Steptoe

The Cyberlaw Podcast Episode 224: Do we need an international “potluck” cyber coalition?

Stewart Baker: [00:00:03] Welcome to Episode 224 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking technology, security, privacy, and government. We've got a great lineup today. We're going to do our interview with Duncan Hollis, who teaches law at Temple Law School and knows a lot about international and cyberlaw because he was formerly at the Department of State and Steptoe & Johnson. Duncan, do you actually have to work at Steptoe & Johnson to do international cyberlaw?

Duncan Hollis: [00:00:35] I mean, I think so. I mean, I don't know about causation, but there's certainly correlation, right, between folks that spend time at Steptoe and then end up in this field.

Stewart Baker: [00:00:43] I agree. Alright. And if you didn't start at Steptoe like Brian Egan didn't, you have to come back to Steptoe. Alright. We've also got Maury Shenk, who was formerly the managing partner at our London office and now an adviser on European technology and cybersecurity issues. Maury, welcome.

Maury Shenk: [00:01:06] Good to be here, Stewart.

Stewart Baker: [00:01:07] OK, and to talk about the Securities and Exchange Commission, we've got Chris Conte, who was formerly with the SEC's Division of Enforcement, now partner in our Washington office. Chris, welcome.

Chris Conte: [00:01:20] Great. Glad to be here.

Stewart Baker: [00:01:21] And Jamil Jaffer, well-known to our audience as the founder of the National Security Institute and professor at George Mason University. Jamil, great to have you.

Jamil Jaffer: [00:01:33] Thanks for being here.

Stewart Baker: [00:01:35] And making a guest appearance, a summer associate from Steptoe's Washington office, Laura Hillsman, who is going to take on the first topic of the podcast. But first, I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. I should note before I jump into the News Roundup that in a new experiment I tweeted out all of the stories that I thought we'd cover today at the end of last week to see what kind of interest there was, and I'll probably do that again in the future a few times. Maybe I'll put it on Facebook and LinkedIn as well. And if you've got comments, if you think a particular story is really important or stupid or there's something that you'd like us to talk about, just respond on social media, and we'll try to fold it into the discussion as we go forward. Why don't we jump right in to the new California privacy law? Very extensive and you'd think it was a big step forward, a big victory for privacy campaigners, but that may not be quite true. Laura, how did this come about?

Laura Hillsman: [00:03:06] So last Thursday, on June 28, California passed a new privacy law. And this was actually passed in exchange for getting rid of a ballot initiative presented by California citizens that was trying to improve California's privacy measures. So this law gives Californians the right to know what data is collected and who it's shared with, and then they can opt out or ask for some information to be deleted. There are also some remedies in the event of a data breach, so they could sue for that. However, this is noteworthy predominantly because it's one of the first privacy protection laws we've been seeing. GDPR, as many of you may be aware, came out somewhat recently, and that's a huge privacy protection law over in Europe. However, in the United States we've tended to focus more on data breach protection, so this is really noteworthy in that case.

Stewart Baker: [00:03:56] This is, in some respects, this is just California saying "me too" to GDPR in a lot of ways. That's what the law does. It takes GDPR, translates it into Left Coast language and adopts it.

Laura Hillsman: [00:04:13] Yeah, that's a good way of characterizing it. However, one important thing to note with this as well is that because the California legislature passed this instead of it being the ballot measure, this will be open for amendment before it takes effect in 2020. So there's a lot of wiggle room to see exactly how robust these privacy measures are going to be.

Stewart Baker: [00:04:32] That's what I was hinting at with the intro. My sense is this was adopted by the legislature precisely to head off the initiative so that they could change it before 2020 if they were lobbied hard enough by Silicon Valley, which they couldn't do with an initiative but they can do with legislation of their own. So I'm not sure we're done fighting about what California's privacy laws should be.

Laura Hillsman: [00:05:03] Yeah, I think that's absolutely true. We'll have to see. Even looking at the differences between the ballot initiative and the law that was passed, there already's some broadening out. So it'll be interesting to see what the legislature does before it comes into effect.

Stewart Baker: [00:05:17] Alright, well we will cover it for sure. Thanks, Laura Hillsman. Did a great job. Fell right on that grenade. Speaking of grenades, the SEC is rolling them out for people who have traded in advance of — in the wake of — a cyber breach but before it's been announced. This is the second insider trading conviction they've gotten, isn't it?

Chris Conte: [00:05:48] Well, it's the second one that they've brought. They're doing it with the US attorney's office in the Northern District of Atlanta. So the consequences here are even more significant given the criminal footprint that exists in the two cases they've brought so far. I was going to start out by mentioning that you know back in November there was a special committee that took a look at four senior executives and concluded that those four senior executives had not engaged in insider trading for a

number of reasons: both that they didn't have knowledge they had complied with company policies and procedures and that the trades comported with company policy. So the first case that was brought was brought back in March of 2018 where there was an individual who was a former chief information officer who exercised all of his vested options after coming into possession of information from which he was able to deduce that Equifax had been breached and not some customer that they had sort of said...

Stewart Baker: [00:07:02] I'm guessing he deduced that his time at the company was really short.

Chris Conte: [00:07:08] Well whatever his thought process was, he exercised all of his vested options and netted proceeds of about a million dollars, which because it was a losses-avoided case ended up being $117,000. But with last week's action it involves a software engineer. Again both charged criminally and by the SEC, and there again the allegations were that he had received confidential information while creating a website for the consumers that were impacted by the data breach. Again this individual was able — who was working on the website — was able to figure out that in fact the unnamed potential client was in fact Equifax.

Stewart Baker: [00:07:54] So you know to give him you know some credit here. They didn't tell him that. He figured it out. And I wouldn't be surprised if he said, "Wait, if you're not gonna tell me, it's not inside information. I just figured this out from the internals of the assignment." Now, in fact, that's still insider trading because he wouldn't have that information if he hadn't been working there. But I can see why he might have been — fallen prey to the illusion that this wasn't insider trading.

Chris Conte: [00:08:28] Yeah. He has settled with the SEC but is going to be litigating the case with the criminal authorities. Perhaps the arguments do very much involve his criminal intent and awareness.

Stewart Baker: [00:08:44] So here's what I think he really should go to jail for. That website itself was hackable. The website you were supposed to go to say, "Have I been hacked, and what do I do to protect my identity?" "Please put your information in here,

and we'll tell you." It was subject to cross-site scripting. And if he designed that website, he probably was responsible for half of the damage in reputation that Equifax suffered, plus all the harms that occurred to people who entered their data, if there were any. I don't know if the site was actually hacked or just that everybody discovered the flaw. So he doesn't look so good. If you realize just how bad his code was.

Chris Conte: [00:09:31] Right. Well, it's also the case that in terms of how he went about doing his trading. You know these are the trades that he engaged in are the kinds of things that typically bring everybody out of the woodwork. And so he did options...

Stewart Baker: [00:09:45] Options that were the own company's stock. You know, duh!

Chris Conte: [00:09:48] Options out of the money. Two week expiration. He traded in his wife's account where he could have done it in his own account with money that was available. Contrary to company policy...

Stewart Baker: [00:10:01] His argument that there was no criminal intent is gonna be a tough one.

Chris Conte: [00:10:06] It's gonna be tough. You know he made $75,000 on a $2,000 investment. Look in terms of sort of lessons... Look, the SEC has been out there for a long time. It issued guidance earlier this year to tell public companies and individuals you've got to put controls in place around the potential for insider trading. You've gotta restrict trading if you're aware of material breaches. And so you know this is the kind of thing that we'll continue to see. But the onus is on companies to put into place what they need to do to prevent this from happening as best they can.

Stewart Baker: [00:10:45] So it would have been better off to tell him and then to tell him that by the way this is inside information and you absolutely have to treat it as such. Ok. Lots of action between the president and China, particularly ZTE, but also policy on Chinese investments. Maury, what happened last week?

Maury Shenk: [00:11:12] Well, like the president did in North Korea — or there are starting to be signs that like on North Korea beyond the trade war bluster, there are some more traditional nuanced solutions being pursued. So ZTE which is a big Chinese equipment manufacturer was — well people would think maybe they'd be put out of business by Commerce Department sanctions not allowing them to buy from US suppliers — was offered relief by the president, and the Senate came back and tried to overturn that relief. The president said, "No, that's not right. Let us be flexible."

Stewart Baker: [00:11:53] So that was a statement of administrative policy which is this the standard expression before a bill is adopted of what the position of the administration is on provisions. What I thought was interesting is he used the language, "The president objects strongly." I didn't see a veto message or even the president's advisers will recommend a veto. There is none of that in the context of a bill that is almost never vetoed, which means that this is a strong objection but maybe not a nuclear one.

Maury Shenk: [00:12:38] No, I think that's right. I mean two reasons for that. As you say the [National] Defense Authorization Act is not something the president would veto lightly because there's a lot hanging on it. And second I think Trump is playing a game of shifting positions which is clearly his negotiating strategy. It may be more important to him to get the position out there than actually make this particular position fit.

Stewart Baker: [00:13:03] Ok, so he may be saying to the Chinese, "Look I'm fighting to preserve this deal, but if I can't preserve the deal, I can't preserve the deal." And at the same time he has said — interestingly it's in the same bill, the National Defense Authorization Act — that he's going to wait for the investment review changes that Congress is making and not try to make them as a matter of executive order.

Maury Shenk: [00:13:34] Yeah, that was the other big development that Steven Mnuchin, the Treasury Secretary, seems to have won the battle of using reformed CFIUS process to deal with Chinese investment rather than sanctions along the lines that have been used for imports. And again suggests some flexibility in the US's position.

Stewart Baker: [00:13:59] Yep. So David Aitel, responding to my tweet of this issue said, "What does this mean more broadly? For example, for Kaspersky is there is there a broader issue here, and do we have a hint about how it's going to be addressed?"

Maury Shenk: [00:14:17] Well, you know predictability is not this administration's strong suit. But it — I mean the administration seems to be developing a track record of taking big aggressive positions and then doing a deal. Could that happen with Kaspersky? You know, I don't know. I mean the Russian situation is obviously caught up in a lot of top political issues, notably newer than that [unintelligible]. And Kaspersky is — you know there was a lot of damaging evidence there. So I don't think it was — I mean there was damaging evidence against ZTE as well. But I don't think that a deal on Kaspersky is as likely as a deal on ZTE, including because Kaspersky is a much smaller company. I mean Russia doesn't care about Kaspersky like China cares about ZTE.

Stewart Baker: [00:15:12] Fair enough. OK. We've got a whole bunch of stories for our Lightning Round. Jamil, USA Freedom Act was designed to take a bunch of metadata out of the hands of the National Security Agency and leave it with the phone companies that collect metadata about our calls. And now it looks as though that's not working out quite as well as everyone had thought.

Jamil Jaffer: [00:15:42] Well, I think we always knew there were going to be challenges in getting the records back and forth from the providers: how long they'd store them for and how we got them and what we do with them once we had them. What it looks like here is that NSA on its own identified some technical irregularities in the data they were receiving from companies. They were authorized to get the data. They got it, they looked at it, and it didn't look right. They determined that apparently they got some records they weren't supposed to get. They then consulted with the Department of Justice. The Office of Director of National Intelligence decided they couldn't figure out how to segregate the records they weren't supposed to get from the records they were supposed to get, and as a result they decided in an amazing turn to delete all the records. So you know this just goes to show they had gotten some valid data and they had gotten some invalid data. Because they couldn't segregate it, they threw it all away.

They apparently have fixed the problem and won't get the unauthorized data going forward. Doesn't change the fact though that what was designed to be a terrorist threat early warning system just had a bunch of data dumped out the back door because this having the phone company keep the records and get it over to the NSA in the right fashion just hasn't worked out properly.

Stewart Baker: [00:16:54] Yeah. So it's not as though they dumped every piece of data available to be searched. These are the results of them asking for finding say 30 or 40 — which is what these searches ran in the past — 30 or 40 suspicious numbers asking who called that number, and then say, "Who called the people? Who called that number?" And what they got was data about who called that number that might have been over-inclusive. And then of course they asked for data about who called the people who called that number and got a lot of over-inclusive data. But it's still the results of 30 or 40 searches a year, right?

Jamil Jaffer: [00:17:38] Well, I mean it's hard to know, right? For all we know the number has gone up or gone down. We just don't know what the number of searches is. At least it wasn't disclosed in this press release. But I think what we can say is back in the era when NSA held the data and only pulled at the right cell, it would only get the data it was looking for because it just pulled the thread, get the numbers that were connected to the number it sought, and that was it. Yes, they maintained the data, but they weren't looking at it in that sense. Now you go to the providers. The providers do what they're going to do, and if there's a problem, they dump a whole bunch more data in NSA's hands. And now it's looking at data that it shouldn't have. This is a good example of a scenario where you know Congress takes action to protect privacy may have actually made things worse for privacy when it came to this particular scenario. Luckily though they have solved the problem. NSA caught itself. They did the right thing: told the Justice Department, told the court, have gotten rid of the data, and are now collecting in a proper way and working with the providers in a way that doesn't get them this over-collection of data. A good story I think for government oversight but a good example of where sometimes private laws can get you into more privacy trouble than you might have thought initially.

Stewart Baker: [00:18:41] Yeah, my guess is the people who created this problem in Congress will rush to blame NSA for it. Ok. Well, reality has won, and Reality Winner has taken what looks like a pretty good plea deal: 63 months in jail for releasing highly classified documents. And you know I'm not sure — she's kind of a sad sack, and this is probably about right — but it sounds like a pretty good deal compared to some of the other sentences that people have gotten for releasing classified information. Speaking of sad sacks, there's a story out about how much sharing has gone on over the last two years of malware and other signature information in the two years since the Cybersecurity Information Sharing Act was passed with a bunch of liability incentives to encourage sharing. It turns out that there are only six private sector entities that are sharing that kind of information on a regular basis with the government through DHS. And that's being covered as a pretty poor showing considering how much effort there was to encourage private sector sharing. I don't know. Jamil, how do you see that?

Jamil Jaffer: [00:20:19] Well, you know obviously the CISA bill is a derivative bill that was passed in 2015. We had originally done this original bill called CISPA in the House Intelligence Committee. Some of the differences between the two bills I think that may be relevant to why people are sharing are: the more limited regulatory posture in CISPA that was eliminated here. You can still regulate based on this data in a large sense — you regulate the whole industry. You can't regulate individual entities, but you can regulate whole industries. That raises concerns with companies who don't necessarily want to share. The sharing is required to be with DHS. You can't share with anybody else in the first instance. It's true that DHS still has to push it out. There are companies as we know who have had concerns about doing that. There are a variety of other provisions in here — I've got a whole law review article on it if anybody wants to look at we can get out to folks — that it's just why you might think this law was a good step in the right direction but could have done more with. And there's actually legislation in the House Small Business committee that looks to solve some of these problems at least for small businesses. So you know more to be done there. But then there's a larger issue, obviously. You know I think that we heard Jeanette Manfra, the Assistant Secretary for Cyber at DHS, talking about — she understands some of the challenges that AIS, the automated indicator sharing system has. They're working to fix those. They've got a good team on cyber at DHS now with Kirstjen Nielsen at the top, Chris

Krebs as the undersecretary, Jeannette Manfra there as the assistant secretary, so I think they're committed to trying to address some of these issues. But you know it is a challenge. So it's not surprising that on the sort of input end companies aren't ready to share as much as they might. On the flip side you also see you know the information coming out of DHS, out of AIS has been not as useful as people had hoped. The same was true [unintelligible], so it's not like it's just a DHS-only problem. But that being said, you've really got to figure out how to get companies incentivized to share. There are a lot of ways we can think about to do that. But there are companies today that want to share both with one another and the government. I happen to work with a cybersecurity company that does some work in that space. So you know I think there are opportunities out there. It's just really a matter of: give a legal structure in place but then also keep the right incentives in place to encourage people to do this and clear out the roadblocks. And we've gotten three-quarters of the way there. There's still another 25% to go, and so we'll see what happens going forward.

Stewart Baker: [00:22:34] So my guess is that we only have half the story here. The CISA encouraged sharing. It didn't specifically encourage sharing with the government, or at least its liability protections weren't limited to government sharing. I'm willing to bet that there's a lot more sharing going on in the private sector — private sector to private sector — and the reason they don't share with the government is they don't know what will happen and they don't know how much value they're going to get out of it. So they're being conservative which is certainly my experience with GCs of big companies that have that data.

Jamil Jaffer: [00:23:11] You know, Stewart, you're exactly right. I think that CISA has incentivized and actually has promoted a lot more sharing in industry. Part of the challenge that we've always had with government is government really explaining to industry why there should be value in this. And the real trade-for-value here is for industry to understand and believe that the government will take the information they're given, they'll use it to go out in the foreign space, identify threats, identify new threats they didn't know about before, and then share that back to industry. And government has been talking more recently about doing that. But actually making that real hasn't happened. And so I really think in part the onus is on the government to really say, "OK,

we're ready to share with you some of the crown jewels to show you what we're seeing out there in foreign space. You can better defend yourself going forward." There are ways to do this. The government hasn't quite gotten over its own hurdles about sharing that with industry on a large scale at speed and at you know in real time.

Stewart Baker: [00:24:00] Alright. Quick question: Is the story in *The Intercept* where they point to a whole bunch of big windowless high-rises in major cities — which house a bunch of Internet routing structures and also are alleged to be where NSA pulls off certain kinds of lawfully authorized intercepts — is there any reason to wade through that endless story, Jamil?

Jamil Jaffer: [00:24:37] I mean the government has made clear that there are lawful authorities that it utilizes to conduct surveillance in the United States against foreigners located overseas. It's called Section 702. We've had three debates over it. It's been reauthorized every time, sometimes minor changes. There's a variety of other pieces of legislation that have authorized government surveillance collection. So the methods by which the government does that, the specific facilities that may do that, the ways in which it carries it out. I mean it strikes me as you know stuff that goes beyond sort of — maybe there's a prurient interest of some folks who read *The Intercept* and that's good information. But at the end of the day the government's been very clear. Yeah we collect foreign intelligence on American soil through court orders directed to telecommunications companies both on the upstream as they say, on the backbone, and at the end point or at providers. The government's been public about that since the Snowden leaks. There have been lots officially revealed by the government where specifically it takes place and how it's done. You know I think the government likes to maintain that a secret, so you know I mean if *The Intercept* wants to [unintelligible] what they think the answers are, then I guess, I suppose, they can do that and they can use classified information to do that. It is unfortunate, inappropriate if in fact that's what they're doing. If in fact this is true. But you know at the end of the day — if it's a question about law and policy, I think the law and policy have been debated and *The Intercept* lost.

Stewart Baker: [00:26:02] Yeah, and meanwhile they're going to cover 83 of the last two surveillance scandals. OK. Last point. Maury, the Pew Foundation came out with a study of Americans' attitudes toward "Big Social Media," and I was kind of surprised not at the views, which I share, but at how many people share them. Seventy-two percent of Americans think that the "Big Social Media" censors views that they find objectionable, and that turns out to be almost all people. Even Democrats think social media censors the Right, not the Left. And something like 60% of Republicans thought that social media needed more regulation. These are surprising numbers and scary if you live in Silicon Valley.

Maury Shenk: [00:27:04] Yeah I was trying to think — well thinking about the Republican points of view. I was trying to think what maxim applies best here. Whether you can't have your cake and eat it too, or if you want to listen to the music, you gotta pay the piper. The evidence seems to suggest that right-wing voters are more easily swayed with social media. But I think it's undeniable that all media and media companies tend to be left-leaning, and there probably is some censorship out there. You gotta decide on which side of the fence you sit. I, like you, come down on the free-speech side of the fence.

Stewart Baker: [00:27:39] Yeah. Well, we'll see. I will say I tend to think that those studies that show that the people on the Right are more swayed by social media were designed by people who think that people on the Right are stupid and were eager to prove it. But I could be wrong. Alright, let's move on to our interview with Duncan Hollis because it combines two things that I have a wonk-ish delight in: cybersecurity, which everybody listens to this podcast probably has, and the Proliferation Security Initiative, which probably only four people who listen to this podcast know something about. Duncan and Matt Waxman have written a paper that says combining those two is exactly what we should be doing. And I've thought, Duncan, can you give us the elevator speech for your paper?

Duncan Hollis: [00:28:36] Sure. I think to begin with we're kind of — Matt and I started on this idea that you know we're in this world now where the global efforts to regulate state behavior in cyberspace are either failing or at risk of being led by the likes of

Russia and China, and so we were kind of looking at what would be a good plurilateral method of cooperation among states and that's where the PSI think set up about 15 years ago now stands out. It's a relatively unique architecture for cooperation that we think could benefit cybersecurity. And I should be clear at the outset although the Proliferation Security Initiative (PSI) focuses on nonproliferation, Matt's and my interest in PSI is not in treating cybersecurity like cyberweapons or like nuclear nonproliferation. Our interest was in the architecture where you basically have like-minded states via political commitment agreeing to cooperate not necessarily collectively but through coordinated actions with people or states of different capacities. And we were kind of just interested in thinking about how that architecture has certain features that might work for cybersecurity as it exists today particularly with all the problems at a global level.

Stewart Baker: [00:29:45] So it's potluck policymaking in a sense. People bring what they have to the table and say, "This this much I'm willing to put into the effort to make a meal." And when you're done you actually you know you do have a fair amount of nourishment.

Duncan Hollis: [00:30:03] I think that's right. I mean if I can continue that. I mean it's the idea that you might have more than one chef in the kitchen, and some chefs are going to actually be really good at certain things right. Somebody might have some great knife skills. Somebody might be really good at doing the dishes. And I think one of the things that PSI focused on was having almost tiered participation. So we can talk a little bit more about what PSI is, but one of the core features of it was that there were a group of states, appropriately known as the Core Group, those with the capacity and information on nonproliferation risks and the capacity to do interdiction and then a group of a kind of supporting cast, if you will, that would on a case-by-case basis lend either assistance or just their voice of "Yes we support this activity and this behavior." And you know you could think about that in terms of parallels in terms of what states — and I guess industry and even individual users — can bring to a table when you're dealing with cybersecurity threats and so that you know it's designed as you say kind of to be a little bit potluck. Bring what you can to the table, and as long as everybody contributes hopefully the end product is a good one.

Stewart Baker: [00:31:11] So I don't think we should go too far further down the PSI road without noting who the architect of this was. It was John Bolton, who's back in the news again. It does lead me to ask: is there like a position for international law professor in residence at the National Security Council that you might be — you or Matt is hoping to get?

Duncan Hollis: [00:31:39] Well, I can't speak for Matt. I think I'll say I'm pretty happy as a law professor in the private sector and doing some consulting and the like. It did not escape our — we actually started working, I should be clear, on this paper more than a year ago. But yes it did not escape our thinking that this was in the current White House the sort of thing — and in the current geopolitical environment where you know some things the US is going to float others are going to say “absolutely not” to, and similarly these things that are getting floated in Europe or by other stakeholders are also going to meet resistance from the US — was this this model might be something where you could hopefully find some common ground. And that you know I certainly think Mr. Bolton has experience with PSI. He did play a critical role in it, and so he may know as well as anyone what sort of legs it might have on global cybersecurity.

Stewart Baker: [00:32:32] Let me — I actually wrote about this when I was trying to figure out what Bolton might be like as national security adviser, and everybody saying, "Oh my God, you know get your children into a fallout shelter right away." And I said you know he's very critical of a lot of international policymaking for good reason. There are a lot of flaws with the way we made policy, but his critique of nonproliferation was it's not really enforceable, people drag us into endless negotiations over you know how much we're going to bribe the less-developed countries with in terms of funds and expertise, we've got all these people who want the whole enterprise to fail who are dragged along, and then — I don't know if he made this objection, but I do — any organization you create that has a secretariat, immediately the secretariat defines the United States as its natural enemy. And so it too tries to get in the way of US initiatives or at least tweak them and slow them down and demonstrate its value to all the other members by making sure that they are not pushed too hard by the US into a particular direction. So if you can come up with something informal and fast moving and agile and without a

secretariat, you have a chance to make policy much more effective and much more likely to be something that the US government supports.

Duncan Hollis: [00:34:14] I think I might disagree with you on some of the means but probably agree with you in the end, right? I, as a professor of international law, you'll not be surprised that I'm probably not as negative as Mr. Bolton on the nonproliferation legal regime. You know I tend to think of it kind of like speed limits. It doesn't stop speeding, but you know it may have put some brakes on some things that might have otherwise happened. That said, I think what Matt Waxman and I were thinking about with this piece was again this idea that what can you do that has low entry costs, and that's one of the features I think that the PSI has and that you could think about as a model for cybersecurity is you know it doesn't — PSI is not based on a treaty. It's based on this statement of interdiction principles which is a couple-of-pages document that's like a political commitment. Nobody expects that you know states who sign on to the statement of interdiction principles need to go through their treaty-making process. They don't need to change their national laws. Again you're kind of taking the states as you find them, so states can join pretty easily, and it can be put together — and it was put together pretty easily. You started the — PSI I think started with 11 states in 2003, and today it's about 105 states have signed onto those interdiction principles. And so I do think that this kind of voluntary, kind of low entry cost model without a secretariat, without having to get into some organization that's going to require budgetary support is going to be more feasible at least in terms of where we are right now.

Stewart Baker: [00:35:40] So let's think about what this would mean in cybersecurity. Some examples. So when you're talking about getting everybody to agree on some principles — or at least not everybody, you can push aside people that you think will never agree and then try to get others to agree — agreeing with the Europeans and perhaps other states — India, Brazil — that certain kinds of cyberespionage or cyberattacks are inappropriate that we ought to cooperate in stopping denial of service attacks. And setting up rapid reaction systems for taking down compromised DDoS-ing security cameras, for example. That's something that could be done, and we could try it out to see how it works. And if it doesn't work, well the first time recommend that people change their laws to allow them to move more quickly against compromised machines

that are attacking other people. And you use the weight of the economies that are in the boat to lean on people who haven't gotten in yet and to say, “You need to change your law too, Thailand or Vietnam, because everybody else is doing it.” All those are PSI-like moves in cybersecurity, right?

Duncan Hollis: [00:37:13] Yeah, I think they are. I think if you go back to PSI, I think one of the original motivations for it was there was this incident in 2002 that this North Korean freighter — I think was So San it was called — you know it gets detained by Spanish Marines. They find 15 Scud missiles on board. And you know I wouldn't work on it, but I was at the State Department at the time. And you know there's a lot of anxiety as you know. Could the vessel be held, or did you have to let it proceed on to Yemen — I think it was where it was destined? And you know the eventually the decision was under the existing international law rules the vessel was allowed freedom on the high seas, vessel freedom of navigation, vessel was allowed to continue on to its destination. And I think that was the impetus for PSI, and it certainly was this idea that well let's try out and maybe think about whether we could get to new rules. I think one of the ironies of PSI was that it didn't actually change you know international maritime law or international aviation law. What I think happened was as states began to cooperate in this kind of ad hoc coalition, voluntary participation is they found that there was actually a lot of strength in their existing national laws in the ability that if your national law didn't actually provide authority maybe just by your consent you know the executive of certain countries could say, "Yeah we're willing to allow your customs officials to do an investigation in our territory, or we'll do...." They did a number of I think we call them ship rider agreements where certain countries would allow other countries' forces onto their ships, and they'd do these joint operations together all by consent. And so again Matt Waxman and I were thinking you know there's a lot of utility for that given the nature of the cybersecurity threat problem which is inherently global. You know the jurisdictional limits as strong as US law enforcement might be within US territory and their efforts to act extra-territorially. You know there are plenty instances where you need cooperation from other states — either their consent to operate in their territory or getting them to put their own national laws to work — and you can move forward on that. And as you said as states realize hey you know our national law is not as strong as

it needs to be you could see a process where through that national-level measures you could see changes that improve this.

Stewart Baker: [00:39:30] Yeah, and there were probably a dozen flag of convenience countries who were not the strongest economically or militarily or any other way. This was an important source of income for them. And the US and the other members were able to lean on them to say, "Yeah, sure you want a board my ships? Go right ahead." Well, that solved the problem without ever having to change the freedom of navigation principles.

Duncan Hollis: [00:40:02] Right. I think that's right. And I mean we should also emphasize that you know the PSI is not universal. It's 105 states. There's some you know 80 plus states that are not in it. And you know I'd imagine you might see something similar if this were tried out in cybersecurity. You know Russia for example objects to the Budapest Cybercrime Convention precisely because it thinks it's too intrusive in terms of the pre-commitments states make to allow law enforcement investigations in the territory of state parties. So you know I do think that this is not going to be a global solution. What we were thinking about in this paper was in an imperfect world what could a plurilateral solution [be], right? Could you get the US, the Europeans, the Singapores, Japans, some of the OAS states to coalesce around a certain set of principles and then act on them. I think that's the other thing that we were really interested in was you know the PSI is not a talk shop because you said it doesn't have a secretariat and it doesn't have you know global meetings that are you know with observers and civil society participation. It just does stuff, or it's you know stuff is done in its name. And we both I think thought you know the time is to try and do — not to undermine the talking that's been going on, there's a utility to it — but we might also want to see some more experimentation, some more action, as it were.

Stewart Baker: [00:41:25] Still when you write the next paper, you should say what does the Financial Action Task Force (FATF) tell us about possible cybersecurity solutions because that's a similar kind of potluck, informal, agile international policymaking effort led by the United States that has had enormous impact. So I'm looking forward to the next installment of your international policy guide to cybersecurity.

Duncan Hollis: [00:41:56] We've been working our way through all the analogies over the years, Stewart. So I think right the next one is the FATF paper, and then we'll keep going. I mean look all analogies have limits. But I do think that this kind of a sense of a political commitment with kind of tiered participation, like-minded, and as you point out I think one of the strengths of the FATF has been that it built out norms. I'm not as sure that PSI did. I think PSI was much more about you know the cooperation and getting the consent and leveraging national laws. Whereas I think FATF is most known for getting a group of like-minded states to cooperate around their 40-whatever-plus recommendations of best practices that states should take. And certainly there's nothing inconsistent with that model for what Matt and I have been writing about.

Stewart Baker: [00:42:44] So before you go I do want to ask: Do you have any public events coming up where you're going to be talking about this that the listeners might want to go to?

Duncan Hollis: [00:42:53] So public events wise, not so much. I am a member of the OAS juridical committee — it's like the equivalent of the International Law Commission at the UN. This is the juridical committee for the Organization of American States, and there's 11 of us. And one of the things we've been trying to think about is the cybersecurity problem, and the OAS has already done a tremendous amount in terms of building out cybersecurity strategies and helping countries do that sort of work. But one of the things we're interested in is getting more transparency on what the norms are or what the international law is and what do states you know understand the rules are. So you know a few years ago Harold Koh — more recently Brian Egan — you know as State Department Legal Adviser, kind of came out with these public statements articulating you know here's what we think. You know use of force means for cybersecurity or here's what we think the international humanitarian law or non-intervention means. And so one of the things I've been working with the committee on is whether we could try and get other OAS member states to kind of come forward with similar statements again to kind of try and build out what the rules of the road here are because I think if there's a difference between say the PSI model and what we've been writing about is you know the PSI, you and I might disagree on the utility of the rules,

but there was no existential crisis. Everybody agreed. There were certain treaties, and the treaties said certain things, and you know the fight was over what they meant. Right? Like, you know how do you interpret these things? And I think in cybersecurity we do have existential fights. You know you see the fight over whether it's sovereignty a rule that states violate by their cyber operations, or not? You know the UK attorney general a few weeks ago seemed to suggest it's not a rule. The Tallinn Manual says it is. You know that's something that needs to be worked through, and so I've flagged that something that the OAS I'm hoping will work on. I should also confess that I've been working with Microsoft advising them on some of their international legal proposals particularly relating to the Digital Geneva Convention.

Stewart Baker: [00:44:50] Oh God, really? Tell them to give it up. That is the dumbest idea to make its appearance in the international policy discussions in a decade.

Duncan Hollis: [00:45:01] So I do think that the Tech Accord, which is the direct product of that, might bear fruit yet. I mean I don't know what you think. But I mean I hope you know the story of that was you know you have the speech and the proposal and then the call. Well if you're going to you know if states do something, you should do something first. And you know there is this Tech Accord out there now, and there may be other moves. I did at least say the verdict is not yet out, but I note we probably have to agree to disagree on that.

Stewart Baker: [00:45:31] Yeah well, Brad Smith you are invited to come on this program and defend this you know godforsaken idea anytime you want, so pass that on to Brad. Duncan Hollis, thank you so much. This is terrific. Thanks also to Maury Shenk, Chris Conte, Jamil Jaffer, and Laura Hillsman for joining me. This has been Episode 224 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Before we go I should say if you got guest interviews to suggest send your nomination to cyberlawpodcast@steptoe.com, and we'll send you a highly coveted Cyberlaw Podcast mug if your suggested interviewee comes on the show. Duncan, if Brad Smith comes on, I'll send you the mug. And if you want to hear your voice on this show because you've got something that only makes sense if people hear it, you can leave a message at 202-862-5785. Don't forget to look for my Twitter feed or whatever I've got on

LinkedIn or Facebook. I'm @stewartbaker on Twitter. I will be test driving some of these stories during the week to see if there's interest in particular stories. And please rate our show. Give us reviews. I promised to read the most entertaining recent reviews, but I didn't see any that were at all that entertaining, so please say something novel in the iTunes review, the Google Play review, whatever your favorite podcast aggregator may be. Upcoming guest interviews: we've got Michael Hayden, who's written another book, this one about intelligence in the age of Trump. He's not a Trump fan. Bobby Chesney and Danielle Citron are going to come on and talk about deep fakes. And I want to thank the Doonesbury Sunday comics for illustrating exactly how important deep fakes will be to our modern political culture. You're going to have to go find Doonesbury from last Sunday to figure that reference out. We're trying to get Woody Hartzog from Northeastern on to talk about his book which I probably disagree with. Noah Phillips, FTC commissioner with a particular interest in privacy, is going to be coming on just before we go on our hiatus. So plenty of stuff happening just in the next month. And we hope you'll join us for those and other episodes as we once again provide insights into the latest events in technology, security, privacy, and government.