Episode 230: Click Here to Kill Everybody

Stewart Baker: [00:00:03] Welcome to Episode 230 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. We are back and full of energy. Thank you for joining us. We're lawyers talking about technology, security, privacy, and government. And if you want me to talk about hiking through the rain forest of Costa Rica and just how tough my six-year-old granddaughter is, I'm glad to do that too. But today I'm joined by our guest interviewee Bruce Schneier, an internationally renowned technologist, privacy and security guru, and the author of the new book, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. We'll be talking to him shortly. For the News Roundup, we have Jamil Jaffer, who's the founder of the estimable and ever-growing National Security Institute. He's also an adjunct professor at George Mason University. Welcome, Jamil.

Jamil Jaffer: [00:00:57] Thanks, Stewart. Good to be here.

Stewart Baker: [00:00:58] And David Kris, formerly the assistant attorney general in charge of the Justice Department's National Security Division. David, welcome.

David Kris: [00:01:07] Thank, you. Good to be here.

Stewart Baker: [00:01:08] And he is with his partner in their latest venture, Nate Jones, veteran of the Justice Department, the National Security Council, and Microsoft where he was an assistant general counsel. Nate, welcome.

Nate Jones: [00:01:23] Thank you.

Stewart Baker: [00:01:25] I'm Stewart Baker, formerly with the NSA and DHS and the host of today's program. So because we've been on hiatus for a while and then talking

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

about blockchain and Bitcoin, I thought I would start by asking a few of our folks what, if you were talking to other people who were smart enough to spend August out of Washington or out of the office, what should they read that came out in the last several weeks? Let me just throw that open. Jamil, you got a recommendation for something that people might have missed because they weren't in town and that they really ought to read?

Jamil Jaffer: [00:02:08] Well, it's a layup, Stewart, because we're going to talk about it just next. But it's the *Wired* article on NotPetya, and sort of it gives you some great atmospherics around the events that took place, what actually happened with that malware, and how they identified what was going on. And you know in a lot of ways it's a very small version of the amazing Kim Zetter book on the alleged efforts against the Iranian nuclear.

Stewart Baker: [00:02:38] Yeah. So this is a kind of breakdown of what happened at Maersk, the big Danish shipping giant. And basically NotPetya took out all their computers in about 45 seconds, if I remember right. And they were out for weeks. People couldn't unload ships because they didn't know where the cargo was or where it was going. It was a disaster.

Jamil Jaffer: [00:03:04] It really was, and you know what's amazing about the recovery effort was that in part it depended on one domain controller in Ghana that had not gone down because a power surge had knocked it offline, and so it wasn’t connected to the Maersk network...

Stewart Baker: [00:03:19] At the time when all of the wildfire burned through the rest of the network.

Jamil Jaffer: [00:03:24] Exactly. And so they were able to reconstitute part of network from that. There's description in there of their consultants from Deloitte going out to every store in the neighborhood and buying new laptops and Wi-Fi – mobile Wi-Fi, prepaid Wi-Fi pucks – in order to get them back up and running. Meanwhile, all around the world at the 72 ports that Maersk has operations at, 800 shipping vessels all shut down, making up almost a fifth of the world's bulk shipping capacity. Kind of an astounding thing. And by the way, not the intended targets of the hack. In fact, the entire thing turned on one executive in the port city of Odessa installing this Ukrainian tax software...

Stewart Baker: [00:04:10] Which he needed to pay their taxes, right? And he got permission, and just that one vulnerability which the Russians had introduced was enough to break Maersk's network.

Jamil Jaffer: [00:04:23] It's astounding. It's astounding.

Stewart Baker: [00:04:25] It is. Let me ask David. David, do you believe that this was unintended, or was this the Russians saying, "Hey, you do business with the Ukrainians at your own risk"?

David Kris: [00:04:36] Yeah, it's very difficult to know. I mean one of the dangers in releasing you know computer viruses like regular viruses is they can mutate and they can get all over the place. So it's difficult to assess, but it sure is I guess a lucky piece of bad luck if it wasn't intentional. You know what I mean?

Stewart Baker: [00:04:56] Two other things that I thought were interesting from that story. One: $300 million it cost Maersk. And so the idea that this might have cost $10 billion globally is not out of line. There were several other companies that reported $300 million losses as a result of this.

Jamil Jaffer: [00:05:15] I mean astounding amounts of money when you think about it through an exploit that probably didn't cost that much to develop. At the end of the day, they were using an alleged NSA exploit called Eternal Blue, an older capability called Mimikatz, right, in combination. Yes, it takes some work to put those together and make them work effectively. To be sure, these are not capabilities that the average person has. But at net-net cost, not that high particularly compared to the massive price it cost the world economy.

Stewart Baker: [00:05:45] And that would be another motivation for making this kind of sloppy and easily spread. They thought it would hurt NSA's reputation globally because they were using Eternal Blue vulnerability. So that's the other question. This is completely indiscriminate, completely disproportionate to any legitimate or even illegitimate goal that the Russians might have had. I think you could line up 40 JAGs [Judge Advocates General] in the US DOD and say, "This is what we want to do," and they'd all say, "Oh, that's a violation of the international law of war as it applies to cyber tactics." Russians just did it. Are they paying a price? I don't think that anybody has accused them of war crimes.

Jamil Jaffer: [00:06:37] Well, that's exactly the problem here, Stewart. Right? I mean I think that you raise this point about – you know Kirstjen Nielsen has said, "Look, we need to be more aggressive. We need to lean forward." You've been even more aggressive and out front saying we need a whole realm of capabilities and maybe even to start really punching people back in the face and maybe elsewhere. And so I think that's a part of the conversation that has to be had because you know one of the things Secretary Nielsen said that I think that was interesting was some of these things may be covert or they may be unseen. Right? Part of the challenge with deterrence and part of the reason why deterrence doesn't work when we talk about cyber is because we too often use capabilities that we don't talk about or responses we don't talk about. We don't talk about what our red lines are. We don't say what's gonna happen when you cross those red lines. And I realize "red lines" is a dirty word now because we don't enforce them. But at the end of the day, if you're going to really have deterrence work – it's not that deterrence doesn't work in cyberspace, it's that we just don't practice deterrence in cyberspace. If we were to, I bet you it might work, but you've got to be willing to punch back. And that punch might come in cyberspace, or it might come somewhere else. We're just not ready to do that yet.

Stewart Baker: [00:07:36] So in the world of punches in the dark, my favorite story is the Intrusion Truth site which is kind of DCLeaks for good guys. It is basically a site devoted to outing the APTs, the government advanced persistent threats, and disclosing again sort of what we've started to get used to. And there are stories about Intrusion Truth that are really kind of fun because they show that the Ministry of State Security in China... You know there are a lot of ways to read the indictment of PLA members and the reaction to it, but one way to read it is that it spurred a turf fight in which the Ministry of State Security went to Chairman Xi and said, "Those bozos can't hack their way out of a paper bag without getting caught. Leave it to us. Kick them out. We won't get caught. You can promise not to steal commercial secrets because we ain't gonna get caught." And clearly the PLA was shut down for a long time. Now it turns out that the Ministry of State Security is getting caught as well. And it's an anonymous site that might or might not have some ties to official hackers that is disclosing some of this stuff.

Jamil Jaffer: [00:09:06] Yeah, I mean look, you know it's funny you might imagine some of these discussions in China might mirror things happening in other parts of the world you know where there are capabilities the Intelligence Community and capabilities the military and the debate about who should be doing what and what axes are being breached, are being blown up when you know an effort takes place. And so it would not surprise anybody to know that China is not the only place these conversations are happening and these back and forth internal dynamics take place. And you know as far as who's outing them, I mean you know the Russians aren't the only people who play covert influence operations.

Stewart Baker: [00:09:43] Right. Okay. Nate, David: your favorite story that people should go back to be sure they read now that they're back in town?

David Kris: [00:09:52] Well, mine is the 170-plus page criminal complaint filed against a gentleman named Park Jin Hyok. It was filed in June but released more recently. And he is the only defendant charged in that complaint with the Sony Pictures hack from 2014, with a theft of $81 million from the Bank of Bangladesh, and for various misconduct involving the WannaCry malware which did some damage to the UK and particularly to its health system. The complaint is long, and it's interesting reading, if you have an appetite for that sort of thing, in I think three ways. First, it tells you a bunch of things about cyber tradecraft and what people do and certainly some tricks on what not to do since this guy got caught. And then there are two aspects of this that are interesting from the perspective of responses to these threats in the name-and-shame category. So let me sort of step through some of it. On the tradecraft side, you have a very detailed explanation of the behavior here by the arm of the North Korean government sometimes referred to as Lab Number 110 that Park was a part of: the reconnaissance that they engage in, the spear phishing that they engage in, and the way in which in the spear phishing they actually have evolved from using made-up emails that purport to come from Facebook or Google or whatever and usually have bad English and can be detected to just cutting and pasting actual emails that those providers send and then inserting different hyperlinks so that if you click, you're dead. It just shows how difficult it is for end users individually to resist these kinds of spear phishing attacks. There's a nice analysis of the forensics of malware and signature analysis. There's a nice detail about how this group of North Koreans was operating in China physically.

Stewart Baker: [00:12:04] Yep.

David Kris: [00:12:04] You know North Korea doesn't have that many IP addresses, so maybe they needed some better bandwidth. Anyway. And the big lesson I think for the cyber crooks out there is you know do not use the same email address or a variant of your email address or the same IP address for your open and public business consulting that you use also for your illegal and improper malware-based cyber malfeasance because, believe it or not, eventually the Federal BI [i.e., the FBI] can connect the dots there. So that's what happened to poor Mr. Park. So that's sort of a summary of the tradecraft stuff that's in here. It's really got a lot of detail and vocabulary and other interesting reading for those who care. I think it's part of a trend towards you know the US government naming and shaming. Jamil was talking about sort of the difficulty in developing red lines and a broader cyber strategy. I think that's particularly challenging these days as our adversaries are both using cyber techniques in a standalone and as part of a broader array of challenges mixed with propaganda and related efforts and as we continue I think to look at things in a silo’d fashion. And what you've seen since the indictment of the Chinese Army folks awhile back is this move towards naming and shaming. We've indicted uniformed personnel. We've indicted what amount to cyber mercenaries and then outright cybercriminals. And you know people can debate whether that's a good strategy, whether it's kind of a pathetic flailing in the absence of any real deterrence or strategy that we have...

Stewart Baker: [00:13:48] Don't you think that the more that we do it, the more it feels like pathetic flailing? I was a big supporter of doing this, and I'm not saying it's a bad idea to have done what we've done. But it's very easy to jump the shark if you just keep doing this and nothing happens to the people that you've indicted.

David Kris: [00:14:06] Yeah, well, you know the one counterpoint to that is the Southern District of New York was just able to extradite a Russian hacker who was taking aim at US financial institutions and news organizations. Now he doesn't have any alleged direct connection to the Russian government – although, who knows? – but it does point out the long arm and the long memory of the law here. So Stewart, without really taking issue you know with your skepticism, I will say at least those GRU officers will not be coming to visit Disney World anytime soon, or if they do you know they'll get nabbed. So we have that satisfaction, I suppose.

Stewart Baker: [00:14:48] This is why the Chinese wanted their own Disney World inside China!

David Kris: [00:14:53] Right. [Laughter] People are agitating in mainland China to be able to visit, and once they get indicted you know they can't travel.

Nate Jones: [00:14:59] I also suspect Mr. Park isn't taking a lot of overseas vacations for fun.

David Kris: [00:15:05] Yeah.

Stewart Baker: [00:15:05] Well, it's not like the North Korean tourism is a big part of any country's plan for the future.

David Kris: [00:15:12] Oh, isn't that the truth. Yes, yet another reason you can't leave. So and then the second aspect of name and shame – which is you know is schadenfreude for some of us – is there is an article in BuzzFeed just reminding the world of all these cyber experts who at the time in 2014 expressed deep skepticism at the FBI's then-public assessment that it was indeed the North Koreans who were responsible for the Sony Pictures hack. This complaint you know is pretty detailed and represents the US government saying that it's prepared if necessary to prove beyond a reasonable doubt that that's what happened here. And so it sort of comes in even above a high-confidence assessment from the Intelligence Community, and this BuzzFeed article takes pains to point out all the people who said to the contrary and now are either out of business frankly in some cases or are eating their hats. You know and that's fun for the anti-contrarian contrarians among us you know who see that indeed it seems like the FBI could put its money where its mouth was.

Stewart Baker: [00:16:27] Oh, yeah. This is kind of satisfying because there was an element of seeking publicity by picking on the FBI and trading on skepticism about government. And the accusations that the FBI got this wrong we're loud and self-righteous, and then they sort of gradually kind of pulled back. There was never a reckoning, but this BuzzFeed article really is the reckoning to say you know there are consequences and there ought to be consequences for being so flamboyantly wrong in trashing your own government.

David Kris: [00:17:09] Right, which is you know not to say that you shouldn't be skeptical, but it is to say that I think you know those who said, "Oh my god, you just fell for the old spoofed IP trick and merely because this appeared to have an IP address associated with North Korea, you FBI knuckle draggers you know just sort of jump to conclusions." Well, it turns out if you read the 172-page complaint, you know there's considerably more detail and analysis behind it. So you know I guess that's a good thing, and it is only fair to have the skeptics now called out as indeed they were in that BuzzFeed article.

Stewart Baker: [00:17:45] Okay so let's try to pick up a couple other things that actually did happen in the last week. Also in the last week there was something called a Five Country Ministerial that got lots of coverage on encryption. Nate, is this new? And who the hell is the Five Country Ministerial?

Nate Jones: [00:18:09] I'm not sure I can answer the last question. But no I mean it's been referred to in the press as the Five Eyes. I mean it is the Five Eyes countries, so to speak, but it is generally a different part of the government. It's the homeland security and public safety components of the Americans, the Canadians, Australians, Kiwis [New Zealanders], and I've forgotten one...

David Kris: [00:18:36] The Brits.

Nate Jones: [00:18:36] The Brits, yes, of course!

David Kris: [00:18:36] Don't forget the Brits!

Nate Jones: [00:18:36] Don't forget the Brits. The statement itself is not anything particularly new, I don't think. You know it sort of recited their support for encryption, some of the challenges they're facing in criminal investigations, and you know I think they've continued to try to encourage technology companies to voluntarily do what they believe is the right thing and provide these governments with appropriate access even to encrypted data. Probably the newest thing was that it contained a written threat, I guess of sorts, where they said you know if technology companies don't do that, they'll pursue "technological enforcement legislative or other measures to achieve lawful access solutions." You know again this doesn't necessarily represent a whole of government endorsement for any of these countries. It's just a particular component, but I think you do have to read this in the context of other recent developments including some that have appeared in the press lately. In the US, for example, this would have at least been vetted by other departments and agencies who have a stake in this, so I think you can kind of assume that it represents the view of the Trump Administration and the executive branch. You know further supporting that view, you have the ongoing litigation reportedly about the wiretapping of messenger calls, voice calls. And what I think you're seeing in the US, for example, is Congress remains reluctant to get involved. They're worried about the security implications, not sure they really understand either side, but they're just reluctant to pick a side. Whereas the executive branch is I think getting more aggressive, and they're turning to existing law on the so-called "technical assistance" authorities they have to seek to enforce those companies and force them to decrypt data. Outside of the US, I think we're seeing that this is more likely to represent a whole of government view that the Brits were obviously the first to go with their legislation. The Aussies are not far behind. And even beyond the so-called Five Eyes countries we're seeing other governments including in Europe pushing for some kind of action on encryption. So I think on the whole what we're seeing is Five Eyes is certainly leading this effort to deal with the so-called "encryption challenge" that law enforcement is facing. The governments are taking a common approach on this by resorting to "technical assistance" authorities, either enforcement or legislation. Non-US countries, countries outside of the US, are moving more aggressively and actually legislating on this, imposing these "technical assistance" obligations, making them clearly applicable to US tech companies. And finally again they're not alone. There are other governments who are agitating on this. And so while nothing to me feels particularly imminent on this front, there seems to be a trend in this direction of having a reckoning on this issue.

Stewart Baker: [00:22:00] Yeah, I think if you're a company that has taken a strong stand on this – the image I have is of that Yukon prospector who's got a big fire, and every time he looks up, the wolves' eyes look a little closer. A lot of countries are creeping up on this issue, and they are not retreating. They're keeping the ground that they've taken, and then the next one comes in for a nip or to grab a piece of the pack. And you kind of know how this movie ends. But it may take another 10 years.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

David Kris: [00:22:43] You know, Stewart, what's interesting just to sort of underline a couple of points that Nate made, I do think this statement from the Five Eyes represents an expression of solidarity across the English-speaking Intelligence Community. And it's an extension of the kind of "Going Dark" complaint that the FBI has been making for a long time. The ironic element of it is the different tactics that these circling wolves are using to bite the poor prospector around the campfire because although this Five Eyes statement threatens legislation, and as Nate was saying, the Brits and the Aussies and others are enacting legislation at a pretty good clip, in the US we're seeing a different approach which I think is more to rely on litigation under existing authorities – the "technical assistance" provisions, in particular – and sort of either build a record for the need for legislation or get what they can get from the courts. So the different governments seem to be adopting different strategies. In Europe they are enacting laws. In the US they seem to have taken a break from those efforts and are instead going to court. And so it's going to be interesting to see which set of tactics produces which results going forward.

Stewart Baker: [00:23:55] Yeah, I wrote my meanest op-ed ever about what discovery might be like if the government sued Apple and was able to get discovery of the files, and I think discovery of the correspondence among the engineers about why they are doing certain things is bound to be damaging to the companies because it's going to show a kind of contempt for law enforcement and the FBI and the government and even the victims of crime. That you know shouldn't surprise us. These are engineers often not noted for their social skills, but who have a strong ideological opposition, who are bound to say things that the companies will regret. And so I wouldn't be surprised if one of the strategies for litigating this is to get access to those engineering emails.

David Kris: [00:24:58] Yeah, Stewart, when you say it's your meanest op-ed ever, that really sets a pretty high bar.

Stewart Baker: [00:25:02] Yes, it does!

All: [00:25:03] [Laughter]

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Nate Jones: [00:25:04] I've got to go out and read it!

Stewart Baker: [00:25:04] You should. It's called "Deposing Tim Cook," and I won't say I'm ashamed of it, but it is the snarkiest thing I've ever done.

All: [00:25:16] [Laughter]

Stewart Baker: [00:25:16] So I will never be allowed to buy an iPhone. Soon as they find out that it's my credit card, they'll cancel the sale. Alright. I think we ought to wrap it up there. Thanks to David, to Jamil, to Nate. And let's go to our interview with Bruce Schneier. I'm really delighted to have Bruce here. Those of you who relentlessly listen to every one of these podcasts got a bonus episode while we were on hiatus of me and Bruce dueling over his last book. And he's already got a new one out. It's called *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. Bruce is really internationally renowned and has been first as a cryptographer and then as a policy analyst, privacy and security guru. He's worked in industry. He's written book after book after book. It's remarkable. Some of them very technical. Some of them increasingly policy focused. This is policy focused, and I think what's interesting about it is the evolution in your views, Bruce. So why don't I just ask you to give us sort of the elevator speech of what this book says and maybe a little bit about what's new from your point of view?

Bruce Schneier: [00:26:38] So what I try to explain in this book is how everything is becoming a computer. Our appliances, our cars, our power plants, our consumer goods, they are all now computers with things attached to them.

Stewart Baker: [00:26:52] Our refrigerators. Soon I expect all our bridges are going to be computer connected, right?

Bruce Schneier: [00:26:57] Our everything, and it's less computer connected as that they are computers. A car is a computer with four wheels and an engine. And what that means is that everything we know about computer security becomes true about everything. But the difference is, is that these computers can affect the world in a direct physical manner. So a car can crash. An implantable medical device can kill somebody.

Stewart Baker: [00:27:23] So you and I are both old enough to remember those really funny jokes about how what if a car ran Windows and you had to be rebooted in the middle of the highway. It's happening.

Bruce Schneier: [00:27:34] That's going to happen. So everything that we've done in our industry, in computer security, has assumed that the computers were effectively benign. That it was just data. And when it becomes physical action, computers now affect life and property, and that just changes everything.

Stewart Baker: [00:27:55] Right.

Bruce Schneier: [00:27:56] It doesn't change the tech, but it changes how we interact with the tech. It changes our policy.

Stewart Baker: [00:27:59] Bad security kills people.

Bruce Schneier: [00:28:02] Right. As opposed to bad security just means your data's stolen, which could be loss of money, loss of privacy, lots of bad things, but nobody died.

Stewart Baker: [00:28:10] Right.

Bruce Schneier: [00:28:10] And that's what's going to change. And that's really what the book's about: how do we get security in a world of physically capable computers?

Stewart Baker: [00:28:19] And you make the point that complexity, expanding the attack surface, means that security problems that we've had in the past are just the beginning. We will continue to have more security problems. We're not likely to be able to fix them if we go down the road we're going down now.

Bruce Schneier: [00:28:40] Well, certainly not with the current business and political environment. You know we have made all these compromises with innovation, with companies, because like it didn't matter. So we don't mind patching. We don't mind really kind of lousy products that we have to secure after the fact. Even something like extensibility. This is a property of computers that they can be programmed to do anything.

Stewart Baker: [00:29:06] Right.

Bruce Schneier: [00:29:06] Right. So your phone can do anything, right? There's an app for that. I had a phone growing up. You remember it. It was big and black and attached to the wall. And no matter how hard you tried, it couldn't be anything other than a telephone. That's fundamentally different from your iPhone or any other computer. This is why we see malware on cars.

Stewart Baker: [00:29:25] Although I will say people have valued extensibility in computers, but the latest generation of computers – the ones that we call iPhones and Android phones – are a lot less extensible at least for the owners. And I wonder if we aren't seeing, as people struggle with security, a move toward locking these things down ever more tightly and the OS [operating system] provider taking responsibility for security in a way that reduces people's ability to tinker but also makes it a little less likely that we're going to have security holes.

Bruce Schneier: [00:30:09] I think the key is a little less likely because yes your phone gets lots of apps, your refrigerator doesn't, a power plant doesn't, a car doesn't. Those are extensible because they're computers and which just means you can have malware. You cannot have malware on an old school telephone, an old school refrigerator. There's no such thing.

Stewart Baker: [00:30:28] Well, there was that Captain Crunch whistle, right?

Bruce Schneier: [00:30:32] Yeah, but that's different.

Stewart Baker: [00:30:33] Yes.

Bruce Schneier: [00:30:33] That's different than someone dropping unwanted functionality onto your device.

Stewart Baker: [00:30:38] Right.

Bruce Schneier: [00:30:38] So as long as computers have CPUs [central processing units], are general purpose, and we're so bad at securing them, we have to worry about something like the Dyn botnet which attacked routers and webcams and digital video recorders, which shouldn't be extensible, shouldn't be able to get new software. But it turns out they can.

Stewart Baker: [00:31:00] Extensible was the default because that was the cheapest.

Bruce Schneier: [00:31:02] Right.

Stewart Baker: [00:31:03] It had already been developed for a much more sophisticated audience who wanted to be able to think where their computers, and it was just easier to rip off that entire library than to come up with something that was limited to doing what a router should do.

Bruce Schneier: [00:31:17] So this is an important point. This is the economics of the Internet of Things because everyone always asks: why does your refrigerator have any connection? Isn't that stupid? And the reason is and will be that it will be cheaper than not doing it. So it used to be 20 years ago refrigerators had CPUs. They were specially designed embedded systems. Today the cheapest thing to do is to pull a CPU off the rack and stick it in the device, and that CPU comes with an Internet stack. It comes with video software. It comes with all this functionality that costs so little to make active, and that's why you're going to see toys and all these devices that you can't imagine being on the Internet on the Internet. Now my guess is it will be cool that there will be applications and uses that you and I can't think of that the younger generation will revel in. And good for them. But that's also going to bring these vulnerabilities, and that's really what I want to talk about. What does that world look like?

Stewart Baker: [00:32:17] So some of the things you talk about as incentives for lack of security, I'm not sure I quite buy into. But let me talk about them. You basically talk about surveillance capitalism or surveillance as a business model, and it's pretty clear that companies that live by advertising live by selling much more granular detail about the potential buyer that you're serving the ad to. And I guess I feel as though that ship has sailed. We could probably make it harder for third parties to do that, but the people who collect the information – the Facebooks and the Googles – they're not ever going to go away. And the idea that they're going to collect more information is sort of built into the system, but they don't collect information through bad security. In fact they try to give us better security than we would get on our own.

Bruce Schneier: [00:33:17] Well I mean the way I think of it is everyone wants you to have security except from them.

Stewart Baker: [00:33:20] Yes.

Bruce Schneier: [00:33:21] So Google loves to give you great security as long as they can eavesdrop on everything. And to me as long as these businesses need surveillance to operate, they will have holes in your security so they can spy on you. And those are holes that others can piggyback on.

Stewart Baker: [00:33:40] So even if they give you end-to-end encryption, they need to know your location. They want to know your location, and they probably have come up with apps that make it cool to know your location like traffic apps.

Bruce Schneier: [00:33:52] And most of the time they don't want to give you end-to-end encryption because they want to mine that data, and you want them to do useful things with the data on their site. Gmail is useful precisely because it doesn't have end-to-end encryption, and they can sort mail and check for spam and do you know automatic responses and all the cool things that Gmail does that I don't know because I don't use Gmail. I think more importantly than surveillance is the architecture of control. So a lot of these companies want to very minutely monitor and then sell what you can do with your device. So Amazon doesn't just sell you books. They want to know how you're reading.

Stewart Baker: [00:34:34] What you're underlining.

Bruce Schneier: [00:34:35] What you're underlining. And they will decide depending on how you purchase it whether you can do text-to-audio, different things. I know a coffeemaker that monitors usage so it can up-sell you supplies and parts.

Stewart Baker: [00:34:50] Right.

Bruce Schneier: [00:34:51] Sony wants to put software onto their music to make sure you don't make illegal copies. All of those things are holes in your security as well. When we get to physically capable computers, when the car dealer wants to be able to automatically turn off the car if you don't pay your loan –

Stewart Baker: [00:35:10] And that happens.

Bruce Schneier: [00:35:11] and that happens – that opens the door for the bad guy to do the same thing. And I worry about that a lot more with physical computers than I do about surveillance. You're right the surveillance business model is here. I think forever is a long time, but in the near term, we're not getting rid of surveillance capitalism. I worry about control more in this world of physically capable computers.

Stewart Baker: [00:35:32] Okay. So I see what you're saying is that the people who sell us stuff want to be able to reach in later and tweak the experience or stop it if we haven't continued the stream of payments. And any such capability is something that if they're fully hacked means that hackers can do it to us too.

Bruce Schneier: [00:35:55] And it could be benign. I mean I have a programmable thermostat, and you can easily imagine the power company saying, "Hey, you know give us the ability to raise your thermostat a degree in the summer when there's peak load. We'll do better. We'll give you a discount." That's a perfectly reasonable thing to do. And you know any environmentalist would say, “Yes, that is a great thing for the planet.” Yet it's also a vulnerability.

Stewart Baker: [00:36:18] Yeah. If you're taking a shower and suddenly the state decides that you shouldn't, it's sort of annoying to have the hot water cut off.

Bruce Schneier: [00:36:25] I think the water wars are a few years off, but yes.

Stewart Baker: [00:36:28] [Laughter] Okay. You also say that you think that governments have an interest in taking away security. And you point to some famous examples: the proposed Clipper Chip, which I was a proponent of when I was at NSA, and controls on encryption (export controls). But you know I do feel as though those stories are getting a little long in the tooth. And all the people who in the '90s said if you would just get the state out of the way so that we could offer encryption and we'd have security, those people look dumb now don't they? I mean because we're so far from security nirvana that we can't even see it from here.

Bruce Schneier: [00:37:15] Oh, this gets back to everyone wants you to have security except from them. So yes, I mean we are both veterans of the First Crypto Wars. It's kind of amazing that was the mid-90s. I still have the t-shirts.

Stewart Baker: [00:37:25] Yes, that's right. And the poster.

Bruce Schneier: [00:37:28] The poster. I still have the poster. So yes, I mean right even now the governments are saying you know, "Yes, we want you to have security except from us."

Stewart Baker: [00:37:38] Right.

Bruce Schneier: [00:37:38] And it was fanciful to think that if we just let the government go away that companies would prize security because in fact corporations also want to spy on us. And I see it now as this kind of alliance fundamentally between the companies and the governments. And the bits of security we have – I think you're right – are few and far between. My worry – and again this is this is my point of the book– is as computers start killing people, that's going to look harder and harder to sustain. To say you know we know it makes our power plants more vulnerable, but we really want to spy on people. That was an okay thing to say, and we could argue about it when computers were fundamentally benign. It becomes harder when they're actually dangerous.

Stewart Baker: [00:38:29] So I wonder about that. It strikes me that if computers start killing people, it'll be people behind the computers who are killing people. And the response to that is going to be you need to track them down, you need to stop them from killing people, and the governments are going to say, "Well, the only way we can do that is to track them through cyberspace." I mean look at what companies do for cybersecurity monitoring. It's extraordinarily intrusive. They have to do it, but they break encryption on peoples' HTTPS connections because they have to because they have to see what's being exfiltrated. They have to see what's coming in. But that means that if you use a corporate computer to log on to Gmail, somebody down in IT has your credentials. And so don't you think that that's what the government is going to say? We need to do for the Internet what people have been doing for their intranets for 15 years?

Bruce Schneier: [00:39:33] My guess is you're right. They're going to say that, and we'll see how long that's tenable. And this how we're going to have to watch the future. As computers get more dangerous – I'd love to talk about attribution and tracking down bad guys later on because I think it's a really good conversation to have there – we're going to have to figure out whether we are more secure by locking down our stuff or more secure by keeping our stuff open so we can track down the bad guys. Now again, as the cost of getting it wrong increases, the value of locking it down beforehand increases, so it's gonna be an arms race we're going to watch. My guess is that defense dominant wins that – there's the phrase I can't even figure out who to attribute it to anymore: we might have the biggest stones, you also have the glassiest houses.

Stewart Baker: [00:40:26] Right.

Bruce Schneier: [00:40:26] As our house gets glassier, that we're going to need prevention, that detection and response works better against state actors, works terrible against non-state actors. You know it's really hard to tell in cyberspace who's attacking you. We can attribute some things, not others, but this will be the fundamental tension. And I think that's where policy gets interesting.

Stewart Baker: [00:40:50] So I want to move to some of the things you think we should be doing, can be doing, because that's really in many ways what's new here because these other critiques have been common and they were part of your other books to some degree. What is it that you think the United States, the West, the world can do to avoid catastrophes in this new totally connected world?

Bruce Schneier: [00:41:23] I think what's missing is government involvement in cyberspace. That traditionally this has been a government-free, libertarian, let-the-companies-do-what-they-want zone, which was okay when it didn't matter. Now that it matters, that's no longer tenable. So in my book I try to tease out what government intervention would look like, and I talk about a lot of things. We can look at a lot of other industries where government said, "Okay, industry, stop killing people." Right?

Stewart Baker: [00:41:49] Right.

Bruce Schneier: [00:41:50] You need to do these things right. And they can range from very heavy handed, which is like avionics or pharmaceuticals, to much more light touch, would be consumer goods and toys, to things in the middle. And I look at rigid rules and standards and flexible liability regimes and notions of due care. I mean I'm not an attorney, but I talk to many of them. Looking at how we can use international agreements because this is an international problem. How do we build systems that assume there are insecurities but regain security? And my guess is it's going to be a combination of all of these things.

Stewart Baker: [00:42:32] So this is one point where we agree and Silicon Valley doesn't.

Bruce Schneier: [00:42:38] That's right. But I look at the past century, and I can't find one industry that improved security and safety without being forced.

Stewart Baker: [00:42:47] Right.

Bruce Schneier: [00:42:47] Cars. Planes. Pharmaceuticals. Medical devices. Food. Restaurants. Workplace. Consumer goods. Most recently financial products. In every case, the economics rewards skimping on security and safety, taking the chance, hoping you do okay, rolling the dice in the courts if you don't, and stalling regulation as long as possible. That's what happens.

Stewart Baker: [00:43:13] And then something bad happens and people say, "Okay, that's enough. We've had it." Right?

Bruce Schneier: [00:43:18] My worry is that computers fail differently. Right? You know there's tainted lettuce and some people die. That's terrible, and we want to fix that. But computers work perfectly until one day when none of them do. That's the way they fail. So we could easily wake up one morning and all the cars don't work – or more likely all the cars of one particular make and model year. And you know my title of *Click Here to Kill Everybody* is still science fiction, but we could easily have that.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:43:51] Unfortunately, you can see that world from here.

Bruce Schneier: [00:43:51] You can see it, and you can certainly see catastrophic failure where all the cars of a certain make and model year suddenly the brakes don't work.

Stewart Baker: [00:43:59] Right.

Bruce Schneier: [00:43:59] And that's not science fiction. We've had researchers demonstrate brakes failing remotely. There's a great YouTube video of a reporter, and the expression on his face when the hackers actually do is – I don't want to use the word "priceless," but it's worth watching.

Stewart Baker: [00:44:15] Yeah, because it's one thing to know it's possible. It's another thing to put your foot on the brakes and nothing happens.

Bruce Schneier: [00:44:22] Right. And now computers can do that.

Stewart Baker: [00:44:24] Because it's all fly by wire.

Bruce Schneier: [00:44:27] Right. And they're all interconnected. And the disaster we talk about now – the easy ones to talk about are cars and medical devices, also airplanes. Right?

Stewart Baker: [00:44:35] Right.

Bruce Schneier: [00:44:35] You know DHS demonstrated – we don't know the details – but hacking an airplane in the air by someone on the ground. We know in some ways that's been demonstrated.

Stewart Baker: [00:44:45] So medical devices is interesting, and we're going to have the woman from the FDA who regulates the cybersecurity of medical devices on in a couple of months. But the FDA is a regressive regulator. They have a really strong regulatory culture, and yet their handling of cybersecurity really doesn't fit the way most of us think cybersecurity should be handled. They've stayed away from it. They have not really encouraged responsible disclosure and response. And you know part of it is it's a different culture. But you know going in to repair your phone means just taking the back off and voiding the warranty. It's a different thing when you have to actually open somebody's chest.

Bruce Schneier: [00:45:35] Right. And there was a software update to I think a St. Jude medical device that didn't require opening up your chest, which is a good thing, but then we have to worry about can someone drop malware on it? It'd be interesting to watch the FDA. I think they are being affected by this you know libertarian, don't-slow-innovation culture of Silicon Valley. And when I talk, I'm asked a lot: won't this slow innovation? I have sort of two answers. The one is: yes, and maybe that's a good thing because when innovation can kill you, you do want to slow it down.

Stewart Baker: [00:46:07] Right.

Bruce Schneier: [00:46:07] And the other is that if you set the incentives right, you actually get innovation working on your side. We've seen this in cybersecurity in so many areas. The example I always like to use are credit cards. There's been so many advances in credit card security because government went to the credit companies in 1978 and said, "You are liable for fraud."

Stewart Baker: [00:46:28] Right.

Bruce Schneier: [00:46:28] "Not the customer."

Stewart Baker: [00:46:28] And so having internalized it, they had to fix it.

Bruce Schneier: [00:46:31] They had to fix it.

Stewart Baker: [00:46:31] I think you're right. And ten years ago you would have said, "Well, that's just not going to happen. Everybody loves the coolness of the new technology." But I think that climate is completely different in the last two years.

Bruce Schneier: [00:46:47] I think it is, and I think physically capable computers makes even more different.

Stewart Baker: [00:46:50] Yeah.

Bruce Schneier: [00:46:50] I mean we are seeing a sea change in how we treat personal tech, which I think surprised a lot of us.

Stewart Baker: [00:46:57] So even so, regulation is slow. The only thing slower than regulation – the only two things I can think of slower than regulation are: one, using the courts and expecting them to enforce standards long after the fact. Some judge says, "Oh, that sounds insecure to me." What do they know? And even worse, even slower is trying to do this internationally as you had suggested. We are still waiting for the world to adopt the 1985, I think, Budapest Convention, which just takes the CFAA [Computer Fraud & Abuse Act] and writes it into treaty saying, "Yes, people who attack, who engage with computers in an unauthorized fashion, without rights should be punished. And you need to have a 24-hour hotline so we can call you to help track people." The Indians, the Chinese, the Russians have said, "Oh, that sounds like Western imperialism to us." If we can't even get agreement on that, how are we going to get agreement on the NIST [National Institute of Standards and Technology] cybersecurity framework?

Bruce Schneier: [00:48:04] So I don't know, and here's our problem. I think it's bigger than cybersecurity. I mean are we moving into a world where tech moves faster than policy?

Stewart Baker: [00:48:14] Sure!

Bruce Schneier: [00:48:14] You're right that any kind of regulation is going to be slower than we want. I don't have an alternative though. So who's most agile? The courts can be agile. They're slow, but they're better than the legislators. The regulatory agencies? You know if they have flexible standards, you can see them ratchet it up. That's the best I got. And you might be right that they're going to be too slow. If they are, we're screwed. You know we are moving to a world where tech is moving fast, where catastrophic risk is moving fast, and we're going to need to figure out what agile government looks like. And this is a good place to start as any. I agree with you that international treaties are going to be slow. We need them. I agree with you that norms are even slower. We need them. We need to figure out how to make this work. I mean right now I don't see the US government doing anything anytime soon. I'm looking to Europe, who really is the regulatory superpower on the planet right now, and they are flexing their muscle. And to some of the US states. California, New York, Massachusetts are aggressive states in this area.

Stewart Baker: [00:49:31] In privacy, not in security.

Bruce Schneier: [00:49:33] They're going to move there.

Stewart Baker: [00:49:34] They're going to have to go to security.

Bruce Schneier: [00:49:34] They have to. I think GDPR [General Data Protection Regulation in Europe] was just step one. I think security is next because security is actually more important, more dangerous than privacy.

Stewart Baker: [00:49:45] Yeah, but the problem in Europe is of course that privacy ideologues don't care about security or at least they think that that's a subordinate concern to privacy.

Bruce Schneier: [00:49:55] So I'll argue that in this area we've gone past the debate of regulation / no regulation that the debate is now smart regulation versus stupid regulation.

Stewart Baker: [00:50:06] Right. Okay.

Bruce Schneier: [00:50:06] When something happens, when there's a catastrophe, people will demand the government must do something. And you know the government can move fast. The Patriot Act was passed really fast.

Stewart Baker: [00:50:16] Right.

Bruce Schneier: [00:50:16] Because something must be done. Here was something. Therefore we did it. With no thought. Nobody read it. It just was passed. And that same thing will happen when cars kill 500. And that worries me because we're going to get really lousy regulation that way.

Stewart Baker: [00:50:31] So the United States is almost certainly going to borrow the techniques of Europe, even if we don't borrow the GDPR, and just say if you do business with the United States, if you send your stuff here, you're subject to our security regulation. And that's standard tort law anyway. But isn't that a way of regulating that doesn't require a lot of international negotiation?

Bruce Schneier: [00:51:00] It might be. I mean I worry a lot about some of the Third World countries because you know these toys are gonna be made in some random country. It'll be interesting to watch how this works. So the car I buy in the United States is not the same car I buy in Mexico.

Stewart Baker: [00:51:16] Right.

Bruce Schneier: [00:51:16] Right. Environmental laws are different. And Ford sells different cars. But the Facebook I get in the United States is the same Facebook I get in

Europe. We saw GDPR, and we in the US have to deal with all these annoying warnings that are showing up on our websites.

Stewart Baker: [00:51:29] [Laughter] Yes, exactly.

Bruce Schneier: [00:51:30] Because it's easier for these companies to have one product or service and sell it around the world.

Stewart Baker: [00:51:35] Right.

Bruce Schneier: [00:51:36] So here's the question: Europe passes a law – cybersecurity law – and an interconnected toy is illegal in Europe. The manufacturer's probably going to change how it's made and sell that better toy everywhere, so we win. Right?

Stewart Baker: [00:51:50] Ah, yes.

Bruce Schneier: [00:51:50] I would like to see some of these international laws have positive spillover effects. And I think they're more likely in security and safety than in privacy because if Company X... Refrigerator manufacturers are going to spend the money to design a more secure refrigerator for European markets. I think they're more likely to sell it in the US and tout it as a feature because it's free. They did it already. It's easier to make a bunch more than to make a separate design.

Stewart Baker: [00:52:17] So there's a lot. It's a great book. It is thoughtful about all of these issues. And that's not always the case in this area. Let me ask about one thing that you don't embrace the way I do, which is you know when you talk about terrorism, as you have, you kind of mock the US government for trying to get to zero acts of terrorism, risk of terrorism and have encouraged a much more risk management, criminal law approach. Why isn't that the case here too? Why aren't we bringing to bear the tools of criminal law and design the technology so we can find the people who are carrying out these attacks and punish them, whether they're nation states or individuals? It just seems to me there we are moving in the direction the technology wants to go anyway. That is to say, you know yes, our security sucks, but so do the people who are attacking us. And we can identify them as the last ten years have shown. We've gotten really good at finding the Facebook pages of the people who are launching attacks on us.

Bruce Schneier: [00:53:42] So there's a bunch there. I think law enforcement is part of both solutions. I spent a bunch of time and how to make the FBI smarter in this world. And I think that we have to invest a lot of money in making the FBI able to solve crimes in this age. And I think we're skimping on that.

Stewart Baker: [00:53:59] How about cutting down on anonymity and enabling attribution, making that part of the design?

Bruce Schneier: [00:54:05] I think that's dangerous. I think there's a lot of value to anonymity. I wrote that in my previous book on the social value of anonymity and privacy. I think we'd be giving up a lot as society to do that, so I want to solve these problems without that. I think we'll have a more robust better society.

Stewart Baker: [00:54:23] You think we can?

Bruce Schneier: [00:54:23] I don't know. The jury's out. In my darker days, I wonder if the whole freedom bit was kind of a neat blip in history when a lone individual couldn't do a catastrophic amount of damage, and I hope we can get beyond this. A wildcard here is AI, which I think will benefit defense more than offense by a lot.

Stewart Baker: [00:54:50] Really?

Bruce Schneier: [00:54:51] I actually do. But let's talk about attribution. I think there's a split in attribution, that we the United States are good at it at the intelligence level. You know when North Korea attacks us, we can figure out who it is. When Russia does, we can figure out who it is. When the FBI has to do attribution for crime, it's a lot harder.

Stewart Baker: [00:55:13] It's harder because they have to use tools that they have to blow in order to...

Bruce Schneier: [00:55:18] It's not just that. They don't have that broad level of "we're watching everything" that the NSA can do and the FBI can't.

Stewart Baker: [00:55:26] Right. The ACLU is not bringing lawsuits on behalf of Vladimir Putin to say his rights have been violated.

Bruce Schneier: [00:55:33] That's right. So attribution I think is going to be part of it, but I don't think we can rely on it. There's a democratization of attack which I think is important here. Terrorism almost never happens. It is incredibly rare. But conventional crime happens all the time. And as conventional crime moves into cyberspace and you get ransomware against cars at speed because it's profitable or against medical devices that are implanted in your body, that is a different level of crime. And behind these physically capable computers are, you're right, physically capable attackers at distance, and the scale changes. And that's where I think we have to start rethinking things.

Stewart Baker: [00:56:18] So my guess is we aren't going to get a choice about this because China is going to create a market for fully attributed IT because that's what the government wants and the companies there are happy to provide it. And it's actually in some cases easier to do it that way than to build in anonymity. And just like Linux today, it's going to be available for everybody so cheaply that the argument "well we shouldn't do that" is just going to fall on deaf ears.

Bruce Schneier: [00:56:48] The argument will be it's full of Chinese backdoors and you shouldn't do it.

Stewart Baker: [00:56:52] That is true, and so that leads to a truly splintered Internet.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Bruce Schneier: [00:56:57] And that I think would be a shame too, but it's often hard to see another option as countries are moving in such different directions.

Stewart Baker: [00:57:04] So Bruce, we are out of time, but is there something that we didn't cover that we ought to cover? And then I'm going to ask you for any events that you've got coming up that people who want to see and hear more from you can they attend?

Bruce Schneier: [00:57:20] We didn't cover so many things that are in the book that everyone must immediately buy and read.

Stewart Baker: [00:57:25] It's great, though. There's something new on every third page, maybe every second page. It was a lot of fun to walk through this because at every point you stop and say, "Actually, there's three issues here. One. Two. Three." That's two pages, and you're on to the next topic and three more issues that people have to struggle with. So it does reward slow reading.

Bruce Schneier: [00:57:49] And I'm doing events this week and next week in New York, Boston, and Washington, DC. I'd list them all, but easier is to go to Schneier.com and look at events and they're all listed there. So people can come see me there. This has been probably the most agreeable interview I've ever had in my life with Stewart Baker, which is phenomenal.

Stewart Baker: [00:58:09] [Laughter] It's true! It's true!

Bruce Schneier: [00:58:12] So as the world gets scarier, he and I agree more. I don't know if that's a good thing or not, but it seems to be true.

Stewart Baker: [00:58:18] Well it may just reflect that I have an eye for scary things, and I've been seeing them for a while. But that's Bruce Schneier, author of *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. It's now available on Amazon. I got it down on Kindle. I've got a paperback here. Great book. Worth reading.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

And I wanted to say we've got some great people coming in for interviews. Michael Chertoff, also an author now, is going to be talking about his book. Peter Singer has a new book. He's the guy who famously had the Chinese use conventional arms to take over Hawaii at one point. Suzanne Schwartz is the associate director for science and strategic partners at the FDA, and we'll be asking her how the FDA's security culture matches with the Internet of Things. And the general counsel GCHQ [UK Government Communications Headquarters] will also be joining us. I'm not allowed to use his name, but...

Bruce Schneier: [00:59:30] That just sounds totally spooky.

Stewart Baker: [00:59:32] It does, doesn't it? It's very cool. Okay. And for those of you who are looking for more Stewart Baker, I'm going to be appearing on This Week in Law, which is part of the TWiT network, I think the next version of that, with Denise Howell. If you've got other guest interviews to suggest, send them in, and we will award you one of our highly coveted Cyberlaw Podcast mugs, which we'll be giving to Bruce in a minute. Send comments and suggestions to CyberlawPodcast@Steptoe.com. Send me notes and comments on Twitter and LinkedIn. Not because I'm mad at Facebook, but just because they have made it harder to post, there I'm posting less on Facebook. And wherever you see us, rate us and leave a review. iTunes, Google Play, Stitcher, Pocketcasts. That's how people find us. So this has been The Cyberlaw Podcast. Please join us next week as we once again provide insights into the latest events in technology, security, privacy, and government.