Steptoe

Episode 241: "You'll never know how evil a technology can be until the engineers deploying it fear for their jobs"

Stewart Baker: [00:00:05] Welcome to Episode 241 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking about technology, security, privacy, and government. We've got a great lineup today. We've taken what would have been an interview topic and transformed it into part of our News Roundup, and we'll be talking to Adam Candeub, who's a professor of law and director of the Intellectual Property, Information, and Communication Law Program at Michigan State, about the USMCA (the United States-Mexico-Canada Agreement). And also we have Paul Rosenzweig, founder of Red Branch Consulting and former deputy assistant secretary for policy at DHS. We've got Jamil Jaffer, founder of the National Security Institute and a professor at George Mason. We've got Gus Hurwitz, who's a professor of law at the University of Nebraska. We've got Nick Weaver, senior researcher at the International Computer Science Institute and a lecturer in Computer Science at UC Berkeley. And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. So that'll get us going right away. There was an astonishingly depressing story about how Uber managed to kill that woman in Arizona and the build up to that. I think there's a whole new law of technology, but what did you draw from that?

Nick Weaver: [00:01:43] Tragic and inevitable. The problem is self-driving cars are actually a really hard problem. It's easy to get the 90% there, the drive on a freeway. It's hard to get that last 10%, and Uber as a corporate culture is rife with awful. And so basically what it is is multiple things. They were cutting corners on the computer, going, "Oh, the safety driver will save us," then cutting back on the safety drivers. And the user experience is you don't have a human back up a computer; you have a computer back up a human because humans get bored and watch videos and the like. And so in many

ways, this accident was tragically inevitable. But to inject a little levity, they do have to keep up with Tesla in that department.

Stewart Baker: [00:02:39] [Laughter] Fair enough. Yes.

Paul Rosenzweig: [00:02:40] So what I was gonna say, I'm a little more optimistic than Nick about the long-term prospects, I think, which is to say 90% is better than most human beings. And the question is not going to be is it perfect but how much better or worse is it than human driving, and I think in the mid-to-long term it's going to clearly be safer. I do agree with one thing, though, which is that there is a real culture conflict here between the [Silicon] Valley move towards rapid development and deployment – the Facebook move fast and break stuff. That works just fine when all you're doing is writing code and maybe breaking people's privacy but not killing people right away. It doesn't work as well in the Internet of Things where human safety and well-being is at risk. I think what this portends – I mean, since we're lawyers talking about law, to quote my favorite Baker-ism – is likely greater regulation in this field that will probably stifle the pace of development a fair bit and at uncertain long-term gain or loss.

Stewart Baker: [00:03:53] Yeah. So the law that I think you can derive from this – because it appears that these engineers really were afraid they will all lose their jobs because [Uber CEO Dara] Khosrowshahi was going to come down and take a ride and it would be bumpy and stop and go and he wouldn't like it and he would say the whole project is misbegotten, and so they turned off a lot of the braking in order to avoid that – and the law I would derive from this is that you don't really know how evil a technology is until you've seen it used by engineers who are afraid they're going to lose their jobs. That's when people start throwing out the stuff that they don't care about and revealing the technology in its essence. That's why Twitter is so woke-ridden. It's not making any money, so they're afraid of their customers. They're afraid of their own employees. And in order to pacify them without giving them money, they're embodying "social justice warrior" norms into their decisions about who can speak on Twitter. Yahoo security? Same thing. They didn't have any security 'cause they didn't have any money. And that shows you that at the end of the day, these social media companies are gonna throw

out your security because it doesn't pay. I love this. There was the story suggesting that airlines now have an AI algorithm that says, "Is this a family unit? Do they all have the same last name? If so, let's spread them around the plane and then make them pay to come back together."

Gus Hurwitz: [00:05:38] [Laughter]

Stewart Baker: [00:05:41] Ryanair apparently does the most to randomize their family unit seating and then does charge people to pick their own seats. So it's only when people are really starting you know down to the last nickel that they start showing you how this technology is gonna be used in the long run.

Gus Hurwitz: [00:06:02] I think they charge more than just a nickel for that, Stewart.

Stewart Baker: [00:06:06] [Laughter] That's true. Okay. Fair enough.

Nick Weaver: [00:06:07] And the heuristic is actually pretty easy, and it's just do not give the people seats until they check in, at which point, well, all the contiguous blocks are already taken. You don't need an AI for that.

Stewart Baker: [00:06:24] You may well be right. Although, yes, it is true that you're gonna get random assignment and you'll know it and they'll offer you a chance to avoid random assignment; although, I would have thought that if you said, "Oh, we'll take the middle seat," that that would work. Next thing you know they'll say, "You're not allowed to change seats with people to get your family back together," which of course is how people work it out in real life on the plane. And they'll come up with some safety reason why you can't do that. So Jamil, Gus: Facebook is talking about – or at least Zuckerberg is talking about – having a "Supreme Court" that would get it out of the "woke-ness" dilemma in which you can just never be more woke than Twitter. And frankly, Zuckerberg is just not very good at this kind of policy stuff, so he'd like to turn it over to a "Supreme Court." Does that make sense?

Gus Hurwitz: [00:07:26] So my take is that this is either the worst idea ever in true Zuckerberg fashion or it's a really brilliant business move on Zuckerberg's part. It has all of the tell-tale signs of a traditional Zuckerberg-doesn't-understand-how-hard-these-problems-are, naive sort of let's-just-push-this-to-someone-else-and-wave-a-magic-wand-and-the-problem-will-go-away. The hard question with this is: What are the rules that this "Supreme Court of Content" would enforce going to be? And that's the hard thing to answer. It's hard to figure that out. On the other hand, the thing that makes me think this might be brilliant is if the goal here isn't just to create a "Supreme Court of Content" – a really bizarre term, but a "Supreme Court of Content" – for Facebook but to truly create an independent third-party arbiter of these content disputes that could be used by other social media companies and in other industries. That might be a really good way for Zuckerberg to highlight: "Hey, this isn't a Facebook problem. These are hard content questions. These are wicked problems that we as a company can't answer. And this is an industry problem, not a Facebook problem." If he's able to spin it that way, that would be a really interesting move.

Stewart Baker: [00:08:44] Anything to get out of the barrel. Paul?

Paul Rosenzweig: [00:08:47] I'm less persuaded that it'll be an effective method in the long run. I think I agree that it is a good PR move, but it can't really obscure the fact that somebody is managing content. Right? And in the end, Facebook is going to own it. I mean, you jocular[ly] said, "Well, what if he gets Merrick Garland?" Right?

Stewart Baker: [00:09:13] Yep. I hear he's available.

Paul Rosenzweig: [00:09:15] I hear he's available, but it's really got to be both Merrick Garland and somebody from Germany and maybe somebody from India and maybe somebody from China, and then let's throw in a Brazilian just to make it five. And you know it isn't gonna work very well unless it has – for Facebook to really head off its problems around the globe – unless it has global buy-in. So Merrick's not enough.

Gus Hurwitz: [00:09:40] Yeah, there is no way that this idea is going to work because it's trying to solve what is a classic wicked problem where you've got different values of speech from around the world and we can't resolve them. Even if we do have a representative body of judges on this court, all that that will reveal is the same problem that we have in every cross-border fight. There are different competing values that are oftentimes irreconcilable.

Stewart Baker: [00:10:06] But there is the value of being able to say to everybody, "Look: We've created this place that you can fill with your content standards. You figure out what they are, and we'll be glad to enforce them." And that lets people fight among themselves as opposed to everybody beating up Facebook first for what they've done and then what they haven't done and back and forth. So maybe it is particularly clever.

Nick Weaver: [00:10:35] Except that it doesn't actually solve the Facebook problem. The Facebook problem on the content moderation is not the few big, high-profile Alex Jones types. It's the grinding day-to-day things.

Adam Candeub: [00:10:50] Yeah, but it does solve one problem in the sense that you know when the president didn't want accountability for handing out radio and television licenses, they gave it to this independent entity called the FCC and thus it was able to pretty much get what it wanted without very much accountability, with less accountability. And I think that could be exactly what Zuckerberg wants is that they'll have this facade of independence and it will act in the public interest, whatever that is, just like the FCC does. And if they make a bad decision, he can say, "Oh, it's not me. It's this independent body of good, wise thinkers who are representative of the world. Not my problem." And from that perspective, it could be very effective.

Gus Hurwitz: [00:11:39] Everyone should go to law school and take administrative law because what Adam is really getting at is independent agencies have a long history. We generally create them with the idea that "Hey, this is going to bring about technocratic expertise that will solve these really hard problems," when the reality is it's more a politically expedient way to push the politically hard problems to someone else. And

then the folks who create the agency, if it succeeds, can say, "Look what I did. I'm great. I created that agency, that independent body." And if it fails, the person who created it can say, "Look at that failure. We need to have more resources, and we need to try harder. And you should give your trust to us because we're trying to solve this problem."

Jamil Jaffer: [00:12:23] And that really is the theme of what we've seen in this space. I mean, we see Zuckerberg not only doing that with the sort of "Content Supreme Court," but we've seen Brad Smith do it with Microsoft and these "Tech Accords" and the "Paris Call" and the like. And we even see Zuckerberg doing it here when he talks about the idea that Facebook is working with governments to create regulation. And so again this is not necessarily a bad thing in the sense that somebody has got to do this, and political accountability for these decisions won't necessarily be a bad thing. And bringing you know governments and industry together to work on these problems is probably the right call. That being said, let's call it what it is, which is everyone's trying to toss the hot potato to somebody else while saying, as both Adam and Gus have said, "Well, look, we're trying to work with these guys. We try to make it work, and if it doesn't work, well, then you know we can solve this problem for you, but you might not like the way we do it. But we tried."

Stewart Baker: [00:13:17] Yeah. So as a good example of just how hard it is to be Facebook these days, I am looking at the procedures in a case called *Six4Three v. Facebook*. You've got to love this. Six4Three was a company that created an app for Facebook that would show you pictures of all your friends and your friends' friends wearing bikinis. And when Facebook said, "We don't really like that app," Six4Three decided that its real future in business was suing. And they collect a whole bunch of stuff under a confidentiality order, and then in an absolutely bizarre sequence of events, one of the guys who had access to the materials that Facebook had produced under a confidentiality order but wasn't supposed to, went to the UK and just happened to be talking to a *Guardian* reporter, who just happened to introduce him to somebody at the UK Parliament Committee on Mass Media and the like, who just happened to have the serjeant at arms handy to tell this guy that he was obliged to cough up all the data that he was holding under a confidentiality order. And lo and behold, he did, but he says it's

not his fault. It's kind of just an astonishing and, to my mind, highly suspect chain of events. Is there any possibility that this was just, as it's portrayed by the Six4Three guys, a series of unfortunate events that led to the exposure of all this confidential data?

Nick Weaver: [00:15:18] I find it plausible, having read through it, that it looks like he was basically leaking it to the reporter going, "Hint, hint: The un-redacted version of these filings is interesting," back and forth, back and forth. And he did get caught up in it, but damn, this is hardball on the British MP's part. Why don't they just ask this from Facebook itself?

Stewart Baker: [00:15:44] Yeah. Wouldn't you think?

Paul Rosenzweig: [00:15:45] But they have! I mean, I think this is felony failure to balance grape, and Facebook is getting exactly what it deserves.

Stewart Baker: [00:15:52] [Laughter]

Paul Rosenzweig: [00:15:53] They've been asked to come to this thing twice, and Zuckerberg just says, "No. I'm not coming." And you know, good for him. Now good for you. I have no brief in the fight over whether or not this is actually relevant to anything that the British government is reasonably interested in, but governments are the alpha predator. You mess with them at your own risk, and I have zero sympathy with Facebook. Yeah, sure it's collusive, but so is every congressional investigation that's ever happened in America.

Stewart Baker: [00:16:31] Yeah, fair enough.

Paul Rosenzweig: [00:16:31] Every one of them involves some disgruntled loser in some regulatory or legal thing who finds a sympathetic ear.

Stewart Baker: [00:16:40] Yeah. I'm pretty skeptical that the serjeant at arms has ever been used in a discovery dispute before. And I am conscious of the fact that the ethical

rules of the UK Parliament don't actually prohibit members of Parliament from having second jobs, as far as I can tell. They just have to disclose them. And that makes me wonder whether the second job of some of the committee members or this committee chair might have some bearing on their interest in this dispute.

Adam Candeub: [00:17:08] Yeah. My vote is always for Perfidious Albion, and I think there's a lot of... It seemed to me, reading through it, that I would agree with Paul. There's a lot of collusive behavior going on here that at least strikes my American sensibilities as a bit extreme, even for Facebook.

Stewart Baker: [00:17:29] Okay. So the Commerce Department has published an Advance Notice of Proposed Rulemaking, which is it's not even a Notice of Proposed Rulemaking. They're taking comment on *whether to take comment* on what are emerging technologies that ought to be subject to export control, tied to the new FIRRMA [Foreign Investment Risk Review Modernization Act] bill, the new CFIUS [Committee on Foreign Investment in the United States] bill. The goal was to identify the technologies that really scared the Defense Department if they turned out to be developed and accessed by the Chinese, to be candid. Gus, this is a complex rule and a lengthy one, but it's also a little formless.

Gus Hurwitz: [00:18:15] Yes. So my take on this is basically we are all trade lawyers now. I had a conference last month that I helped to organize with ICLE (the International Center for Law & Economics) and the University of Leeds that was an antitrust conference, and at the end of the day, we were talking about international issues. And the conclusion, I think, of everyone in the room was if you're an antitrust lawyer, you have to be a CFIUS lawyer today. You have to understand trade law. You have to understand all of these emerging dynamics. And I'd say if you're an IP lawyer, this is increasingly the case as well. So I think what the Department of Commerce is doing with this advanced NPRM, it's no surprise. This is a requirement that it look at these emerging technology areas and decide how they should be classified for export control purposes. This was in the NDAA [National Defense Authorization Act], so we've had four or five months' notice that this was coming. But the range of emerging technology

areas is really broad, from AI and machine learning to GPS technology to data analytics, robotics, additive manufacturing – that is 3D printing – and hypersonics. That one might make more sense or be less surprising to see included in here. But it's basically every technology that any tech company, tech industry, is working to develop is covered by this. And that doesn't mean that they're going to be subject to export controls. It means that BIS [Bureau of Industry & Security] is going to do a study. There are, I think, six or seven different questions that they're asking about each of these sectors, and they will determine which of the different ITAR [International Traffic in Arms Regulations] classifications these technologies will be subject to, whether or not they can be exported at all, or whether or not you just need a license in order to work on them if you have international contacts. And the questions that are being asked include: What is the current status of these technologies? How intrusive or obtrusive to research and development would these restrictions be? How disruptive would it be to industry? So it's entirely possible Commerce will take a light-touch approach to looking at these, but depending on the amount of political influence, in particular, that goes into the process, this could be a dramatic burden on wide sectors of the high-tech industry.

Stewart Baker: [00:20:57] I'm guessing that the Commerce Department, which likes to spur commerce in the United States, is sort of hoping that they get some critical comments from industry about the scope of these things. But Paul, this does sort of look to me as though it is an American – or at least an American Defense Department's – version of industrial policy for the 21st century.

Paul Rosenzweig: [00:21:23] Yeah. No, I think it is. I think it is destined to be the – I mean, I think as we were just talking about it, is destined to be the – venue for much of the controversy over the next 10 to 15 years. I think that the big problem is going to be that it's unlikely to really be successful. Industrial policy works with hard stuff that is within your physical control. It's much more difficult with tech that is ideas-based, like 3D printing. And so it can have a slightly palliative effect, but I don't think that it's going to... I think in the end we're going to see that the costs are greater than the benefits, but it's going to be the main thrust of how we try and control military technology for the next 10, 15 years.

Nick Weaver: [00:22:16] I don't think it'll work.

Stewart Baker: [00:22:17] Yeah.

Paul Rosenzweig: [00:22:18] Yeah.

Nick Weaver: [00:22:18] Because the problem is the real threats are so incredibly dual-use-y, like a 3D printer will be used for guns included. And so with such dual-use nature that anybody who's trying to remotely participate in the modern technology will have the resources necessary and the ideas necessary to take advantage of this dual-use stuff.

Gus Hurwitz: [00:22:47] Yeah. Nick just hit the big problem out of the park. Everything, all these technologies are dual use. We saw these fights back 25 years ago in encryption, and of course, as Paul says, the "ideas" element makes it very difficult to use trade controls to control these technologies. And add in the supply chain aspects of this. The nature of dual-use technologies we've been struggling with for more than 25 years, but it's pervasive in every aspect of the tech industry today. And it poses real problems for going back to how Paul described the governments of the world. I forget the exact phrase that he used, but they're the "big bads" of the world. They have lots of power to control things, and if you mess with them, they're going to mess with you back. Well, they're not just messing with individual companies here. They're messing with entire industries, and it's hard to see how that doesn't have negative effects for civilian uses.

Stewart Baker: [00:23:47] So here's my prediction: That within a year we will see this list again, but it will be on China's industrial policy priority list. And indeed if the US government is thinking carefully about this, they'll put a whole bunch of stuff on there that they think is intriguing but actually ultimately dumb, dead-end technology in the hopes that the Chinese will pour billions into it in imitation of what it thinks US policy is. Alright.

Nick Weaver: [00:24:20] That's called "stealth aircraft."

Jamil Jaffer: [00:24:23] If only we were that smart.

Gus Hurwitz: [00:24:25] Worth noting the comment deadline is December 19th, so they gave a minimal 30-day comment window on the ANPRM. So warm up your typewriters, everyone.

Stewart Baker: [00:24:35] Alright. So the thing that I wanted to talk to Adam about is an interesting piece he wrote for RealClear Politics on what most people who are calling NAFTA 2.0 but which formally is known as the USMCA (the US-Mexico-Canada Agreement). And Adam did what I always meant to do but didn't, which was to actually read the USMCA as it affects platform and software companies to see what's in the agreement. And I got to say, Adam, you found some pretty surprising and somewhat troubling things.

Adam Candeub: [00:25:19] Well, I'm glad you agree. I was really shocked. What we saw was that the USMCA does sort of *sub rosa* expansion of [Communications Decency Act] Section 230 immunity. Specifically, it enlarges the immunity that big platforms enjoy with regard to material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable. Right now Facebook, Twitter, they can remove such obviously sexual or child-unfriendly language with complete immunity from liability, but what the USMCA does is it takes out "obscene, lewd, lascivious, filthy, excessively violent, harassing" and just leaves the "otherwise objectionable." So right now it gives Twitter and Facebook the ability to remove any material it finds objectionable without any legal consequence. And this is kind of ironic coming from our president who has criticized the social media platforms and has promised to be a populist. So it to me is very troublesome.

Stewart Baker: [00:26:43] So Section 230. Twitter just apparently has decided that it's going to treat as hate speech what's called "dead name-ism." That is to say, if you're transgender and you change your name from a boy's name to a girl's name, people who

continue to use the boy's name are engaged in hate speech. I have actually, in my a never-ending quest to get suspended from every social media platform, I have tweeted that I want to know whether that means I can say that "Bradley" Manning is a traitor or whether that means that I'm engaged in hate speech. So we'll find out once again as I take my social media identities in hand and put them at risk. But if I didn't like that, I could sue Twitter saying, "You don't have an immunity for decisions of that kind. Having made a decision of that kind, you are engaged in editorial action, and you're responsible for everything everybody tweets." And so the scope of the 230 immunity has been part of the debate about social platform discrimination against conservatives and the extent to which it ought to be honored. And now it looks as though this administration has agreed to dramatically expand the immunity.

Adam Candeub: [00:28:13] Exactly. Because, for instance, right now if they kicked you off for saying something like "Bradley Manning is a traitor," presumably you'd have some sort of action perhaps in consumer fraud, in contract, perhaps even some type of anti-discrimination action in those states that protect you against discrimination based on your political beliefs. But now essentially what the USMCA says is, "No, Twitter can just cut you off if they find you objectionable for any reason." And it's really troubling because Twitter seems to be getting very erratic and a little irrational in whom they're kicking off. I mean, every day it's someone different who doesn't really say anything that's obscene, who doesn't say anything that's particularly hateful, just someone Twitter doesn't like. And that seems the problem.

Stewart Baker: [00:29:10] Yeah. They've kept Louis Farrakhan and kept his ["verified"] check, so certain kinds of hate speech apparently are okay with Twitter. But what I'm struck by here – we just were talking about a private "Supreme Court" to decide what you could say or not say – this is a kind of private lawmaking. These negotiations happen largely behind closed doors, and the agreements are written to bring on board a critical mass of effective lobbying groups, mostly business groups, so that the agreement will have the support of industry at a substantial level, which means you're basically asking industry, "Well, what do I have to give you to get you on board with this agreement?" And then once you've given it to them, it becomes law. Not just the law of

the country, which you know these days it's hard to change, but it becomes almost a constitutional amendment because you have to negotiate with the Canadians and the Mexicans in order to change US law.

Adam Candeub: [00:30:16] You're right. It's kind of shocking because, as you pointed out, Trump is supposed to be a populist. This is a decision about utilities and services that everybody uses all the time, and it's not even being regulated by a law coming out of a bicameralist process. The House of Representatives has absolutely no say whatsoever; it's what the Senate decides to approve. And it seems to go against the promises that Trump made, but it also goes against sort of a basic democratic process in regulating the Internet. And we'll see what happens in the Senate. I mean, there certainly are senators who have expressed interest in this provision, and we're hoping that they might take action.

Stewart Baker: [00:31:00] So the USMCA comes up for approval in the lame duck [session]?

Adam Candeub: [00:31:07] It sure does. And you know all the moving pieces are moving, and we'll see what will shake out. But again this is something that senators have expressed some interest in, and you know we're hoping that moving forward, it will be stripped out of the final agreement.

Stewart Baker: [00:31:23] Okay. Nick, Cozy Bear is back. Fancy Bear is back. There's been a lot of attention to some of their recent tactics. What's the takeaway?

Nick Weaver: [00:31:35] Yes. The Bear's hack in the woods.

Stewart Baker: [00:31:39] [Laughter]

Nick Weaver: [00:31:39] The takeaway is it's really hard to change your identifiers as an attacker once you've been identified. It's basically they don't care anymore about getting caught.

Stewart Baker: [00:31:50] Yeah. Well, that's a lesson they learned from China and continue to put into effect. I do want to point to a China story about an artificial intelligence fail that really deserves to be recognized. Gus, you pointed me toward this story, and I just loved it.

Gus Hurwitz: [00:32:13] Yeah. So this is the story. It's been in the news yesterday and today. A CEO of a local business took out an ad for her business by putting a big picture of her face on the side of a van, and that van was driving down the street. And the AI saw it and recognized her face and issued a citation to her for jaywalking. And I believe – I've seen different stories talking about it different ways, but I believe – this is a technology being deployed and developed relating to the new social credit system. So this raises a fair number of questions about the quality of that system. My thought was folks should start printing out masks of their favorite political leaders and walking down the street and jaywalking with them to see how they like the social credit system in action.

Nick Weaver: [00:33:00] The big question is: If you were wearing a Winnie the Pooh head, does it get recognized as Xi Jinping?

Stewart Baker: [00:33:05] Yeah. That would wreck his social score in a heartbeat. Yeah. I was thinking you could actually turn this into a business by getting a high-def screen that you put on your van and then charge people to take their pictures off it.

Gus Hurwitz: [00:33:27] [Laughter]

Stewart Baker: [00:33:28] Alright. And Gus, Nick, you also pointed me toward a recent what I would call kind of acqui-hack. That is to say, somebody acquired a bit of a JavaScript app and turned it into a piece of malware.

Nick Weaver: [00:33:47] More importantly, a JavaScript library. Programmers are lazy and just borrow libraries from other things, and there's this infrastructure in JavaScript

that takes all the libraries together and sends them all out. And so somebody took one of these libraries that people used, took it over with the consent of the maintainer, and added code to it to steal cryptocurrency because "Hey, why not?" But the acqui-hacks are actually another problem, and any bit of software that's maintained or that has cost to maintenance and is widely deployed, including libraries, extensions, etc., where there's an update mechanism in place are vulnerable to this. We've seen these acqui-hacks on Chrome extensions and Android apps where you get a widely deployed app or extension, somebody then buys it and turns it basically into malcode.

Gus Hurwitz: [00:34:48] And it doesn't even need to be buying. I think this is a really interesting liability challenge or puzzle here, especially for the open-source community. Frequently you'll have someone develop a widely used library five, six, seven years ago, and then they stop maintaining it because they move on with their life or they just get a job or whatever and they stop maintaining it. But it's still widely used. So then a couple years later, someone comes along and says, "Hey, give me the keys. I'm happy to take this over for you. It's still really important to the community, and I'd love to see it developed." And there's a lack of human capital here, a lack of resources. So it's unsurprising to see these libraries getting handed off to someone new. Does the original maintainer have some fiduciary duty or some obligation to do due diligence before transferring this intellectual property or the keys to these kingdoms over? If the answer is yes, that's imposing a great deal of potential liability on individuals who tend not to be sophisticated and resourceful legal actors in this area. They are developing these libraries because they're interested in programming and the technology side. So there's a really interesting and important, I think, legal question there, especially as we enter the third decade, fourth decade of the open-source movement's existence where a lot of packages, an increasing number of packages, are un-maintained. So this is a really interesting set of, I think, in many ways emerging issues.

Stewart Baker: [00:36:33] Yeah. It's going to be a big problem if you don't know who is actually maintaining something. You're in deep trouble because you know half the time they're going to say, "Oh, I don't need to be paid because I can fall back on my GRU salary." Last topic: Airbnb. This is apparently the international conflict episode of the

podcast. But Airbnb has now announced that it is going to refuse to allow Jewish settlers in Palestinian-claimed parts of the Levant to rent out their apartments. And it's done that essentially under pressure from Human Rights Watch, which was about to write a report siccing "social justice warriors" on Airbnb. Paul, there's a lot of legal liability issues floating around this one.

Paul Rosenzweig: [00:37:35] Well, I think that's right. I mean, in effect, Airbnb is having its own foreign policy. Let's leave aside the inconsistency of what they're doing and ask if they continue to operate in other jurisdictions that are even more significantly problematic with respect to human rights in Israel. Say, oh, Saudi Arabia where we murder journalists, or Russia where we invade foreign countries and blockade things. As a matter of law, now the question for Airbnb is going to be: How are they going to be affected by anti-BDS [Boycott, Divestment, and Sanctions] legislation in the United States, and what is their liability going to be for succumbing to that? Meanwhile, what is their liability going to be in Europe for failing to succumb to that? So they're kind of stuck between a rock and a hard place. And it's demonstrating yet again that international tech companies are kind of the pointy edge of the sword when it comes to conflict-of-laws questions.

Stewart Baker: [00:38:38] Yeah. I think that's all right. It's interesting. You know the US has had anti-boycott laws since the '70s, but this probably doesn't fall foul of that because the anti-boycott provisions were all aimed at the Arab nations' attempt to force countries to boycott Israel by using their oil wealth and saying, "You can't have contracts with us if you have contracts with Israel." This seems not to be a state-mandated decision and therefore probably isn't covered by any of the existing boycott laws.

Paul Rosenzweig: [00:39:14] That's true, but there are 26 states right now that have anti-BDS laws themselves. I'm sure Airbnb operates in some of those.

Adam Candeub: [00:39:26] I'm curious to know how Airbnb knows that the person renting the home is Jewish. Do they just say that they're not? Or do they have to

register? You know put a yellow star on their advertisement? I don't know, but to me that's the disturbing part.

Stewart Baker: [00:39:41] Yes.

Nick Weaver: [00:39:42] Or the other question is: How many places outside that would actually be on Airbnb? So they might just be accepting a little collateral damage and just geo-blocking the entire area.

Stewart Baker: [00:39:57] Yeah. There are plenty of occupied territories around the world, from Morocco to eastern Ukraine and Cyprus. And so if they want to be consistent about this policy, they're going to have to start doing some pretty fine-tuned decision making about who's going to be allowed on the platform. Okay. That finishes a really lively episode, Episode 241 of The Cyberlaw Podcast. Adam, Paul, Jamil, Gus, Nick, thank you all for taking turns and providing a lot of different points of view on this one. I'll encourage our listeners to send us comments for additional participants and interview subjects at CyberlawPodcast@Steptoe.com. Go ahead and follow me on Twitter for as long as I last. I'm @StewartBaker, and I usually try to put up the stories we're going to cover so that you can comment on them and tell me which ones you think we ought to discuss. And leave us a review on Apple iTunes or Google Play or whatever you use to subscribe to our podcast. Coming up we've got Jim Langevin, who is, as I've said before, one of the most thoughtful Democrats soon to be in the majority in Congress working on cyber issues. So we'll talk to him about what the future may hold for cyber in a Democratic House. Denise Howell of This Week in Law, which is like the oldest, longest, and longest-running law podcast, is going to be a special guest commentator coming up. Finally, show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio engineer; Michael Beaver is our intern; I'm Stewart Baker, your host. Please join us again next time as we once again provide insights into the latest events in technology, security, privacy, and government.