Steptoe

Episode 226: Where are all my Twitter followers?

Brian Egan: [00:00:03] Welcome to Episode 226 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Thank you for joining us. We are lawyers talking about technology, security, privacy, and government. Today I am *not* joined by Stewart Baker, who is in the wilds of the United States somewhere purporting to be off the grid, although I suspect that he's listening wherever he is. I am joined by a great panel, though. We have Matthew Heiman, who is visiting scholar at the National Security Institute at George Mason University's Antonin Scalia Law School. Previously Matthew served as a lawyer with the National Security Division at the Department of Justice. Welcome, Matthew.

Matthew Heiman: [00:00:44] Thank you. Good to be with you.

Brian Egan: [00:00:46] Also here is Jim Lewis, senior vice president of the Center for Strategic and International Studies. Welcome, Jim.

Jim Lewis: [00:00:53] Thanks. Glad to be here.

Brian Egan: [00:00:54] And we have Dr. Megan Reiss, who is a senior national security fellow at the R Street Institute, a senior editor of Lawfare, and a visiting fellow at George Mason University's Antonin Scalia's Law School's National Security Institute. Welcome, Megan.

Megan Reiss: [00:01:09] Thanks for having me back.

Brian Egan: [00:01:11] And I'm Brian Egan. I am a Steptoe partner formerly with the State Department and the National Security Council, and I'm the host of today's program. So let's get started. We've got a lot of news to cover this week, and let's start

with Friday's announcement by the Justice Department by the deputy attorney general of an indictment of, of course, the 12 Russian GRU officials for federal offenses that were tied to alleged interference with the 2016 presidential election. So according to a press release, these individuals were "engaged in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the DNC, and the Hillary Clinton campaign and released information under a couple of pseudonyms and through another entity." So Matthew, you are our resident alumnus of NSD here. This is not an indictment that's likely to lead to any prosecutions. So why does the Justice Department do something like this, and what did you find in the indictment to be particularly interesting?

Matthew Heiman: [00:02:19] So on the first part: why does the Justice Department do it? Often the reason the Justice Department is doing it is to express you know political unhappiness by the United States government with whatever bad acts are being perpetrated by foreign powers. We saw this with the PLA and the OPM hack a couple of years ago during the Obama administration, and we're seeing the same thing here. So you know no one should expect these GRU folks to turn up at a US courtroom anytime soon to start arguing their innocence. That being said, what I found interesting in the indictment is what I find interesting in so many of these hacks is: when you hear the GRU is involved you imagine all these super sophisticated cracking software and people with multiple screens in front of them, and what you find out is it's really simple. It's: send a dopey looking email that looks something like Google, get someone to be dopey enough to click on it or forward to other people in their office, and then you're off to the races. So it points out the fact that most of these major hacks, wherever they are, whoever's perpetrating them, depend on the gullibility of someone sitting in front of their computer or iPad.

Brian Egan: [00:03:32] And is there anything that can be done about this? I mean I've heard people say you know 80% of an organization knows better than to click, but it really just takes one person to click in the wrong spot.

Matthew Heiman: [00:03:44] So yeah, I mean there's always things that can be done, and I'm not a[n] IT expert, but I'm familiar enough to know that there are some pretty sophisticated screening systems that most organizations of size have. I think the question I'd be asking the Democratic Congressional Committee and the DNC is: what level of cybersecurity sophistication did their IT systems have? And I think that's the question that the RNC should be asking itself as well. I suspect that their level of sophistication lags far behind that of a multinational company that has to protect assets and profits and you know hit a number every quarter. I don't know that.

Brian Egan: [00:04:23] Right.

Matthew Heiman: [00:04:23] That's my suspicion.

Brian Egan: [00:04:24] I see. Now Jim, Stewart has weighed in on his Twitter account which is a dangerous new weapon that we're going to have to learn to cope with here on the podcast.

Jim Lewis: [00:04:33] That's okay. I don't read it.

Brian Egan: [00:04:34] Good. Perfect. So Stewart says, "In principle, no one deserves Bob Mueller and his company team more than the GRU, but neither Mueller nor DOJ get to make their own foreign policy. The Obama era PLA indictments [that Matthew mentioned] were subject to heavy interagency coordination. What about these?" I mean do you see this as having a foreign policy impact, or is this something that's appropriate to talk about in diplomatic channels?

Jim Lewis: [00:04:59] So there's general agreement in the US government — up I'd say to the three-star level — that the best thing we can do to dissuade the Russians is to punch them in the snout. Right? And so I found no one who disagrees with that. And the problem is to punch them in the snout, we need one guy to sign off on that. And that's where it's a foreign policy issue is we don't really have a Russian policy. Anyone who thinks they can look into Putin's eyes and see his soul probably needs to go and

get their eyes checked. So no, this is a foreign policy issue. We're not doing so well on it. But across the board, our Russian policy is confused.

Brian Egan: [00:05:38] Although maybe we'll hear coming out of the summit that President Trump actually turned over the extradition request as part of the meeting, and we'll see a completely different story.

Jim Lewis: [00:05:46] He said that while he loves the intelligence community, at least on even numbered days, he found Putin very persuasive, which that and a $1.50 will get you a Coke in most places.

Brian Egan: [00:06:00] Ok well, let's stay on election interference for the moment. So Matthew, last week Senators Lankford and Klobuchar had held a hearing on a bill that they've been past you know advocating for some months, the Secure Elections Act. Can you tell us more about this bill? Is this something that we need? Will it help us? And why the bipartisanship?

Matthew Heiman: [00:06:25] Well, I think, why the bipartisanship — that's a good question in this era — is because I think both parties recognize that if elections are perceived to be swayed by foreign powers, no one is going to believe that anyone — you know, in the legitimacy of the government. So it's one of the few times where Republicans and Democrats can both agree that this is bad for business. In terms of the act, you know the broad outlines of it say that it's going to streamline cybersecurity info, information security sharing among the states, it's going to provide security clearances for state election officials so that they can get at some of the intelligence we have, and it's also supposed to provide resources for states to upgrade their election equipment. Those all seem like good things. Those all seem like you know sort of table stakes given the situation we're talking about. The wrinkle in all this of course is the federal government can't control state elections because we have this thing called the Constitution that gives the states power to control elections. But we certainly can you know — talking about the federal government — enable them to better share information. It should also be noted there's sort of a dueling bill out there that's largely

supported by Democrats. I don't think any Republicans signed on, but this is Ron Wyden's bill, and Senator Wyden wants a regime where all the election machines must have a paper trail behind them and there has to be a certain amount of auditing that takes place. I will say this: if you are in the private sector providing election machinery and the Senate is holding hearings on security and two of the three biggest competitors in the space don't show up, that's not good for industry. And that's not a good way to be able to shape outcomes because what it says to the Senate is: we, the private sector, don't care about this. And it gives the Senate a green light to craft whatever solution it thinks is right, which may not be the ideal one. So not the smartest move by those folks.

Brian Egan: [00:08:25] I do think that on the issue of federalism and the principled concern in some way that seems to be one of the issues that's going on behind the curtain because the Senate considered including this in the NDAA. They were happy to include the funding part. I think some of the even information sharing and other things that could look like federal intervention in state-run elections are going to be difficult for some folks to swallow.

Matthew Heiman: [00:08:56] Yeah, and I would expect people like Mike Lee and Rand Paul to be leading the charge on "Hey, this is a state issue. The state should own this." And so that's the tension I think particularly within the Republican caucus. I'm not sure that there's a real strong feeling within the Democratic caucus around keeping things within the states. But I think that probably is a tension on the R side of the aisle.

Brian Egan: [00:09:17] Okay, well let's turn to another favorite topic of the podcast here which is the travails of ZTE in its quest to get out from under the denial order that had been issued by the Commerce Department in April and that looked like it would have meant the end of ZTE. So Megan, we've had some developments this week. On Friday, Commerce, in a Friday afternoon press release, they lifted the denial order. So what's your take on what's going on? What can we expect to happen in terms of next steps? What does this action by the Commerce Department do?

Megan Reiss: [00:09:52] So basically ZTE will be able to get back on its feet and be able to use American components for its phones and everything else pretty soon, and once they deposit $400 million into an escrow account which is basically there to assure that if they do something bad again, if they engage in sanctions violations, if they don't follow through with the requirements that they agree to, that the US can keep that money. But I think you're going to see pretty significant pushback from Congress on this, and there are three major buckets that that's coming in. There's the trade stuff: this was lifted seemingly as part of the trade negotiations between Trump and President Xi. But then there's also the sanctions violations: the folks who see this as an issue with if a company violates sanctions and then just can give a little bit more money, they'll get off the hook. That's a problem. That's a deterrence problem. And then there's the espionage issue: they've been accused of spying on behalf of the Chinese government. So you have these three big buckets that Congress is going to want to deal with. And even though ZTE may end up complying and have to pay some pretty large fines and deal with a lot of American oversight, I actually don't see this issue going away because of those other issues involved with the company.

Brian Egan: [00:11:30] Yeah, I'd just be interested in a poll of the room here on: so, as Megan said, ZTE's now agreed that if they've paid another $1 billion, to put up another $400 million in escrow, they've fired their entire board of directors and leadership, they've agreed to this intrusive monitor for ten years. To me this sounds like a pretty serious penalty. But there is a congressional and political overlay that really makes it hard to kind of look at this only on the merits. And just curious what your thoughts are. Is this a real penalty? Is this something that Congress should be concerned about?

Jim Lewis: [00:12:06] Oh Congress is deeply confused on this, and they have this strange notion that if they can sacrifice ZTE that will somehow make us less vulnerable to Chinese spying. Wow. These people... That's like the Flat Earth Society. Second, the Chinese government is not going to let ZTE go under. What they'll do is they'll keep them afloat until such time as there's a replacement Chinese technology, which is not what we want. I mean, so if you redefine this as let's punish Qualcomm because we're

mad at ZTE, now it looks a little different. So I think that the thinking on this... What's the opposite of strategic? Whatever it is, that's what we've been doing.

Brian Egan: [00:12:48] I see. Okay. So that's going back to Mr. Baker's Twitter account, we have...

Jim Lewis: [00:12:55] Uh oh.

Brian Egan: [00:12:56] ...somebody who — not Stewart — Dave Aitel who weighs in and says, "It's painful that the only weapon we seem to have in our quiver is tactical nukes. In the long run, this sort of thing is counterproductive" — along the lines of what you said, Jim — "It highly incentivizes China to invest in domestic production of entire verticals." So let's go back to you, Megan. So in other Chinese espionage allegations news, we have another company. The industry that — the surveillance video camera industry — which has taken it on the chin a little bit from our Congress, and one company in particular is outspoken in objecting to this. What's going on there?

Megan Reiss: [00:13:36] Yeah, so this is different. Hikvision — if I'm saying that properly — had some vulnerabilities that they think could have been used by the Chinese government for espionage purposes. The company denies it, full throttle, and they're actually accusing the US and Congress in particular of needing a scapegoat, another company to push against for the cyberespionage stuff. And they say, "You know we've actually set up an oversight center in California where you can have your police come and look at our source code for our technology. But you haven't done it." And so there's some legitimate concerns here that the pendulum is swinging so far in Congress to oversight over Chinese espionage that maybe they're pushing against companies that just have the same sort of cybersecurity insecurities that other companies do. On the other hand, this company — the parent company is 43% owned by the Chinese government, and that does raise some very legitimate flags that a lot of this technology could be used for spying.

Brian Egan: [00:14:54] You know it almost — if you're a Chinese company trying to do business in the United States, you almost have to wonder what it is you can do to get out from what actually may be some legitimate concerns on the US government side, at least some cases. How do you prove your bona fides and your independence from your own government? It may be impossible in some of these cases.

Megan Reiss: [00:15:17] And independence from your own government when you're owned by your government.

Brian Egan: [00:15:23] Particularly when you're owned by your own government. Yes.

Jim Lewis: [00:15:24] It's impossible to prove independence, and we set up a lot of these business arrangements. They're all predicated on the view of a sort of globalization, one world, everyone will be friendly. And in fact, China's a military competitor, and so we're stuck in some ways. We have a supply chain where China is deeply integrated into it. They have the same problem with our stuff. You know as we just talked about with ZTE. And there's really no easy way out. I'm not sure Hikvision — great name, by the way — I'm not sure Hikvision would be the centerpiece of any espionage strategy, but there is good evidence that if the Chinese want to get into some technology made by a Chinese company, they will do so.

Megan Reiss: [00:16:09] The big question is: when can a company be compelled to spy on behalf of the Chinese government? And I'm not sure we're not moving towards a place where the US military, at the very least, and other government systems are going to have increasingly strong concerns and oversight over every single one of these Chinese companies to try to figure out the extent to which that can be compelled.

Brian Egan: [00:16:33] Well, let's stick on the theme of espionage, US and China, for a moment. Jim, there's been talk in the news. The State Department says that they are taking steps to monitor China's compliance with this somewhat famous agreement that President Obama and President Xi entered into in 2015 about cyber-related espionage and economic secrets. What's going on there? Is this agreement something that's ever

been worth its salt in some way, and have there been changes that are significant over the past couple of months?

Jim Lewis: [00:17:10] You know I think if you talk to people, you get very uneven, very different responses. But in general most people seem to think it's working, noting that the agreement was very carefully scoped. It says that China and the US agreed not to use government entities for purely commercial espionage. It doesn't say no espionage. In fact, the US wrote that the espionage could continue. So one of the dilemmas is: you know you break into a Navy top secret weapon facility. That's perfectly legitimate under the agreement. Right? Hopefully we're doing the same thing to them. On the commercial side, what I hear though, it is still working, although it's beginning to fray a bit.

Brian Egan: [00:17:51] And so it sounds like from what you say this isn't an area though where it's worth the government's continuing to talk, and this is an area where there may be a meeting of the minds — or at least somewhat of a meeting of the minds — as opposed to other areas of espionage which I think both countries would say are still off the table for such an agreement.

Jim Lewis: [00:18:11] The dark secret for the Chinese is that they, despite all their propaganda, they still depend on Western technology to make progress. So there's a powerful incentive for them to steal it. And that temptation will come up again and again for the US. The agreement hasn't stopped them in Germany at all. The Germans didn't get an agreement. So it's not like Chinese commercial espionage has stopped. It's just it's gone down considerably in the US.

Brian Egan: [00:18:41] Okay. Matthew, back to you. So this is a story I really wish Stewart were here to talk about. This story, which is last week Twitter cleaned up a number of suspicious accounts. The numbers were actually staggering in some cases: over two million followers were dropped from President Obama's account; seven million followers were dropped from Twitter's own account.

Matthew Heiman: [00:19:03] I think Katy Perry and Justin Bieber also suffered losses of followers as a result of this housecleaning by Twitter, so everyone suffers.

Brian Egan: [00:19:14] Across-the-board losses. What is Twitter trying to do here? Is this a good use of time? Is this something that we should be worried about? Is this a long time in coming?

Matthew Heiman: [00:19:24] I think it's a long time in coming. But I think it's driven by Twitter's customers. Twitter's customers, who are advertisers and who look at how many followers Jim has or Brian or Megan have, are saying, "How do I know that when my message goes out to Jim or Brian or Megan, it actually reaches all those people that supposedly follow them?" And so while Twitter is not stupid to dress this up as you know "We're all for integrity and purity on our platform, and we want everyone to know what the truth is," I think it's really driven by customers saying, "I don't actually believe that Stewart Baker has five million followers in the Ukraine. Tell me how that can be true." I think when Twitter has gone and looked behind it and said, "Actually, Stewart's got five followers in the Ukraine," the advertiser says, "Okay, fine. Then rate I'm paying you for my advertising has got to change." I think it's really more of a reaction to what their customers are demanding more than anything.

Jim Lewis: [00:20:23] My kid works for a hip-hop website, and the scales fell from my eyes when he told me there was — maybe this has changed — there's a market in buying Twitter followers, and you buy them in blocks of like 5,000 or 10,000 or 100,000. There's a price. You go out. Companies will give you... So if you want to have a million followers, it's probably going to cost you about $3,000. They're not real, but you know they still show up on the scorecard.

Megan Reiss: [00:20:50] Wait, can I sell a follow for people for like $1 each? Yeah, I'd totally do that.

Jim Lewis: [00:20:55] It's worth a try.

Brian Egan: [00:20:56] Right. Right. Well, your account — you're inherently suspicious, though, so you may be blocked before you know it. And then finally, this is something that in the normal course, a GAO report on a Defense Department program, is normally not newsworthy, but it's on CFIUS which is something that has been rather newsworthy lately. GAO released a report early last week talking about the Defense Department's CFIUS capabilities. Jim, what's the takeaway from this report, and is this something that's going to impact the ongoing discussions in Congress and the administration?

Jim Lewis: [00:21:30] Yeah, because they kicked one of the most important parts of the bill. The bill's gone through all sorts of travails while people struggle to either keep loopholes open or close them. But the biggest one is it says that CFIUS will now have to look at advanced technologies. And so then you say, "Okay, that's great. What is an advanced technology?" We have no idea. More importantly, DOD and the intelligence community dismantled the process they had during the Cold War to identify advanced technologies. You know anyone can say, "Quantum computing? It's important." Okay, what does that mean? And we don't have the infrastructure that we used to have in the IC and in DOD to give us a level of precision. So I think the important thing here is everyone gets that we want to keep advanced technology out of the hands of the Chinese. We'll have to move a little bit further in defining it.

Brian Egan: [00:22:22] Yeah it's — the bill talks about — I think the words used in the current bill are "emerging and foundational technologies" — and this is something that I think DOD has really been pushing as part of its own concerns about the CFIUS process. It is interesting because I think everybody will turn to DOD for some leadership in this space. It's probably what they want, and the report suggests that they don't have the facilities as you said, Jim, to do this right now.

Jim Lewis: [00:22:49] And they want to rely on the export control lists, which at least in the case of the Commerce list probably is better at catching *submerging* technologies. So we've got a ways to go to rebuild this capacity.

Brian Egan: [00:23:03] To say the least. Okay, well, I think that that is a wrap for this week.

***

Stewart Baker: [00:23:09] Alright. I'm sorry I couldn't do the News Roundup this week, but I am going to do the interview with Woodrow Hartzog, who goes by "Woody," who's a professor of law and computer science at Northeastern University and who has written *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, which is essentially an effort to rethink privacy regulation by focusing on the design of systems, social media, and the like. But I'm not going to try to lay that out. Woody, welcome and let me just ask you: can you give us the elevator speech for the theme in your book?

Woodrow Hartzog: [00:23:58] Sure, and thank you so much for having me on. It's a pleasure. So the thesis of the book is that the law should take design more seriously than it does. And by that I mean I try to identify several areas in the book where design plays an important role in determining what I call privacy winners and losers. And a lot of this — the way in which design works in our lives — doesn't seem to be properly recognized in US or really international privacy law and policy, and so I try to suggest a way in which lawmakers can more cohesively approach design. I say they should embrace... They should identify values, and some of the values I say that we should focus on are trust, obscurity, autonomy. And I focus on autonomy as distinct from control and consent. One of the big critiques in the book is that privacy law and policy relies pretty heavily on this concept of "informed consent" and "notice and choice." I think that that doesn't scale in the modern age, and I think that design actually can be used to thoroughly corrupt and weaken that as a regulatory mechanism. And then in the back end of the book, I say that once you identify values, we articulate boundaries, reasonable boundaries, so not micromanaging every aspect of design really just articulating the outer boundaries of dangerous design, abusive design, or deceptive design. And then I talk about many different ways in which lawmakers can approach... Regulating the design of technology doesn't always have to be robust. It doesn't have to wind up in some sort of tort liability or heavy regulatory scheme. It could be soft,

educational efforts. It could be better funding opportunities. It could be simply better recognizing the role of design in existing things like contracts. And then in the back end of the book, I try to play out what I call this framework or design agenda or a blueprint with three different kinds of technologies. The first is social media. The second is what I call "Hide and Seek" technologies — technologies like surveillance technologies or technologies like encryption that are designed to hide. And then finally the Internet of Things, which I talk about ways in which that poses a really significant privacy problem largely due to design choices. So that's the elevator pitch for the book.

Stewart Baker: [00:26:26] Alright, I have to say my first thought on imagining the government contribution to design is a little like imagining that their contribution to literature as demonstrated by the Facebook terms of service. No one thinks that's a great work of literature or even something you would read for pleasure. And the design of websites is surely not going to become better — at least aesthetically — if the government starts telling people how to do their design.

Woodrow Hartzog: [00:27:08] Well, so I understand that worry. I think that when it comes to things like user interfaces, I think it would be a mistake for the government to say, "Here's what all user interfaces should look like," and you know from A to Z, top down, “this is the way it's going to look.” And that's why I propose more general, loose standards rather than a really micromanaging, heavy handed approach. But if you look at the existing rules we have now, the notice and choice model is already junking up the way in which websites work. If you log onto any website in Europe and you're going to get that annoying ad that pops up and says, "We want you to know that this website uses cookies, and cookies are surveillance trackers."

Stewart Baker: [00:28:01] It reminds me of... I kind of wish for somebody would take the Southwest Airlines approach and say, "You know if you haven't been in a car since 1965, here's how seatbelts work."

Woodrow Hartzog: [00:28:12] Right.

Stewart Baker: [00:28:13] And easily, somebody should say, "You know the drill. Click here."

Woodrow Hartzog: [00:28:20] Right. Exactly. Right. And it's all just a meaningless sort of rote exercise that doesn't do much of anything other than to really transfer the risk of loss onto users. My actually preferred approach would be to transfer a little more risk back to the designers and give them a lot of autonomy. Right? So we have loose boundaries where we say, "Don't create things that are unreasonably dangerous. Don't create things that are deceptive. Don't be abusive." And then we leave the rest to the designers rather than sort of engaging in this farce of saying, "Okay here are all the risks, A to Z. You agree to them." And then you agree, and then all of a sudden it's on you. It just strikes me as counterproductive from a design engineer's perspective.

Stewart Baker: [00:29:05] I'm not going to defend the idea that people are reading and agreeing after thinking about it to these terms because none of us does and there's not enough time in our lives to do it. But I do think you sort of shortchange the value of a notice and consent system in a couple of ways. First, it does allow for flexibility — allows people to try things and to try things with some confidence that they will be acceptable to regulators and to users. And second, one reason they have that assurance is we aren't all reading these terms of service, but somebody is reading all of them. And somebody is going through and blacklining the last version against the newest version so that they can look for outrages and bring them to our attention in the media. So there is a feedback loop. It is not the feedback loop that the GDPR actually imagines is occurring, but it's very real, isn't it?

Woodrow Hartzog: [00:30:15] So I think that's a great point. Yes, I think that private privacy policies and long terms of use serve a role, and they serve a role for the audience that I think you've identified which is advocates, regulators, people that actually do read these things from start to finish. But the farce that I really want to avoid is that these things are meant in any way at all for users. And it goes back to this larger — somewhere along the way, and I'm not sure when we decided, but the regulators and industry decided that informed consent was the right way to proceed in making sure that

people's privacy was respected while using technologies. The idea being of course the way that informed consent works is tort law, which is if we tell you about all the risks and you agree to take on all those risks and you do so anyway, then sometimes stuff happens, but for the most part, you've taken those on and we can proceed accordingly. But informed consent doesn't work for three really important reasons in the modern ecosystem. One, informed consent was designed around decisions that don't occur often. Right? So you have surgery. I just had some recent minor surgery, and I signed of course you know a slew of documents. And I listened very intently to all the possible things that could happen, and I had a chance to make that decision, but I don't have to make a decision very often. Meanwhile, we make that decision 10 to 50 times a day with websites. The next reason informed consent doesn't work is that the consequences are so visceral when things go wrong. Right? So I can envision for things like surgery what could happen. Right? Someone could leave something inside of me or something could keep bleeding and be unable to stop or there could be an infection. But it's really difficult to reject that kind of harm with the misuse of data into the future. And then the final reason is that the stakes typically are so high for standard informed consent regimes. Surgery, you could die, right, or have a serious complication, whereas that the harm that comes from these small decisions in the data ecosystem is very small, and so we tend to sort of discount them. That's why we click "I agree" as quickly as possible because we perceive the stakes to be so small, so there's no real incentive to put any investment in them. So my move would be to move away from notice and choice for users entirely. People just want to use technology in a reasonable way without getting hurt. Let's not bring you know massive — my argument would be let's not bring massive boilerplate contract law into this.

Stewart Baker: [00:32:58] So that maybe there should be a box to check that says, "I'm too busy to read this, but I'm willing to trust you"...

Woodrow Hartzog: [00:33:06] Possibly, yeah. Oh, absolutely.

Stewart Baker: [00:33:07] ...which is a fairer interpretation of that little chat.

Woodrow Hartzog: [00:33:10] Right. I think that's a much fairer interpretation. And I think that's what people are actually doing. Right? If you look at some of the research, one of the highest drivers of people's willingness to trust companies is actually not anything that's said in these terms, but brand recognition. Right? If everyone is using Amazon, then they must be relatively safe to use, so I'll use Amazon as well.

Stewart Baker: [00:33:32] Well, isn't that really part of our lived experience? We will try things where we don't see obvious terrible consequences, and if nothing bad happens, we'll try again. And about five times in, we just don't expect anything bad to happen, which is not — that is human nature, and it's also kind of not a stupid strategy. Rather than relying on us to read all the possibilities — frankly, I don't spend as much time on those medical disclosures as probably I should because I know they're going to include every conceivable terrible thing that would happen even if it isn't very likely, and it's just going to make me crazy and I'm still going to get the surgery. So I am not convinced that we should be assuming there's a better way to get informed consent, and maybe we should be just saying, "Yeah, people try this out." Until you disappoint them, they're going to count on you to do the right thing.

Woodrow Hartzog: [00:34:35] Yeah, and maybe there's a middle ground which is something I've thought about on a level that exists in things like products liability law, which is we don't frame this as some kind of informed consent where the full litany of what is going to happen with your data is presented to you. But rather, we view these things as warnings. Products liability law says, "You can't make anything that's unreasonably dangerous." There are certain things that you can make that are dangerous that are obvious to people, so you don't have to put a warning on a knife that says, "Watch out, this knife is sharp," because it's relatively obvious. But if there's a hidden danger or a danger that might not be evident, then you have to give warnings. And then if a warning wouldn't cut it, then products liability law says, "Well you can't make it. It's unreasonably dangerous." There's no way to really warn people when they're going to use it in a certain way. So maybe a way to sort of cut the difference is to say, “Let's frame this not as an attempt to fully inform you, but rather just an attempt to warn you of the risks that you probably want to know about.”

Stewart Baker: [00:35:42] So the problem I...

Woodrow Hartzog: [00:35:43] The warnings would look differently than I think a lot of the things that we see now.

Stewart Baker: [00:35:48] The problem I have with that — I take your point, and I think the analogy to strict products liability will chill Silicon Valley to its bones, but it's certainly a plausible model to employ, except that for products liability, with a few rare exceptions that are still controversial. Something really bad has to happen to somebody before you start talking about liability for the company that made it possible. And yet, you're pretty scathing about the fact that traditional privacy law requires a harm. And I guess I'm asking: are you really imagining that there will be strict products liability for stuff that causes harms that are purely theoretical?

Woodrow Hartzog: [00:36:44] No, that's a great point. I mean a lot of the harm problems that exist in tort law gave rise because there are hard requirements for a reason. Right? You don't want to create a cause of action where everyone can sue for punitive damages for something that's completely made up. A lot of what I'm advocating for is not necessarily opening the floodgates on tort law, though I think we're probably going to get there with things like the Internet of Things sooner rather than later, particularly if the IoT becomes hard to distinguish from a lot of non-software counterparts that combine to cause some sort of physical or heavy emotional harm. I think that there are sorts of harm that should be better recognized. I think the massive exposure that can result from data security harms could be better recognized. This is a lot of what I call "obscurity lurches" in the book. But a lot of what I would recommend actually is just a more regulatory approach that embraces the wisdom that's been developed in products liability law. So in other words, not creating massive liability from civil lawsuits, but rather regulatory fines. And it doesn't even have to be output based. Some of the things that I advocate in the book are actually process based. In other words, one of the ways that we can make products safer is simply require companies to go through a series of steps that are designed to help ensure that most of the time their

product is reasonably safe. If you fail to follow those steps, then that's when you're liable regardless of whether it results in harm on the back end or not. And this is largely the way that data security is regulated in certain sectors, maybe not necessarily tort law, but in other sectors. I think we could...

Stewart Baker: [00:38:32] Yeah, I agree with you. I agree the on the security side because you can then say, "Yeah, you know I had to go get all new computer or credit card numbers and then reauthorize all of my recurring charges, and it was a pain in the neck and it took me three hours online to do it. And that ought to be worth something." Fair enough. But if somebody says, "Well, I'm afraid now that my information is out there, or it's embarrassing that people know something about me and you should be strictly liable, Google or Facebook or Twitter, because you enabled people to find out something that I didn't want them to know, and I didn't realize that this was going to be possible, so the company should be strictly liable for that." It strikes me as you're now at a point where the harm is just kind of based on the sensibilities of whoever the plaintiff is.

Woodrow Hartzog: [00:39:38] Well, there are several ways that you could conceptualize this. One is I don't argue necessarily for strict liability in all circumstances. A lot of what I argue for is sort of standard negligence liability, which would be as long as you acted reasonably, then if the harm occurred, you're not liable because there was some sort of unforeseeable harm. I think that foreseeability is a key component in a lot of the design protections that I've been arguing for. But a lot of what I'm arguing for is actually two different kinds of harm. One is based on the massive exposure and vulnerability that can result from information being exposed in the marketplace, whether it comes because of a hack or whether it comes because someone violated a contract and sold you know 550 million user profiles to Cambridge Analytica. There's a certain kind of exposure that results when a large amount of personal formation is out there. And so a lot of it depends on whether you buy into significantly increased vulnerability as a harm in and of itself. We could debate that. But then there's another harm that results here, and that's the breach of trust harm, which is I think well-established in lots of other areas of the law, which is that when I enter into a relationship, when someone

asks me to trust them — which is what we were talking about earlier, and they say, "Trust me with the information. I'll protect it. I'll do the following things for it" — and then they don't do it, then that's a relational harm. This is what's — we enforce nondisclosure agreements all the time sort of based on this idea of a relational harm. Now, I relied upon something, and my reliance interest is now...

Stewart Baker: [00:41:24] Yeah, but in that case, I signed a contract not to disclose things. It was very clear to me what I could and couldn't talk about.

Woodrow Hartzog: [00:41:33] Not always. Depends on the wording, right?

Stewart Baker: [00:41:35] Fair enough.

Woodrow Hartzog: [00:41:35] I've seen some NDAs that are pretty vague.

Stewart Baker: [00:41:38] Fair enough. On the other hand, if what you're proposing is that we should turn Twitter into a fiduciary or Facebook into a fiduciary, I mean that's famous for making up obligations after the fact on the fiduciary. And we're creating this free-floating liability, and the response of social media companies is going to be to become extraordinarily conservative about what they do. And so instead of permissionless innovation, we're going to have innovation at the speed of lawyers, and I'm not sure that's really what we want.

Woodrow Hartzog: [00:42:23] Sure. So there will be costs. I embrace the fiduciary-like model along the lines of what Jack Balkin has proposed, and Neil Richards and I have written several articles about the role of trust. And Ari Waldman has a great book out on "privacy as trust," and I generally like that model. I realize that it does come with a lot of costs that it will mean that platforms will not be able to do everything that they want to do. But on the flip side, I think that there's a real positive that can come if — particularly if companies voluntarily adopted a fiduciary model, which is one of the ways that we could do this, is have it be an opt in, and if companies are serious about protecting people's trust, then they can opt into that model. We can make it mandatory, which is

the way to do it. But one of the real advantages of that is then that companies will have something that they can take to users and say, "Just trust us with your information. We're promising to be bound by this set of rules." Because when companies respect the trust that people give them, then they can do things with that information, they can benefit from that information while still keeping the users safe and keeping the trust that they've been given, and then everybody wins. If we proceed under that model, will it be at a slower pace? Maybe. But in terms of long-term sustainability, I think that we might actually end up better off. We might be able to still have platforms growing at a possibly slower, but still increasing, rates. We might be able to ease into the digital economy without quite the same sort of disruption — and I use that sort of not in the tech-good sense, but in the bad sense — in harm that we're seeing right now. So if it creates more trust and more sustainability, then I think that that could be good.

Stewart Baker: [00:44:18] So I've been very critical of the European data protection stuff — the rights-of-man approach to privacy — because it is so inherently vague. You never know whether you're in violation of it or not, and you'll find out you're in violation when important bureaucrats come to you and say you're in violation, which means that basically it's a tool of the ruling powers to beat up people that they don't like. And your invocation of Cambridge Analytica reminded me: you know do you really think Cambridge Analytica was even a privacy problem? It's not a privacy problem. There's nobody running around saying, "I gave away the names of my friends to Cambridge Analytica, and now I'm really disappointed." What they're disappointed about is the wrong person won the 2016 election, and that's what all of the emotion is about. And privacy is just a stick to beat Cambridge Analytica and Facebook with.

Woodrow Hartzog: [00:45:21] Well, I mean it's a good point in that this practice that — the academic that added originally designed the survey that then gave the information to Cambridge Analytica — the practice that was being engaged in was actually routine. And it's certainly wasn't just Cambridge Analytica that was engaging in it. And a lot of the questions that I got in the wake of Cambridge Analytica was: why this? Why now? And I do think that one of the reasons was probably had to do was political. But I think that the other one was there's only so many times that you can realize that you thought

that Facebook was working one way and it was working really an entirely different way. And there are only so many sort of apologies you can hear before you just sort of lose it.

Stewart Baker: [00:46:12] Yeah. Fair enough. And I think there've been a lot of criticism of Facebook's design of their systems for exercising the control that it provides. That's one reason why design is salient these days is the design of those screens leaves a lot to be desired.

Woodrow Hartzog: [00:46:38] Right. It gets back to the whole notice and choice thing. So I mean it is a privacy issue in the sense that we've decided that privacy is a notice and choice issue, and the choice that was given to users was this sort of obscure little button nestled you know five screens that I give permission for my friends to share information about me on XYZ platform. Right? And nobody knew that button was there, and it was I believe turned on by default at the time, which just allowed for sort of massive exfiltration of data without people's knowledge. And I think that's really where a lot of people got upset, which is that they didn't even realize how the data ecosystem was working. I think that most people don't. I think that even some of the brightest minds that have tried to figure out the full range of the data ecosystem have trouble wrapping their minds around it. I've looked at some of these charts, and they befuddle me.

Stewart Baker: [00:47:32] So let me push your argument in the direction that at least traditional academics aren't likely to want it to go. Suppose that I'm the parent of the child that Jim Comey made famous, who was abducted, disappeared, probably killed. All that was left was her cellphone — iPhone — that had her diary on it, and the police wanted to see if she had any indication of contact with somebody that they could be investigating, and they couldn't get into the phone. Do the parents get to say, "Hey, Apple you never told us or our daughter about the risks of your locking up this stuff in ways that law enforcement can't get at. And that's a design decision you made that wasn't fully properly disclosed, so we want to hold you liable for your encryption policy."

Woodrow Hartzog: [00:48:38] So in terms of holding someone liable, I'll put that to the side just because I — even though I'm a tort law professor, I don't think that everything

is a tort. But in terms of Apple's responsibility to adequately articulate how their technology works, I think it's a fair point. If we could — depending on what sort of collective consciousness of a significant, appreciable minority of users was regarding whether the information would be stored — Apple's probably has an obligation to adequately articulate how their technology works, and that includes warning people if they're relying on the traceability of a technology. So for example, let's say that's the Find My iPhone app, which I think is a useful app, were somehow rendered inoperable in certain situations in a way that would not be evident to most people who were using that app, maybe even relying on that app, if we could plausibly state a case for that, then maybe we need to have some sort of warning. Not notice and choice, but some sort of warning that says, "Warning: this is not going to work in the following situations that you might have been relying on." If it's foreseeable that people relied upon that, then maybe we do need a warning. I don't know if that...

Stewart Baker: [00:50:00] It's sure foreseeable that there will be criminal evidence in somebody's iPhone. You don't know whose. And you know as you can imagine, it's always possible to say, "That wasn't good enough warning. Adequate warning? Yes, you gave them the notice after they'd bought the phone and were stuck with it, but you didn't give them ability to change it. You didn't tell their parents, who obviously have an interest in their well-being when in the prosecution of their murder." So there are ways in which the idea that the design is faulty if the outcome is unacceptable could turn out to be just an endless sink of litigation for companies.

Woodrow Hartzog: [00:50:48] Yeah. I mean this is... Well, I think that in terms of finding what adequate warnings are, companies wrestle with this all the time and have been in areas far beyond privacy. I mean this is standard sort of products liability law, not just strict tort liability but generally trying to figure out what an adequate warning was. But I do think that it's fair to place the responsibility of adequate warnings on the companies that make the technology.

Stewart Baker: [00:51:22] Fair enough. And I'm going to give you a chance to tell me in just a second what events or papers you have coming up that people can pay attention

to who are listening to this. But I do want to tell you my design story, and you touch on architects — maybe even Frank Lloyd Wright, who was famous for coming to visit the people who had moved into his houses and putting their furniture someplace else because he thought they had you know interfered with his vision and they should live the life he had imagined for them, not the life that they wanted. And that has struck me that I once almost became an architect, and I finally didn't, claiming that it was because there is such a deep well of kind of fascist authoritarianism at the bottom of most architects' view of what their impact on the world will be. And that leads me to the observation that you are pushing on an open door if you take an inherently authoritarian field like design, where basically people are making decisions for the user and telling them how to live and how to operate, and you're selling the idea of using that to governments which have similar tendencies. So I predict great success for the focus of government on design for the future because they're really bedfellows made for each other.

Woodrow Hartzog: [00:53:06] I think that's right. I think that's... I come from this from the vantage point that the ability to design is an exercise of power. Right? When you create an object that is then released into the world, and you make design decisions, you make certain realities more or less likely. Some of those are foreseeable, some of those are not foreseeable. But to the ones that are foreseeable, I think that you have to be accountable for the ways in which your power is creating those reasonably likely scenarios. And that's what government does. Right? So governments — or at least partially — the role of government is to make sure that that sort of power is not abused and that it's used safely in a sustainable way. So that's largely the sort of the font of a lot of this.

Stewart Baker: [00:53:57] Well, that's a great response to my suggestion, which is: yeah, designers are authoritarian, so we should have another authority over them. So...

Woodrow Hartzog: [00:54:07] Or propped up against each other, right?

Stewart Baker: [00:54:09] Exactly! So I promised I would give you a chance to talk about speeches you're giving, papers you're releasing. Is there anything else that our listeners should be watching for?

Woodrow Hartzog: [00:54:20] Sure. So right now I'm working on a book with Daniel Solove that we're working on data security, rethinking the law of data security, calling it *Breached: The Failure of Data Security and How to Improve*. I'm working on a few articles with Neil Richards on the concept of trust in which we're advancing our thesis of trust. One of the things we're working on is the role of the European Union in sort of exporting norms and why that can be good in some ways, but not necessarily great in others. Then I'm working on a piece on facial recognition technologies with Evan Selinger where our argument is it's time to take this technology seriously and think about some real meaningful restraints on it.

Stewart Baker: [00:55:10] And in the meantime you're teaching as a professor of both law and computer science at Northeastern University, right?

Woodrow Hartzog: [00:55:18] That's correct. Yeah.

Stewart Baker: [00:55:19] Talk about taking strange bedfellows and making them lean together.

Woodrow Hartzog: [00:55:24] Right. That's a good point. My job is to make the two groups learn to talk and love each other.

Stewart Baker: [00:55:31] Well that's terrific. Thanks to Woody Hartzog. Thanks also to Matt Heiman, Jim Lewis, Megan Reiss for joining us in the News Roundup, and thanks to Brian Egan who bailed me out by agreeing to host the News Roundup. This has been Episode 226 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Remember to send us suggestions for guest interviewees. Send them to cyberlawpodcast@steptoe.com, and if your nominee ends up on the show, we will send you a coveted Cyberlaw Podcast mug. Somebody suggested Woody Hartzog. Is he

getting his mug? Oh. Alright. Well you just heard from Michael Beaver, our intern. He was the one who found Woody's book. So since he's got a lifetime supply of mugs already, he probably won't get it. But you can get one if you find somebody else as entertaining as Woody has been. We are previewing some of our news stories on my Twitter feed, @StewartBaker, also on LinkedIn and Facebook, if you have comments on them, and we've gotten some good comments already. Before the show we might be able to make reference to your comments or just rip off your insights without giving you credit. If you want to complain about that or something else using actual voice technology, leave a message at 202-862-5785. I'm not going to repeat this number again because nobody is leaving entertaining or even any voicemail messages, so we may just drop this. What we won't drop is our request that you leave a review on iTunes or Google Play or Stitcher or Pocket Casts. That's how people find us. And again, we read them, and if we see something entertaining or entertainingly abusive, we'll definitely read it out on the show. Upcoming guest interviews. We are almost up to our hiatus for August, but we will be hearing from Noah Phillips, brand new FTC commissioner, formerly with Steptoe — because you have to be at Steptoe if you want to have something to say about cybersecurity at some point in your career — and he'll be on in our last podcast before we go on hiatus. Credits for the show: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio engineer; Michael Beaver is our intern; and I'm Stewart Baker, your host. Please join us again next week as we once again provide insights into the latest events in technology, security, privacy, and government.