Steptoe

Episode 249: Black swans, black ops, BlackCube, and red herrings

Chris Bing: [00:00:08] This all kind of reeks a little bit of American foreign policy over the last 20 years, whether it's arming quasi allies, soft allies in the region, and then the negative consequences of that. Perhaps in the past, historically it was providing RPGs to an opposition group of a government that we didn't like and then ultimately coming back to bite us. Here it's the cyber element. We've now – we, speaking as US as a country but specifically the government – allow these licenses to go through, helped develop this capability, to a country that's helping in the fight against terror but perhaps doesn't have the same values or laws as the United States. And now this is the consequence. These are the side effects.

Stewart Baker: [00:00:57] [Music] Welcome to Episode 249 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, and I should say that any resemblance to the views of our law firm's partners, clients, and friends is purely coincidental. Today I'll be interviewing Chris Bing and Joel Schectman, reporters for Reuters who recently broke major stories about how the United Arab Emirates is using US persons – or has used US persons – coming out of the National Security Agency to do some of their hacking and spying, including in some cases on Americans. So it's a fraught story and a lot of fun. So welcome, guys.

Chris Bing: [00:01:43] Thanks for having us.

Stewart Baker: [00:01:44] It's a pleasure. Okay. And joining me for the News Roundup are: Phil Khinda, who is a partner of mine in the Washington and New York offices of Steptoe & Johnson; Maury Shenk, who advises Steptoe on European technology and

cybersecurity issues; Nate Jones, who was the co-founder of Culper Partners and a veteran of the Justice Department; Dr. Megan Reiss, who's a national security fellow at the R Street Institute. And I'm Stewart Baker, formerly with NSA and DHS, host and chief provocateur for the day. So, Phil, I asked you to come down here because there was a lot of coverage of the Yahoo derivative class action settlement for their breaches – $29 million – and some suggestion that maybe this was opening a brand new front in privacy litigation and that $29 million is not something to be sneezed at and perhaps it would change the approach of directors and officers to issues that they hadn't spent as much time on in the past. And since I know you were involved, that makes you a little cautious about what you can say. Can you give us some sense of how we should treat this? Is it a straw in the wind or a black swan?

Phil Khinda: [00:03:08] Happy to talk about it. And again I'm going to be a little bit careful given our role behind the scenes on a number of different sensitive matters for that good company. And first of all, thanks again for having me back.

Stewart Baker: [00:03:19] Yeah.

Phil Khinda: [00:03:20] I would call this one a red herring. And here's why: Yahoo doesn't exist anymore. And so it was acquired in parts by Verizon that combined it with its AOL business, now Oath. And then the Alibaba and certain related assets went to a new entity called Altaba. The liabilities flowed to Altaba.

Stewart Baker: [00:03:41] Because Verizon said, "We're not taking this."

Phil Khinda: [00:03:44] Right. And so I think what people should bear in mind when looking at the derivative settlement, when looking at the SEC settlement, was that the people negotiating the resolution were in a sense not the people whose conduct was being – and not the entity – whose conduct was being assessed. And so the incentives are different. What do they want more than anything else? Closure. Cost containment. And so if you can settle quickly in the current quarter to tell your investor base that's true and you can settle within the insurance constraints, that's the incentive. And you know

in my judgment – this is my opinion alone – I think they did it too quickly; in fact, I'd go on the record saying they did it shamelessly too quickly.

Stewart Baker: [00:04:22] So from their point of view, though, they just hold stock. Right? They're not in this business. They're not going to be repeat offenders. They're not going to have anybody's private data. So if they can get out of this, they don't have to worry that they're setting a benchmark for future settlements.

Phil Khinda: [00:04:40] At least not as to them.

Stewart Baker: [00:04:42] Yeah.

Phil Khinda: [00:04:42] And so it's everybody else's problem but no longer theirs. And so that creates a distinct odd incentive for them to say, "This is not us. This is not us trying to come to a resolution so we can continue to go forward unimpaired. We're not unduly impaired in some way either before the government or vis-à-vis our shareholders. Instead, what do we want? We want to never hear about this again."

Stewart Baker: [00:05:05] "We want out!"

Phil Khinda: [00:05:05] "And best of all, if we can get a release and do this within the bounds of our insurance coverage or with some nominal payment, we can have closure." What it does unfortunately is it leaves those of us who otherwise subject these tea leaves to almost Talmudic study – what does it mean going forward? Not that much.

Stewart Baker: [00:05:22] Yeah.

Phil Khinda: [00:05:23] Now will other plaintiffs' lawyers come in and say, "But *Yahoo*"? Will the regulators occasionally say, "But *Yahoo*"? Perhaps. Now on the regulatory front, I would predict a lot has happened since that settlement. The SEC itself has been the victim of a data breach. Interestingly quieting a lot of –

Stewart Baker: [00:05:39] Which does make you kind of humble.

Phil Khinda: [00:05:41] Indeed. And in Yahoo they actually did catch the hackers. And so that will temper, I think, part of it. On the plaintiff side, I think the same racket will continue. Will it come up? Yes. But I think for those in the know, it can be brushed aside.

Stewart Baker: [00:05:56] Okay. So that makes perfect sense. Take this with a grain of salt as a precedent. But you're gonna hear about it from the plaintiffs' bar. The key here is: what's the second settlement look like?

Phil Khinda: [00:06:12] Exactly. Let's keep watching.

Stewart Baker: [00:06:14] Alright. Thanks, Phil.

Phil Khinda: [00:06:15] My pleasure.

Stewart Baker: [00:06:16] That's terrific. Nate, I want to ask you because this is just a fun story about the efforts to take down Citizen Lab for their stories on NSO [Group], which is a vulnerabilities firm, I guess you'd say, in Israel, by running fake personas at Citizen Lab personnel to try to get them to say embarrassing things. What's going on there?

Nate Jones: [00:06:53] It's a good question. As you mentioned, Citizen Lab is a cybersecurity watchdog organization affiliated with the University of Toronto, and they've done some research and published some findings that has been critical of some pretty significant targets, including the Chinese government and including, as you mentioned, NSO for their role in exporting surveillance tools to, among others, repressive governments to spy on their populations. You know we've seen this for some time now where you have well-resourced clients seeking out former intelligence agencies to dig up dirt, gather information. It feels a little bit to me like it is, as you said, a little bit more focused on duping them into saying things that will undermine their

credibility in the public. A lot of people are sort of linking this to BlackCube, and I haven't seen any specific ties to back that up but –

Stewart Baker: [00:08:02] It's just the tradecraft seems a little familiar if you've listened to the discussions of what happened to Harvey Weinstein's victims. They had LinkedIn profiles. They had you know kind of acceptable but not very deep websites that you could go to check them out. But a pretty shallow cover.

Nate Jones: [00:08:27] Yeah. And you know we saw something similar in the case of the former Obama Administration officials who were also a BlackCube target in connection with the Iran Deal where they were trying to find evidence of corruption there. And you know in some ways, it also feels like this is not a terribly new phenomenon in the sense that it has elements of it that feel a little bit like James O'Keefe for Project Veritas where if this guy was indeed mic'd up and had a camera and was just looking for some salacious material that may be taken out of context to again discredit Citizen Lab.

Stewart Baker: [00:09:08] Yeah, but I got to say James O'Keefe had more of a flair about him. This poor guy. He's apparently holding what everybody believes to have been a camera pen and constantly pointing it at his target in a way that you never would with a pen, reading his questions off of cue cards. O'Keefe was really in character.

Nate Jones: [00:09:31] Yeah. No, I was going to say the difference is this is amateur hour. You know the Harvey Weinstein BlackCube effort seemed a little bit more sophisticated than this. As you said, some of the efforts by, among others, you know some conservative groups to pin things on people are a bit more sophisticated. This guy was a little bit bumbling and ended up stumbling out of a place and knocking over some chairs as he left.

Stewart Baker: [00:10:01] Well, I love the fact that the AP has reporters there at the table because they've been tipped off. They jump up and start asking him questions. He realizes he's blown. He leaves, and then he realizes he didn't pay for lunch. You know

I've got to tell you, I wouldn't have come back. [Laughter] I would have said on the way out, "Those guys from AP'll pick up the tab."

Nate Jones: [00:10:24] [Laughter] Yeah. You know Citizen Lab, to their credit, saw this coming a mile away. And it makes it all the more important for everybody in these positions to be more vigilant about suspicious investors who are reaching out to them out of the blue to throw money at their project. So be careful.

Stewart Baker: [00:10:46] Yes. If you think that just because they're polite and nice, the Canadians don't know how to play hardball, you have never played hockey with them.

Megan Reiss: [00:10:58] [Laughter]

Nate Jones: [00:10:59] [Laughter] Right.

Stewart Baker: [00:10:59] Okay. So another weird kind of mix of tradecraft failures and spying to discredit is something that came up in a Bob Mueller filing. And I don't quite know what to make of this, but maybe, Megan, you can give us enough background to evaluate this filing.

Megan Reiss: [00:11:29] It's a little weird. So basically what happened was Mueller turned over some documents to a Russian company that was indicted as part of the Internet Research Agency scandal. And they were hacked – or supposedly hacked – and these documents were released, and they were filled with fake documents to make it indistinguishable what was actually a real document or not. And with the goal of discrediting the Mueller investigation. So in some ways, it plays along with a lot of –

Stewart Baker: [00:12:10] It's the same old story. Here we are. It's 2016.

Megan Reiss: [00:12:11] It's the same old story. Disinformation campaigns in every way. But I mean it's interesting that they're trying –

Stewart Baker: [00:12:19] There's some doubt that it was a hack at all. Right?

Megan Reiss: [00:12:21] Yeah.

Stewart Baker: [00:12:22] The Russians, for all the naming and shaming we've done, it seems like they're proud of their hacking prowess. And they are pretending to have hacked documents that they've probably gotten a leak from the defendant in this case.

Megan Reiss: [00:12:36] Yeah. The hacker disappeared already. And my guess is this is a strategic leak and a disinformation campaign that looks just like all the other disinformation campaigns. They have some truth in it and then some fake stuff to discredit the US.

Stewart Baker: [00:12:53] Do we know what the fake stuff was?

Megan Reiss: [00:12:55] So they had a list to make it seem indistinguishable, so I think we more or less have to trust that some of these documents are fake. I do not believe that we know what was real and what was "junk material."

Stewart Baker: [00:13:12] Alright. I have to say, it reminds me of nothing so much as that Russian robot that had a guy inside. It's like, "Wow! We are great hackers! When Mueller turns over documents to us, we can release them." Oh, it's hackers! That's it. Yes.

Megan Reiss: [00:13:35] "We are excellent at our terrible jobs."

Stewart Baker: [00:13:39] Okay. So this I guess is annals in BS because from Russian BS to what I think of as Google BS: Google has announced that they're basically doing the same kind of law enforcement lockout techniques that Apple has been pioneering and then claiming that the impact on law enforcement is just an "unintended side effect." They're really trying to protect users from bad guys of other sorts, insider attacks from

Google. Maury, you're probably more sympathetic to Google than I am, but what was this flap about?

Maury Shenk: [00:14:22] Well, it's an update to Android that prevents Google or the operator that's running Android from allowing access to an individual phone without breaking their whole system, which is what iOS is set up to do now. I think whether you regard it as an unintended side effect depends how much you balance the risk of insider and similar attacks against privacy from law enforcement. It definitely has both effects.

Stewart Baker: [00:14:53] Well, yes and no. But if I remember, what this does is it says essentially that we cannot update your phone unless you enter your PIN number or your biometrics. So the updates show up and wait for you to activate your phone. So when is this a security feature? It's a security feature if you stop updating your phone, entering your PIN number. Well, when does that happen? It happens if your phone is stolen or if you are arrested and law enforcement gets access to it. The idea that there's going to be an insider attack from Google in which they have bands of people going out and stealing phones and then using their inside information to give them access to the phone for what purpose, it makes no sense to me. Unless they're paying their engineers a whole lot less than I think they are, the risk of that kind of attack is tiny compared to the possibility that the contents of a phone will be needed for law enforcement purposes.

Maury Shenk: [00:16:08] I mean I may not have a full technical understanding. I thought it was a broader limitation on the ability to install malicious applications by Google or Apple or the operator, but you may be right. If it's the latter –

Stewart Baker: [00:16:23] I'm sure there's somebody from Google listening to this. They can send corrections to CyberlawPodcast@Steptoe.com. I promise to read them or bring you on the show and you can argue with me. But claiming this is an unintended side effect is as much BS as the Russians claiming that they hacked Bob Mueller's server. Alright. Something a little more real, but maybe only a little more real: Apple had a FaceTime flaw that everybody heard about for about 24 hours, mainly because a 14-

year-old boy found it and couldn't find anybody at Apple who would respond to his effort to explain the flaw.

Maury Shenk: [00:17:08] Yeah, I don't see this one as such a big deal. I mean Apple shut it down pretty quickly by turning off group FaceTime once it came to broad attention. And it's a little bit hard to see how it could have been broadly exploited because you had to actually call the person who you would be listening in on. So maybe –

Stewart Baker: [00:17:26] And the fact that you were calling is recorded on the phone. So, yes. You got 20 seconds of commentary, and I suppose if you're the kind of person who picks up a phone and says, "Oh, that [censored] is calling me again," then you would be at risk.

Maury Shenk: [00:17:41] Yeah. I mean if somebody has their phone in their pocket and not on vibrate, then maybe you can do the unintentional pocket call, but that's not a major attack. So I see this is not such a big deal.

Stewart Baker: [00:17:52] Yeah. We've all gotten those calls, and in some cases, they've gone to voicemail. And I doubt any of us has ever listened all the way to the end of one of those because it consists mainly of [unintelligible garbled noise]. So yeah, it's not a serious privacy problem, which of course is why New York State is investigating it. Let me ask you about something I thought was more interesting and maybe spurred by the fact that Apple was taking on bad publicity for about 24 hours because very shortly thereafter, if I remember right, they announced that they were cutting off Facebook and then Google for what they characterized – or at least they allowed the press to characterize – as a big privacy violation of Apple's terms of service.

Maury Shenk: [00:18:40] Yeah, I think this one is a big deal. So Apple had granted Google and Facebook enterprise certificates that allowed apps to be installed on iPhones outside of the app store, so outside of Apple's whole app review process. That was supposed to be used for enterprise apps. Apparently Facebook was using it

broadly for internal apps. And both Facebook and Google used it for research apps with consumers gathering a whole lot of private information Facebook and Google maintained with appropriate disclosure. In Facebook's case, it involved information that would have been encrypted on the phone. Apple was very unhappy about this. It was a clear violation of the terms of service for this enterprise certificate, for which Google apologized. Facebook –

Stewart Baker: [00:19:27] Can I push back a little on that because the purpose of the certs [certificates] that Apple was using was to allow Apple to have much broader access than would ordinarily have to Apple activity for its employees – and of course its contractors. It has contractors working alongside its full employees, and I'm sure they're covered. And the people who were doing this were getting paid – not a lot, $20 a month or something – but they were enrolled in a program as testers under a contract with disclosure. I got to say, they sold their data to Facebook a whole lot higher price than I sell mine. And I wonder whether that's really a serious privacy issue. You kind of have to say, "Oh, yeah, but they couldn't possibly have known what they were doing. So they're idiots, and they got paid too little." And to say it's a violation of the terms of service means that Apple says, "Yeah, if you're only paying 'em $20 a month, that's not an internal use. If you were paying them $4,000 a month, it would be internal use."

Maury Shenk: [00:20:42] I don't know. It sounds to me like it was a clear violation of the terms of service. I mean I think the response that these people did agree to what they were doing maybe answers some of the privacy issues, although you know we've worried about that in other contexts like Cambridge Analytica. But I don't think it answers – I think it was clear that this was intended for use in enterprises, not for this use. I don't think Google would have apologized if it wasn't a clear violation, and their violation was not as broad as Facebook's. Apple is definitely taking a stand for privacy, although it probably doesn't mind poking Facebook and Google in the eye at the same time.

Stewart Baker: [00:21:20] Especially if it detracts from the attention to the FaceTime flaw that was trending until this one came along.

Maury Shenk: [00:21:28] Agreed.

Stewart Baker: [00:21:29] So, yeah. It's hard to know. It is pretty serious because you know using enterprise certs in the computer world is an essential part of cybersecurity and controlling your environment. And it's a little disconcerting to discover that when you're talking about phones you've got some third party with its own motivations that might say, "Oh, I'm sorry. You're not going to be able to use your enterprise cert for those purposes."

Maury Shenk: [00:22:00] Don't you just have to follow the terms of service?

Stewart Baker: [00:22:02] Yeah, well, as I say, I thought it was more arguable than you do. And I suspect that it was internally lawyered at Facebook and they said, "Yeah, I can justify that." Maybe they could, maybe they couldn't. I think having Apple say, "We decide what is a violation of our terms of service. And if you don't like that, how would you like not to be able to communicate with any of the other employees at Facebook? We're going to cut off all of those capabilities until you apologize to us," which is kind of what happened here. You couldn't get a lot of access to other apps that had clearly been designed for internal use because they took back the cert without a lot of warning, as far as I can tell. So I'm not here to carry water for Facebook, but it does feel like there might be a reality distortion field at work here.

Maury Shenk: [00:23:04] Yeah, well, it certainly was an overbroad response.

Stewart Baker: [00:23:07] So here's news that kind of stunned me: the repeal of Net Neutrality might be in judicial trouble. It was appealed. There was a five-hour argument at the DC Circuit. One of my partners [Pantelis Michalopoulos] was involved in it, arguing that the rule that the FCC put in effect basically doing away with the Net Neutrality doctrine should not stand. And at least two of the three judges seem to have been leaning that way, which surprised me.

Maury Shenk: [00:23:42] Yeah. I mean I'm a little bit surprised by this too. You would think that this was something within FCC's discretion. And the argument by most of the competitive Internet industry was they exceeded their discretion by characterizing ISP services as an information service, basically a content service, rather than a telecommunications service, which is subject to greater restrictions. And they drew a panel that has two Obama appointees. Of course, these were Obama FCC-era rules, and the panel seems to have been pretty sympathetic to it. So you know it's a bit political as [unintelligible] often are.

Stewart Baker: [00:24:21] Yeah, surprisingly. Yeah, well, I did hear the FCC general counsel might have been a little overconfident, as I probably would have been thinking about this. I said, "Well, you know if we have the authority to impose these rules, you'd think we'd have the authority to get rid of them." But they apparently wanted a big win and based their arguments on some broad principles that would give the FCC a lot of discretion in the future. And at least two of the three judges had some real problems with it. So it'll be a divided opinion it sounds like, but it's quite possible that this is going to get remanded.

Maury Shenk: [00:25:03] Yeah, although I think it would then be appealed to the Supreme Court, and I think there's a decent chance that cert[iorari] would be granted. And I think this Supreme Court would be pretty likely to defer to administrative discretion, so we could be watching this for a while.

Stewart Baker: [00:25:22] Yeah. I have to say, the relationship between the FCC and the DC Circuit pretty much defines familiarity breeding contempt. So if it got to a different jurisdiction, there probably would be a little more deference paid to what the FCC has done. Alright. We need to move on. But I wanted to touch on two or three stories. Nate, the Pentagon is supposedly falling behind to cyber threats. That doesn't strike me as news.

Nate Jones: [00:26:01] No, it really doesn't. Does it? Apparently this is tied to a report that may come out as early as this week. The conclusions aren't that surprising I guess

for people who follow this stuff closely, that the diversification and magnitude of the threats are outpacing our ability to defend ourselves. I think the critical question is going to be you know as the evidence mounts that this is the case, what is the straw that breaks the camel's back and forces policymakers to actually do something about that? And what exactly are they going to do? I'm not sure this will serve as that final straw. But it is an important voice in the conversation, and we'll see what the specifics of this report say when it comes out.

Stewart Baker: [00:26:52] Okay. Well, this week in dogs biting men, we've got another story: the Ukraine says that Russia is trying to disrupt its election. This is a surprise.

Megan Reiss: [00:27:00] Shocking. That is the entire story. We are all shocked.

Stewart Baker: [00:27:04] Yes.

Megan Reiss: [00:27:04] We'll just sit here in shock.

Stewart Baker: [00:27:06] Okay. There is something new coming from Japan. Japan has said, probably driven by the 2020 [Olympic] games, that they're worried about DDoS attacks from Japanese compromised IoT devices, and they're going to go and do what the hackers do, which is to try to log on to these devices using default credentials or maybe a list of everybody's most common passwords – 12345, monkey123. And if they get in, they're then going to tell the owners of those devices to fix their security. There's a little bit of flap from the usual Left-lib sources saying, "Oh, my god! That's going to hack their citizens," but this strikes me as perfectly appropriate. The question is whether they've really gone far enough because most people don't know how to fix their devices. And if Japan's going to log on to those devices, they might as well fix them too. But that they apparently are not ready to do. Okay. And last: EPIC [Electronic Privacy Information Center] and a few other NGOs filed a document at the FTC saying, "We know that you're looking at Facebook for violating its consent decree. We think they should pay $2 billion and be completely restructured and broken up, among other reasons, because of the 'algorithmic bias of the News Feed that reflects predominantly

Anglo, male world view.'" I have to say, this really feeds my prejudice about privacy law, which is that anybody can be found guilty, and the only people who are found guilty are people whose time it is in the barrel because they're being Twitter mobbed for everything anyways. This is just a kind of legal Twitter mobbing. And to say, "We'd like you to apply massive penalties for privacy violations against this company because of their 'Anglo, male world view,'" is just an illustration of how bankrupt privacy law is today. Not to mention, if you asked for a list of the 20 things that are problems at Facebook, I don't think that being too far to the Right would be on that list. Let's turn to our interview with Chris Bing and Joel Schectman. Welcome, guys. It was a fascinating story. This is the story of –

Joel Schectman: [00:29:56] It was a lot of fun.

Stewart Baker: [00:29:57] Yeah. Why don't you guys tell me the story as you wrote it up?

Chris Bing: [00:30:01] About four and a half months ago, Joel and I had been hearing rumors about Americans coming back from the UAE [United Arab Emirates] with pretty disturbing stories about the work that they'd done in that country. And the majority of Americans were former US intelligence officials who had been hired to essentially do the same job they'd been doing in the US but for the monarchy and to be working with UAE intelligence. It was through these stories that we learned more about the structure, the companies involved, what these former NSA officials were exactly doing. And that's what you see in the story that came out last week, where we revealed this thing called Project Raven, which was a program to work with UAE's NSA, which at the time was called NESA [National Electronic Security Authority], and to help them launch and create sophisticated hacking operations against a really wide range of targets, from rival foreign leaders to dissidents to human rights activists to journalists and then eventually, as we describe, Americans as well. So you had this ultimate terrible situation where Americans were involved in hacking operations against other Americans.

Stewart Baker: [00:31:02] Yeah. So it was a real slippery slope because, of course, when we have allies who are fighting terrorism, we want them to be good at finding terrorists, and so it would have made a lot of sense for the US government to say to the UAE, "You can afford to buy your own capability, and we will help you find people and provide export licenses so people can provide these services." So must've started with US company doing the same thing they'd been doing for the US government and in an allied cause.

Joel Schectman: [00:31:39] Yeah. I mean I think it's clear from reading the early documents of how this arrangement was created – for the Emiratis, actually, it wasn't called Project Raven. It was called Project Dread, just to give you like a –

Stewart Baker: [00:31:52] Like Judge Dredd? Is that the –

Joel Schectman: [00:31:53] They made this like kind of complicated acronym, but in the end they just wanted it to be Dread in an Austin Powers-esque flourish. But you know the creation of Dread, it was very much like that. It was like you know they had no cyber offensive capabilities in the UAE at all. And there was this idea that they had to buy them from outside and that in like five or 10 years of working with these like you know top-notch elite American NSA folks that they'd be able to catch up. And the idea in the beginning was really that it was going to be focused on counterterrorism, but like anything else, I mean you know once they were on the ground, then the national concerns kind of took over. And in the UAE, while terrorism might pose a greater kind of immediate threat – like the mentality there, from what I could tell, was that the biggest threat to the government, the biggest threat to the status quo, was something more along the lines of like an Arab Spring protest kind of situation.

Stewart Baker: [00:32:59] Sure. So when did this get started? Was it getting started right around the Arab Spring?

Chris Bing: [00:33:03] So we can trace it back to 2009-2010. Our story is really focused on 2014 and onward, which is when we have an on-the-record source in this

story, which I'm sure we'll get to, and it tells the stories sort of through her lens. And then on your question around how this was exactly organized under the US government, we were able to review export licenses that were given through the State Department to an American firm called CyberPoint, which is sort of the catalyst for a lot of this program, who had hired a number of these former NSA individuals and then brought them over.

Stewart Baker: [00:33:38] And that's clearly what CyberPoint should have done. This is governed by the ITAR [International Traffic in Arms Regulations] mainly because it would be considered intelligence –

Joel Schectman: [00:33:49] It's a defense service.

Stewart Baker: [00:33:49] Yeah. It's a defense service, and intelligence is covered by defense services. So you have to get a very specific license from the State Department – usually you get it from Commerce for a lot of this stuff – and they would have asked, "Well, what's our general diplomatic view of the UAE? How much do we trust them," etc. And if they licensed it with conditions and CyberPoint accepted those conditions and lived by them, nothing wrong, yet. Right?

Chris Bing: [00:34:17] Well, I think there's a few parts to this. Right? While you can say that there had been significant oversight in just the approval process for the license at first – and we had spoken to a spokesperson who said that human rights concerns obviously play into whether someone gets one of these approvals – the question is oversight over time. As Joel mentioned, once they got on the ground, perhaps the mission at first was counterterrorism, but it quickly morphed into all of these other things, whatever the client deemed the top concern.

Joel Schectman: [00:34:44] Yeah, specifically after like 2011 after the Arab Spring really started to take off, there was like a really great fear in the UAE that anybody who was talking smack about the monarchy in any way you know might be the next person who's like leading demonstrators in the street.

Stewart Baker: [00:35:01] And they did some kids.

Joel Schectman: [00:35:02] Yeah. It was like kids, like human rights activists, journalists, dissidents, and it really took like very little to get on that list, from what we could tell. It was like you know if you said something bad about them and they happened to see it, then you got on the list, and you didn't really like come off the list.

Stewart Baker: [00:35:20] So there was this journalist, this UK journalist, Rori –

Joel Schectman: [00:35:24] Rori Donaghy. It's kind of a fascinating little story because this guy, he was kind of just like a 25-year-old like any other 25-year-old. He got out of college, he wanted to get into human rights. He starts like this WordPress blog in London, and he calls it like the Emirati Center for Human Rights. But it was just a blog he had in London, and there was not like that many people who write on human rights in the UAE. So like you know he would be like high up on the Google search results, and for that reason, the Emiratis took him like deadly seriously. And it wasn't just – and I had never heard about this guy until the operatives told me that he'd become this like focus of their attention. He was like shocked you know. It was basically just a blog you know. And he just became this like source of obsession for them. I mean he was described by some people as being like the crown jewel of their surveillance efforts, was this like 25-year-old kid.

Stewart Baker: [00:36:15] That's fascinating. I saw, if I remember right, over the weekend a separate story on the fight over whether Qatar should be allowed to host the World Cup. And apparently there was an allegation that he [Rori Donaghy] was paid to write a hostile human rights report on Qatar, maybe by the UAE.

Joel Schectman: [00:36:38] That Donaghy was?

Stewart Baker: [00:36:38] Yes.

Joel Schectman: [00:36:39] This I missed. This is an interesting development.

Stewart Baker: [00:36:43] Double check my facts.

Joel Schectman: [00:36:46] That's fascinating.

Stewart Baker: [00:36:47] I always say I don't wanna be on the record until I know whether I'm right. Well, now that he's a big shot in the world of human rights in the Gulf –

Joel Schectman: [00:36:58] Yeah, he's a major target.

Stewart Baker: [00:37:00] He's found a way to have a second act. So, yeah. So they're out starting to do now targets chosen by the Emiratis, as opposed to purely terrorists. Is your sense that the US government doesn't know about that?

Joel Schectman: [00:37:19] Yeah, my sense is that they didn't know, and to be honest, that they didn't really care to know, because you know it's clear from reading the license agreements at the beginning that the activity they're going to be doing is some kind of surveillance-related activity. And it doesn't take like somebody who's a real expert in the region to know that at times where that's going to veer off into, and I don't think that they tried very hard to keep their finger on that pulse. That is the perception that I've walked away with. They just really weren't trying to keep up with this program. They made it very clear that you weren't supposed to be targeting Americans in the licenses. But beyond that, whether you go after a 16-year-old on Twitter or like this British guy, they didn't necessarily want to know about all that.

Stewart Baker: [00:38:06] And you can understand. They're in the business of saying, "Yes, you can have hand grenades. You can have rifles. You can have anti-aircraft guns." And you can't really say, "But you can't use it to shoot demonstrators in the street," because what are you going to do? You can't take it back, or if you do, you'll never sell another weapons system.

Joel Schectman: [00:38:26] I think you have to make a little bit of a distinction here because, yeah, it's an ITAR license, which also applies to anti-aircraft missiles and so forth, but like here you're actually talking about human personnel that are going in there, and you very much can tell human personnel what the ground rules are. Like they could have said you know the extent of this license is to be used against counterterrorism but not against human rights targets. I know that that's a very murky line, but you know.

Stewart Baker: [00:38:50] And let's introduce the woman that you talk to, who's willing to be named: Lori Stroud.

Joel Schectman: [00:39:00] Yeah. The brave soul.

Stewart Baker: [00:39:00] Yeah, that is brave, but she's hiding out, though, isn't she? She's in an undisclosed location?

Joel Schectman: [00:39:06] She's in an undisclosed location. I don't know "hiding." She didn't want us to like name it in the newspaper, but I don't know "hiding."

Stewart Baker: [00:39:15] So she shows up. She goes through this indoctrination into the program, and it says don't target Americans. And so she looks at them targeting reporters and the kids who criticize the regime and essentially says, "I guess that's okay."

Joel Schectman: [00:39:36] Yeah, yeah.

Chris Bing: [00:39:38] How she squared it was that some of these operations, they didn't feel good. She felt perhaps a little bit guilty about them. But she ultimately accepted and proceeded with them anyways because she said, "This is a different country. They have different national security priorities. We're here as essentially their guests, and they're our client and we'll follow them."

Stewart Baker: [00:40:00] "As long as we're not doing something that violates US law or license. They're paying."

Joel Schectman: [00:40:07] She's also used to being like an operator, an operative. And you know at the NSA, she understood there were certain ground rules, but within that, she kind of targeted the people that she was told to target there, too. It wasn't really her job to kind of morally vet it. And she didn't feel like it was her job when she got there either.

Stewart Baker: [00:40:24] And meanwhile, increasingly there are these locked rooms that just Emiratis go into to talk about stuff.

Joel Schectman: [00:40:32] Right.

Chris Bing: [00:40:32] So the program develops over time. That's right. While a US firm, CyberPoint, which I mentioned earlier, was a big part of this program originally, at a certain point, the Emiratis felt more comfortable with migrating the program to a domestic company called DarkMatter, which is based in the UAE. And it's around this time –

Stewart Baker: [00:40:49] BlackCube was taken?

Chris Bing: [00:40:50] [Laughter] It's like all these names are quite similar. And it's during this transition period that the American managers, essentially the architects of Raven and the early architects of the UAE's cyber programs, felt like they were losing grasp. They were losing the same control that they had on the program and its direction. And this is when they began to see things like "Emirati eyes only" lists, so targeting list assignments, specific missions, that they could not view, they could not access in the back-end software programs that they had. And this only further concerned operatives like Lori, who had come from the US, whose red line was targeting Americans.

Stewart Baker: [00:41:33] So CyberPoint at this point is out of the picture? Or are they supporting DarkMatter?

Joel Schectman: [00:41:38] No, they're gone. They're gone at that point. And around the same time, they're also starting to see like more evidence of like what's being described as "incidental collection." "There's a +1 [American] number here. Why is that in here?"

Stewart Baker: [00:41:50] +1 meaning as in 1 (202) ###-#### [Washington, DC].

Joel Schectman: [00:41:52] Yeah, exactly. "Why is there an American country code in here? This guy he seems like he's probably American. Why is he in the targeting list?" And it would be explained, "Okay. No, no. That was incidental collection. That was accidental. We're gonna purge it from the system. Don't worry, guys." And then we see the same name again like three months later. "I thought we put this guy on a list to not target and we purged him." "Oh, it was just a mistake again. Don't worry. Don't worry." Around the time, they're starting to see it kind of more and more, and you know she's [Lori Stroud] getting worried and other people are starting to get worried in the program too. And the reassurances that they're getting from DarkMatter were not the same type of reassurances that they would get from CyberPoint. DarkMatter is like, "No, no. It's not going to happen. You don't have to worry too much about it. And if it happens, it's not going to be you who's doing it."

Chris Bing: [00:42:41] And one caveat just to add there is that the majority of DarkMatter didn't know about this program. While it was organized under them and the paychecks came through the company, the work was still directly with Emirati intelligence. They weren't interfacing, for example, with DarkMatter personnel every day or executives.

Joel Schectman: [00:42:59] It was a contracting vehicle.

Chris Bing: [00:42:59] The nature of the program itself didn't change. They were still sitting right next to Emirati intelligence every day.

Stewart Baker: [00:43:05] So at one level, obviously there's a hydraulic pressure to turn this into a fully Emirati-prioritized program. You kind of say, "Well, jeez, what did everybody expect? What did the State Department expect? What did CyberPoint expect? What did Lori Stroud expect? They're paying for it. They know what they want. And if you give them the capability, they're going to do it."

Chris Bing: [00:43:33] Yeah. This all kind of reeks a little bit of American foreign policy over the last 20 years, whether it's arming quasi allies, soft allies in the region, and then the negative consequences of that. Perhaps in the past, historically it was providing RPGs to an opposition group of a government that we didn't like and then ultimately coming back to bite us. Here it's the cyber element. We've now – we, speaking as US as a country but specifically the government – allow these licenses to go through, helped develop this capability, to a country that's helping in the fight against terror but perhaps doesn't have the same values or laws as the United States. And now this is the consequence. These are the side effects.

Stewart Baker: [00:44:16] Well, so it's not just targeting of Americans. There's like a whole fad for hacking and doxxing the rulers of other countries in the Gulf. You know Qatar and UAE are cheerfully doxxing each other and the Americans who are under contract to them.

Joel Schectman: [00:44:40] Yeah. And it's quite a thing to hear some of these tales, stuff that they would discover on the iPhones of these various government leaders in the region.

Stewart Baker: [00:44:50] Well, you discovered that they were in the emir's own phone, right?

Joel Schectman: [00:44:57] Yeah, yeah. They were in his. It was like 20 or 30 of the highest ranking people in Turkey. I mean it's all over the region. Both sides of the Yemen war.

Chris Bing: [00:45:09] One thing you can say is that they effectively built this capability very quickly, and that's what we saw. Criticism aside, they were successful in building this very, very quickly, and they can thank Americans and the American government for doing that.

Stewart Baker: [00:45:23] Yeah. And the Americans who are on the receiving end of dox attacks from one side or the other may or may not have been doxxed by tools that were developed by CyberPoint. But there's a 50-50 chance, right, depending on which government just doxxed ya.

Chris Bing: [00:45:44] Yeah, it's hard to see where all the lines are. But you know this was surprising story for us. But at the same time, we talked to experts, and it almost feels less surprising.

Stewart Baker: [00:45:54] Yeah. There's nothing about this that is to me surprising except that it's public.

Joel Schectman: [00:46:00] It's funny you say that because I found it so surprising in the beginning when I found out that NSA people, they leave, they walk out the door of the NSA, within two weeks, they're doing the same spy stuff that they did for NSA, but they're working as like a mercenary for another government. Like for me, I thought that would totally be illegal, but it's not. For me, that was the biggest shock of the story. That was something that was totally like a known thing within the industry.

Stewart Baker: [00:46:25] The Gulf is a special world in that regard because they can't develop the domestic capability to manufacture and use all these weapons systems, so US contractors are selling them all kinds of weapons systems and capabilities. And by and large, the State Department says yes to that because they want to maintain

influence. This is just one more weapons system after a fashion. It's just a weapons system that is a little more likely to blow back on us.

Joel Schectman: [00:46:56] It's a human weapons system.

Stewart Baker: [00:46:57] Yeah. An intelligence capability –

Joel Schectman: [00:47:01] Well, what about the thing of these operatives though like taking these techniques that they've learned, real specific things on how you go about casing out these systems, and then taking it and using that spycraft for another country. For you, do you think that that's –

Stewart Baker: [00:47:21] So the question always is: what's the alternative? In this case, I am quite confident that the Chinese have systems that they could sell that are even more effective in some ways. And so you always have to ask, "Am I standing on principle that will just have no impact?" So I see – I should say the Obama – State Department's problem here. They were stuck, and they made the decision they made. And I'm not sure they were wrong. And they certainly didn't make it for the reasons that people would criticize Trump for. I think they just thought, "This is the best we can do. These guys are going to develop this capability, and we can shape it and we should. We should sell it to them and try to shape it, and at some point, we're going to lose control of it," just as they lost control of all the special forces troops that they trained at UAE. It's –

Joel Schectman: [00:48:22] "Maybe we can stop the worst abuses if we're there," or something like that.

Stewart Baker: [00:48:23] I think that's the theory. But I want to come back to Lori Stroud because –

Joel Schectman: [00:48:29] Fascinating figure.

Stewart Baker: [00:48:30] She left NSA to take this job, and she left for a reason that makes her the Zelig of cyberespionage. She's the woman who said, "We need to hire this guy in Hawaii, Edward Snowden. He's perfect for the job." It took her two months from the time she said hire this guy to the time she basically was told, "Hey, wasn't that you who wanted us to hire him?"

Joel Schectman: [00:48:59] [Laughter]

Chris Bing: [00:49:01] Yeah. It's another component of this story, as if it needed to be any more wild. Lori was one of the first people at Booz Allen working in NSA Hawaii to suggest hiring Edward Snowden. And it was her recommendation that was helpful ultimately in him being hired. Through this, he gained access to other systems, more classified information.

Stewart Baker: [00:49:23] Actually, he has said that "I went to Booz Allen so that I could get access to more stuff."

Chris Bing: [00:49:27] Yeah, that's public record.

Joel Schectman: [00:49:28] She likes to joke that she didn't get her referral bonus because he was there for less than three months.

Stewart Baker: [00:49:34] [Laughter] Yeah, I can see that would be one reason. That would be an over-determined result. So what does she think of Snowden now?

Chris Bing: [00:49:42] I think she doesn't view him well. I think at the heart – and you can see this throughout the story – Lori, more than anything, feels that she's an NSA analyst, that she loves the Intelligence Community, that she believed the counterterrorism mission –

Joel Schectman: [00:49:55] The culture of it.

Chris Bing: [00:49:56] Yeah, and she felt it was important. And with Snowden, it was particularly disappointing and hard to deal with because she felt like something she had loved, she was involved in hurting really, really badly.

Stewart Baker: [00:50:08] No other insights into his character? She probably didn't know him that well.

Chris Bing: [00:50:12] No.

Joel Schectman: [00:50:12] She said he was a very quiet guy.

Chris Bing: [00:50:15] Yeah, I don't think there was necessarily great knowledge of Snowden from her perspective.

Stewart Baker: [00:50:19] So the last topic I just want to cover is this is coming to light in part because there's an FBI investigation and has been for a while as the rumors that Americans were getting done by Project Raven started circulating. The FBI decided to open an investigation because of course that is a crime. What's the status of the investigation?

Chris Bing: [00:50:45] So we know as early as 2016 the FBI was investigating this program and the effects of it, and two FBI agents approached Lori at Dulles Airport when she was actually heading back to the UAE after some time home, asking her questions about the program. And we've spoken with a number of other sources who've described their interactions with law enforcement largely since 2016, which is, as you know, the time when DarkMatter came in and CyberPoint was falling out. And their concerns are in two parts. The first being, as you mentioned, hacking of US persons and US companies, and the second is more of a counterintelligence concern around the fact that you had so many cleared individuals, former US intelligence operatives, who –

Stewart Baker: [00:51:31] Who might have spilled what seemed to them insignificant bits about their past exploits. But if you have so many and somebody smart on the other side, you're going to end up with a data spill.

Joel Schectman: [00:51:48] Exactly. In aggregate.

Stewart Baker: [00:51:49] Yeah.

Chris Bing: [00:51:50] So it's one of these things where it's the type of investigation where it's not clear if charges are going to come to light. Perhaps it's only focused on the counterintel side of it. But as recently as this year –

Stewart Baker: [00:52:02] There sure is plenty of opportunity to bring criminal cases. They could bring criminal cases against DarkMatter, I assume, if DarkMatter hacked phones in the United States.

Chris Bing: [00:52:13] That's right.

Stewart Baker: [00:52:14] And everybody in management plus everybody who was witting – there's an argument that you're all part of the conspiracy. You don't have to know everything about the conspiracy to be part of it. So all the American contractors have at least some exposure.

Chris Bing: [00:52:33] Yeah, that's right. It's going to be really interesting to see where the case goes. And this is where I'll drop: if anyone is familiar with the case and would like to reach out to us, we're still investigating it. We're still investigating Project Raven and everything around it. And it's a fascinating case for all the reasons that we described today. It's one where the government was complicit, to a certain degree, in allowing this to happen in the UAE. It got out of hand, and now US law enforcement is cleaning up what was left behind.

Stewart Baker: [00:52:59] Yeah. Okay. Chris Bing, Joel Schectman, that was a terrific couple of articles. Let me ask you one more question completely unrelated to that story: how come good national security reporters are getting laid off these days?

Chris Bing: [00:53:17] That's a hard question. I mean I'm sure Joel and I each have our own opinions on this, but I think for a long time, the model for media has remained kind of stagnant and hasn't changed a lot. And news organizations have not found new ways to create revenue. And it's a failure of media executives at the very top for this. And as a result, there's been cuts. We've seen a ton of cuts across the industry in recent weeks, whether it's BuzzFeed, McClatchy –

Joel Schectman: [00:53:42] I think in terms of national security specifically –

Chris Bing: [00:53:46] And it affects that space too. But the other reason is that it's really, really hard. I'm sure you have your thoughts on this.

Joel Schectman: [00:53:51] No, no. Just in terms of like why – that's 100% true – but why national security reporters specifically? I think in a lot of organizations, those end up being some of the most seasoned and well-paid people.

Stewart Baker: [00:54:01] Yeah. So I suspect –

Joel Schectman: [00:54:04] So when you're trying to cut –

Chris Bing: [00:54:04] They come first. Yeah.

Stewart Baker: [00:54:06] And people had thought, "That's a niche where we can excel and people will pay for the content because it's unique. These guys have contacts that nobody else has. And so we'll build our brand around national security reporting." And it turns out that that isn't enough to sustain a brand.

Joel Schectman: [00:54:29] It's a real shame.

Stewart Baker: [00:54:30] Yes.

Chris Bing: [00:54:30] It is a shame. But I will leave this optimistic note at the end: there are new classes of reporters that are growing up in this industry right now who are quite good in national security and counterintelligence style reporting investigations, and so I'm hopeful for the future of reporting on this beat.

Stewart Baker: [00:54:47] Given that you've probably got 40 more years in this beat –

Joel Schectman: [00:54:51] You better be!

Stewart Baker: [00:54:53] You've got to be hopeful! Okay. Chris Bing, Joel Schectman, terrific to talk to you. Thanks again to Phil Khinda, Maury Shenk, Nate Jones, and Dr. Megan Reiss for joining me. This has been Episode 249 of the Cyberlaw Podcast, brought to you by Steptoe & Johnson. Joel, Chris, I'm going to give you our highly coveted Cyberlaw Podcast mugs.

Joel Schectman: [00:55:13] Oh, nice. Awesome. Thanks.

Stewart Baker: [00:55:14] So you can take those away, and anybody else who sends us suggestions for people we should interview who actually end up on the show will also get mugs. So since I nominated you, I've got enough mugs. But others should be inspired. I occasionally tweet my reaction to stories that are going to come up on the podcast. So if you want to follow me, @StewartBaker, on Twitter, you might see some of the stories, and I'm always happy to get comments there on whether my take is accurate. You can also send suggestions for people who should be here on the program to CyberlawPodcast@Steptoe.com. Rate the show. Please, rate the show. We need as many reviews as we can possibly get on iTunes and Spotify and Google Play and all of the other podcast aggregators. And I promise if they are particularly entertaining reviews, I will read them on the air. Show credits: Laurie Paul and Christie Jorge are the producers; Doug Pickett is our audio engineer; Michael Beaver's our

intern; I'm Stewart Baker, host and provocateur. Please join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.