurwitz:** [00:37:08] I'll jump in and add that I agree 100% that this accelerates the trend towards balkanization, and that's one of the reasons that I cry myself to sleep every night.

**Stewart Baker:** [00:37:18] Alright. And Hainan Island tourism futures take a dive. Alright. Thanks to our panel. Our interview this week is with Representative Jim Langevin of Rhode Island. Let's turn to that. Alright. We are here with Congressman Langevin, who is a Rhode Island Democrat. 20 years?

**Rep. Jim Langevin:** [00:37:38] Well, 18 years in the Congress, going into my tenth term right now. Reelection. Excited for the future.

**Stewart Baker:** [00:37:47] Yes, Rhode Island has not traditionally had really long seniority representation, has it?

**Rep. Jim Langevin:** [00:37:57] Let's see. Going back several years – well, several decades ago – Fernand St Germain was one of the longest serving members of the

House anyway. But generally maybe 10 years or so has been about the average, so I guess I'm pushing the envelope there.

**Stewart Baker:** [00:38:22] Well, I'm guessing you spend 10 years there, you are basically campaigning almost statewide. There must be a temptation on the part of some to run for statewide office, run for the Senate, things of that sort.

**Rep. Jim Langevin:** [00:38:34] Yeah, I guess so. And certainly I have thought of in terms of other offices at some point, but I have enjoyed what I'm doing and for me it's been about public service and trying to make a difference for the people of my state. I actually entered public service very early on in my career as a way to get back and say thank you to the people of Rhode Island who rallied around me and my family after I had my accident that left me paralyzed, and I didn't know at the time it was going to be a lifelong career and endeavor. But I enjoyed the opportunity to serve and enjoy doing what I'm doing. Ambition has not been a hallmark of my time in politics and governance. It's been about trying to make a difference and give back.

**Stewart Baker:** [00:39:23] So you've made a big difference in cybersecurity where you've both been on the Homeland Security Committee, pressing the Homeland Security Department about cybersecurity issues, and you've also been the ranking member of the House Armed Services Subcommittee on Emerging Threats, which has a lot of cybersecurity and Cyber Command responsibilities. Let me start, rather than talking about those particular assignments, this is a moment where the Democrats are thinking what is our agenda going to be as we take over the house in the next Congress. What do you think it is or should be for cybersecurity?

**Rep. Jim Langevin:** [00:40:08] Well, I think it's going to be a front-and-center issue. I'm going to continue to be very involved with cybersecurity, trying to move the ball forward to further protect the country in cyberspace. I've often said it's both the national and economic security challenge of the 21st century and we need more focused support and resources in this area. We're getting better organized with each passing day, month, and year. We're getting better and stronger at protecting the country. But we still don't

have it right yet, and we need to continue to build our own capabilities but also collaborate and partner more with the private sector. So wherever public-private partnerships are possible we should do that, as well as I believe partnering with the international community. This isn't just a US challenge. It's an international one. And so establishing international norms and rules of the road are helpful. I think right now it's sort of the Wild West in the international space, if you will, and we need to bring more stability to cyber and establish norms wherever possible.

**Stewart Baker:** [00:41:23] So I agree with you on that we should establish norms, but I think the idea of going to the UN and writing them down is probably not the way to do it. We have to demonstrate that we're prepared to enforce them. If you violate what we think is a norm, you'll pay a price. And that does raise the question: Do we have the ability to extract a price for people who break the rules, who attack our grid or even just plant malware there that they can execute at a later date? What should we be doing when people take provocative steps like that?

**Rep. Jim Langevin:** [00:42:03] Well, I believe that we should use all assets of state power to respond when necessary to make it clear to enemies or adversaries that we have a number of tools at our disposal to protect the country and that we shouldn't be afraid to use them. But I also do believe that – again, this is an international challenge – I think norms of responsible state behavior in cyberspace should be expected, and I strongly support the US participation in UN Group of Government Experts process and other multi-lateral fora that provide opportunity to further refine these norms. I also support the US taking a leadership role in the G-20 by pushing for a declaratory statement calling on nations to protect the financial system from cyber threats, by way of example. I think that's a great place to start. We got to find some common ground in establishing rules of the road. We're not going to attack each other's financial systems. And I think that can hopefully be a marker and a placeholder and a foundation for building on other norms.

**Stewart Baker:** [00:43:23] I think that's right.

**Rep. Jim Langevin:** [00:43:23] In terms of response, it shouldn't just be a cyber-for-cyber. We should use all assets of state power to respond, to punish adversaries if they try to cause us harm in cyber. And by the way, whether that's just outing them and public shaming, whether it's sanctions or other means, we have a whole host of tools at our disposal and need to use them where necessary.

**Stewart Baker:** [00:43:52] We do. The ones we've used – indictments, naming and shaming – only work if you can actually – after the first few, everybody gets used to it. It doesn't feel like naming and shaming unless you actually catch the guys, and that's hard with their state powers.

**Rep. Jim Langevin:** [00:44:13] Well, it's hard if you're just relying on cyber means.

**Stewart Baker:** [00:44:18] Right.

**Rep. Jim Langevin:** [00:44:18] However, this is where all-source intelligence has to come into play. And the more dots that we can connect, the clearer picture that we have. And we need to respond hopefully with an international response, not just a US response, but you can see, for example, when the US responded on the Russians' election interference, in some cases it would be through our diplomats, we imposed sanctions, we publicly named and shamed. I think that's appropriate. On the other front, when the Russians, by way of example, it was believed that they used a chemical agent to poison the father and daughter in Great Britain [Sergei and Yulia Skripal], there were enough dots that were brought together. There was high confidence that we knew where that came from, and the international community had an international response. It wasn't just one thing. It was all-source intelligence sharing, and it grew to a level of confidence that we felt that we could and should respond, and we need to approach that same kind of methodology, use that same methodology in responding to cyber intrusions or attacks. It gives you a more holistic picture. And by the way, doing it with international partners, the more united we are, the more it makes adversaries think twice before acting.

**Stewart Baker:** [00:45:46] So it does seem to me that in the last five years what has changed for the good on cybersecurity – plenty has changed for the worse – is that attribution happens faster and people accept it more than they used to. What can we do with better attribution to make sure we actually change the behavior of the aggressors?

**Rep. Jim Langevin:** [00:46:13] Well, in my mind it's like the issue if you're playing chess, for example – I'm a fairly decent chess player, and I'll look to see what my opponent is doing and you want to go counter and confront and respond. And again I believe that by just not relying on one source of intelligence, for example, you know what is the threat signature, where it's coming from, per se, but you understand a holistic approach using all-source intelligence. That's how you get a clear picture and then you have hopefully a firm response from there.

**Stewart Baker:** [00:46:53] So when you look over all of the federal resources we put into cybersecurity research, how much of that goes for offense and how much goes for defense, and is the mix right?

**Rep. Jim Langevin:** [00:47:08] Good question. That's something else that we're looking at right now. It has to be a balance. It's going to be an ongoing effort. We're never going to get to a point where you can say we've done enough. It's going to take a sustained effort and research and development, both on offense and defense is important. That's why that public-private partnership is essential. Some of it will come from government research and development and applying tools and the others might be commercial off the shelf the private sector will develop.

**Stewart Baker:** [00:47:37] So as ranking member on the Emerging Threats Subcommittee, you oversee DARPA, among other things.

**Rep. Jim Langevin:** [00:47:46] Yes.

**Stewart Baker:** [00:47:47] And they've started doing more and more on cybersecurity. Is there something they're doing that you think is particularly exciting or interesting?

**Rep. Jim Langevin:** [00:47:56] Sure. I think the next generation of cyber defenses will come through machine learning and AI advanced algorithms. And you know at some point down the road hopefully quantum computing will be part of the equation as well. But those are probably the next areas of investment that we need to continue to look at more closely and invest in properly.

**Stewart Baker:** [00:48:25] So I worked at both the National Security Agency and at the Department of Homeland Security, and I used to joke that I was the child of a broken marriage. You've also seen DHS and at least Cyber Command up close. How is that relationship today?

**Rep. Jim Langevin:** [00:48:43] Good and getting better. But I will say this: The Department of Homeland Security needs to continue to develop its own expertise and can't just rely on expertise from NSA or US Cyber Command, although they have the ability to detail people. We further enabled that in the last NDAA [National Defense Authorization Act] that we just enacted. But Homeland Security needs to have its own team and experts so that they get very good at what is in their area of responsibility. And so they are getting better and just had a major win with the reorganization of CISA [Cybersecurity and Infrastructure Security Agency].

**Stewart Baker:** [00:49:29] Yes, congratulations.

**Rep. Jim Langevin:** [00:49:31] Thank you. It was something we've been pushing for for a long time, and a lot of credit to Bennie Thompson and Mike McCaul pushing hard for that. And we have a great new first director in Chris Krebs at Homeland Security. I'm excited what he will do with this new reorganization, but it clearly sends the message this is about cybersecurity infrastructure protection. They need to continue to have resources to do the job and get better organized and resourced, but great skill set and dedicated people there. The other thing we need is still – Homeland Security needs to have the authorities to reach across government and compel departments and agencies to do what they need to do in cyberspace. That's why a cybersecurity coordinator, by

the way, is so important. And I was disappointed when the cybersecurity coordinator position at the White House was eliminated. It's the first major step backward in cyber, by my count, through several administrations. Even in the early days of Trump Administration, they were moving the cyber ball forward. But when the new national security adviser came in, he eliminated the cyber coordinator position, and that was a mistake. And also we need to have a cyber coordinator position at the State Department. It's not a US problem only. It's a US challenge, an international challenge. And we need to have State Department have a lead role in it too. But right now there's still not enough clarity of who has the authority to coordinate and who has the carrot and the stick. I know the Department of Homeland Security has been named as the lead agency for protecting the .gov domain, but they don't really have the policy and budgetary authority. Nobody does yet. And I'd like to see a director's position in the White House, Senate confirmed. I've had that legislation for the last several years. That actually came out of the CSIS commission as a recommendation, and I believe at some point it will happen. But so far it hasn't. And so OMB is kind of a clearinghouse for what departments and agencies really have to do. The only thing DHS can do is a binding operational directive, but unfortunately that has no teeth.

**Stewart Baker:** [00:51:48] Which is why they call it "binding," because it isn't. [Laughter]

**Rep. Jim Langevin:** [00:51:51] Right. And so I've brought that through the last couple of administrations. And it sounds very authoritative, but it doesn't really mean a whole lot if departments ignore it and there's no stick.

**Stewart Baker:** [00:52:02] So would you give them the authority to make their binding operational directives truly binding?

**Rep. Jim Langevin:** [00:52:09] I think that's a good start for sure. Whether you invest that power in the Secretary for Homeland Security or in the department there or it's a director of cybersecurity or cybersecurity coordinator that has both policy and budgetary authority like the US trade representative, for example, and things need to be cleared through the trade representative before these funds are spent, or whether it be the drug

czar, if you will, that this coordination and there's more authority and you're doing a coordinated effort and response. I think that's the important – somebody has to have that ability. Right now nobody does.

**Stewart Baker:** [00:52:48] It's often hard to sell White Houses on the idea that they should have people inside the White House who have made promises to get confirmed to the Senate. My view has always been that the White House is so attuned to what the president wants, whoever he is, that anybody who has a conflicting set of obligations gets looked at askance and then excluded from the important meetings.

**Rep. Jim Langevin:** [00:53:14] That's unfortunate.

**Stewart Baker:** [00:53:16] But the drug czar is a good example. I don't think people think of him as being part of the White House in most respects. That's where he's technically housed, but I'm not sure that the president is inviting him to a lot of meetings other than the ones that he asks for. So I do think it's unfortunate that they got rid of the coordinator, but what I'm sure they would say is we're doing plenty of coordination as it is. And Treasury and the Justice Department have worked very well, along with the Commerce Department, to impose sanctions on people who steal data, who violate sanctions, who steal Bitcoin or use Bitcoin from ransomware. So there is coordination going on. It's just not happening through somebody with the title.

**Rep. Jim Langevin:** [00:54:16] Well, I think coordination does happen informally, and I think that is fine. But I'd like to see a more formalized role, if you will.

**Stewart Baker:** [00:54:29] And what about breach notification? Is that going to be something that the Democrats are going to take up in the House?

**Rep. Jim Langevin:** [00:54:36] I certainly hope so. I have a bill on data breach notification. Right now we have 50 states with 50 different data breach notification laws. I think it makes more sense to have one uniform standard, so my bill would be a uniform 30-day standard on data breach notification. The FTC would be the coordinating agency

to respond and coordinate response and determine whether or not customers need to be notified or not of data being taken and incentivizes really businesses to do more to protect their own data. For example, if data is encrypted and it gets stolen, it's rendered useless by the fact that it's encrypted, so presumably companies wouldn't have to notify customers because there could be no harm to their data. It's rendered useless if it's encrypted. So again I'm going to push my bill to get through the Congress, but I think it's something has to happen eventually.

**Stewart Baker:** [00:55:36] It's been kicking around for so long, and preemption was always the hard issue. Is the federal standard going to replace the 50-plus state laws? Do you think that's going to be the key question in the debate between the House and the Senate and among the Democrats?

**Rep. Jim Langevin:** [00:55:57] I think preemption is essential. Otherwise it just becomes the 51st data breach law, if you will, and so I'd rather have one uniform standard. I think it's in businesses' interest and customers' interest to have that kind of a mechanism going forward. Customer data needs to be protected. Let's have a uniform standard to do it.

**Stewart Baker:** [00:56:24] So last question on this topic: Cyber Command. You've seen them up close. They've gone through growing pains obviously. How do you think they're doing? What's good about Cyber Command, and what do they still need to work on?

**Rep. Jim Langevin:** [00:56:43] I'm pleased with the progress that Cyber Command is making. Their 133 teams have reached FOC (full operating capability) in May of 2018, and they will continue to mature. And we want to make sure that they have the resources to do their job effectively. Ongoing training and recertification is going to be important. But the different missions and protecting the government and having the teams that are in place to assist combat commanders to achieve the mission in theater is essential. Never gonna see modern warfare again without some type of cyber component to it, and so having those teams in place working with combat commanders is important. And then the national mission teams that are being more proactive and

going out and targeting the bad guys that are targeting us. That's another important mission that they want to take.

**Stewart Baker:** [00:57:47] And that's the "defending forward" part of their approach, getting into the networks of adversaries.

**Rep. Jim Langevin:** [00:57:56] We have the national mission force, and then you have the combat mission teams.

**Stewart Baker:** [00:57:58] When I hear criticisms of Cyber Command, it's that they are not likely to make a strategic difference or nothing that they have done up to this point in a conflict or in preparing for a conflict has been of truly significant impact. Do you buy that criticism?

**Rep. Jim Langevin:** [00:58:21] No. I think they're having a very positive impact. You know we're not going to know about everything, per se, obviously. I absolutely believe that they have had and will continue to have an impact.

**Stewart Baker:** [00:58:37] So I have to say, because I spent a fair amount of time in Rhode Island, I've been to the Bristol Fourth of July day parade –

**Rep. Jim Langevin:** [00:58:46] Oldest Fourth of July parade in the country.

**Stewart Baker:** [00:58:48] Yes, exactly. 1776 or so, or practically. And I saw you go by in what looked like a Segway version of your wheelchair. Does this chair stand up?

**Rep. Jim Langevin:** [00:59:03] It does. So this chair, they call an iBOT, was invented by the same inventor of the Segway, Dean Kamen, and it's a great piece of technology. So it is four-wheel drive as well as the balance mode, where you're popping up on two wheels. Yes, it's changed my life and given me more independence because you know when you're up on two wheels in the balance mode, being able to talk to people at eye level –

**Stewart Baker:** [00:59:28] It makes a difference.

**Rep. Jim Langevin:** [00:59:29] In my business – I have such a social business – to be able to talk to people eye to eye is important, so when I go on the House floor and I'm talking to colleagues, I'm doing it from equal footing, if you will.

**Stewart Baker:** [00:59:39] Okay. So you do use it here in the House.

**Rep. Jim Langevin:** [00:59:43] Oh, yeah. Oh, absolutely, and if I go on site visits and things like that. For example, even on you know rough terrain, construction sites, or groundbreaking, you can put it in four-wheel drive and this will go like a dune buggy on rough terrain and sand and can even take it on the beach. It's a pretty capable piece of equipment.

**Stewart Baker:** [01:00:03] So your paralysis clearly moved you in the direction of the career you've found. It was an accident, wasn't it?

**Rep. Jim Langevin:** [01:00:13] It was. I was a police cadet or explorer scout when I was a teenager, and I fell in love with law enforcement. I thought that would be my career, and I was involved in the cadet program for four years. And unfortunately I was in the locker room at the police station one afternoon, and two police officers were looking at a new weapon that one of them had purchased. And he didn't realize it was loaded and pulled the trigger to test it, and the bullet ricocheted off a locker and went through my neck and severed my spinal cord. So I've been unfortunately paralyzed since I was 16 years old, but I had deep appreciation for public service. Even back then I thought I was going to be in law enforcement. And one thing led to another. I had great community support, and people rallied around, as I said, my family and I. And it made me want to give back in some way. I started getting more and more interested in government, and the next thing you know, somebody suggested I run for political office. And I did, and I thought that was a good way of starting the process of giving back. But I didn't think it was going to be a lifelong career, but I found something that not only did I

feel I was giving back but it was something I really enjoyed. And one thing led to another, and I kept running for different offices. It's worked out pretty well. I'm grateful for the support of the people back home and also the opportunity to make a difference for the folks I represent.

**Stewart Baker:** [01:01:33] Well, Congressman Langevin, it's a pleasure to talk to you, and thank you very much for your candor.

**Rep. Jim Langevin:** [01:01:38] Thank you very much. Great to be with you. Appreciate your expertise and the attention you bring to the topic of cybersecurity. Hope we can continue to talk further.

**Stewart Baker:** [01:01:47] Terrific. I'll see you Fourth of July in Bristol.

**Rep. Jim Langevin:** [01:01:49] Sounds good.

**Stewart Baker:** [01:01:50] Thanks. Okay. Special thanks to Representative Langevin, to Denise Howell, who was terrific, and to Nate Jones, Gus Hurwitz, and Nick Weaver for joining me. This has been Episode 243 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Apart from letting the cryptocurrency folks take over the podcast next week, you're not going to hear from me until January. So everybody gets a Christmas break from all the bad news, which seems to be pretty much all we cover. Have a great holiday, and we'll see you back in January. Be sure to send us suggestions for guest interviewees. For comments and suggestions, send them to CyberlawPodcast@Steptoe.com. Please do leave us a rating for our show. That's how people find us. And I have promised to read the most entertaining reviews, good or bad. And the credits: Laurie Paul and Christie Jorge are our producers; Geoff Kesler is our audio engineer; Michael Beaver is our intern; I'm Stewart Baker, your host. Please join us again in January as we once again provide insights into the latest events in technology, security, privacy, and government.