Steptoe

Episode 242: Nobody Trolls Like the Russians

Stewart Baker: [00:00:04] Welcome to Episode 242 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking technology, security, privacy, and government. Today we're going to have an interview with Michael Tiffany, who's the co-founder and president at White Ops. I loved his bio. I went to look at this bio on a White Ops page, and it begins, "Michael Tiffany is the least talented person at White Ops." I have to say that's great. You go on to say you "hope to hire the kind of people who will awe you." So we're gonna be talking to him about a very complex and sophisticated adtech fraud case and a complex and sophisticated takedown. So welcome, Michael.

Michael Tiffany: [00:00:52] I'm happy to be here.

Stewart Baker: [00:00:53] Okay. And for our News Roundup we've got Maury Shenk. Maury Shenk is just back from Israel where he was commenting on the new Israeli cyberlaw.

Maury Shenk: [00:01:05] It was a very interesting conference, and the most fun part of it was there was a large group of people from the Israeli government and private sector who seemed to know about and be fans of the Steptoe Cyberlaw Podcast. So I felt like a bit of a celebrity. A particular shoutout to the guy at the Israeli Ministry of Justice – and he knows who he is – who claims to have introduced everybody to our program.

Stewart Baker: [00:01:27] This is great. Well, there is a law of cyberspace that because it's the Internet everybody's famous for 15 people. You apparently met four or five of the 15 that you're famous for.

Maury Shenk: [00:01:43] Yeah, exactly.

Stewart Baker: [00:01:44] Okay. And Dr. Megan Reiss, who is with the R Street Institute, Lawfare, the National Security Institute. Megan, welcome.

Dr. Megan Reiss: [00:01:52] Thank you, as always.

Stewart Baker: [00:01:53] And David Kris, co-founder of Culper Partners, former Assistant Attorney General in charge of the National Security Division at the Justice Department, and the only head of NSD who didn't work for Bob Mueller at one point or another. Is that right?

David Kris: [00:02:08] Actually that's wrong. When he was the head of the Criminal Division in 1992 at the end of the Bush Administration, I was an attorney in the Criminal Division. So I did in fact work for him, albeit at quite a distance.

Stewart Baker: [00:02:21] Alright. Bob Mueller: The Kevin Bacon of the national security world. And I'm Stewart Baker, formerly with NSA and DHS. The host of today's program. And I never worked for Bob Mueller either. Why don't we jump right into the stories? David, Apple was in the Supreme Court in a standing case, I guess it's fair to call it, over whether to keep the famous *Illinois Brick* case in effect. Can you give us a little bit more detail on what the Supreme Court was arguing about and why Apple cared?

David Kris: [00:02:59] Yes, I can, subject to the caveats that I am not an antitrust expert and I do have tech companies as clients, so people should take it with a grain of salt. This is a case involving the Apple App Store and app developers who put apps in that store and consumers. And as you know, Apple sort of runs a little bit of a walled garden. It's a closed system, and they get 30% of the price you pay for an app when you download it. And so, as you say, this is a Supreme Court standing case. App developers had tried to sue Apple, claiming that they were monopolizing the market for apps on iPhones. They had made no real progress, but then they added to their claims that they were app purchasers. So Apple is relying on the *Illinois Brick v. Illinois* case

from the Supreme Court in 1977 saying that only a direct purchaser, not others involved in the chain of production, can sue for antitrust violations. Apple is saying that the purchasers bought from the app developers, albeit through the App Store, and the purchasers are saying they bought it from Apple. And so there's just really a fundamental question here of who is buying what from whom. From reports of the argument – I didn't attend – it seemed as if the justices who can often be a technology challenged had a feeling from their own apparent uses of iPhones of some sympathy for the idea that this was a purchase from Apple since they sort of associated with Apple's App Store on their Apple iPhones. But reading the tea leaves at these kinds of arguments can be very difficult, and we'll see what happens when they go back and confer with each other and their clerks and actually have to write the thing to fit within existing antitrust law.

Stewart Baker: [00:04:53] Yeah, I think this probably – I mean, I think I was clerking the year that they decided the *Illinois Brick* case and it...

David Kris: [00:05:02] You're dating yourself!

Stewart Baker: [00:05:04] Oh, believe me, I'm getting the benefit of dating myself! So yeah. The case was sort of an Illinois attorney general saying, "Illinois Brick is charging too much for bricks. And we don't buy the bricks, but we build stuff. And we buy bricks from the guys who buy the bricks, and so we should be able to sue if there is some monopolization of brick prices as well." And it was obviously kind of double dipping. Here you've got a situation where everybody is running platforms. The platforms themselves are a mechanism for monopolization and for controlling both the buyers and the sellers. And I'm guessing that this is a much more complicated antitrust standing problem than *Illinois Brick* and likely to get a much more nuanced decision out of the court.

David Kris: [00:06:02] Yeah.

Stewart Baker: [00:06:03] Alright. We knew this was coming, Megan. The Trump Administration has finally woken up to the idea that maybe there is some leverage in saying, "We're not going to let everybody from China into the country, including people who look like they're going to steal secrets or build weapons when they go home."

Dr. Megan Reiss: [00:06:23] That's probably a good idea.

Stewart Baker: [00:06:24] It does seem like a good idea.

Dr. Megan Reiss: [00:06:25] Reasonable.

Stewart Baker: [00:06:27] Here's my prediction: We will have the most self-righteous, self-interested lobbying we have ever seen on this issue from the universities.

Dr. Megan Reiss: [00:06:35] Well, universities get the bulk of their money from foreign students who don't get any subsidization.

Stewart Baker: [00:06:41] And they have no shame when they lobby.

Dr. Megan Reiss: [00:06:43] Oh, yeah. Well, if your university is going to take massive pay cuts because the US government says, "Hey, we don't want the Chinese students to be stealing a ton of our intellectual property," they don't care so much about the second part. And I will say I was at the Reagan National Defense Forum this weekend, and China, cyber, and technology transfer were some big, hot topics. So it's right up there.

Stewart Baker: [00:07:08] It's nice to be on top of this. Exactly. Okay. So look forward to a fight because the universities will say, "Oh, this is our self-interest. This is our money. This is academic freedom. And on the other side just patriotism and the US economy and national defense. So obviously we win."

Dr. Megan Reiss: [00:07:31] Yeah. Something worth noting is that the stats on Chinese enrollment are up times six since 1999. So this is a large number of students putting in $60,000 a year. So it's going to be a fight.

Stewart Baker: [00:07:46] It is. So what the administration should be doing, it should be coordinating with the Aussies and the Brits and maybe the Germans to say, "Let's all apply a certain amount of scrutiny to the people that we're taking in as students."

Dr. Megan Reiss: [00:08:03] Yes, definitely. Especially when they have access to sensitive information.

Stewart Baker: [00:08:08] Yep. Okay. So let's try Russia for a change. David, I think it's now official: Everybody hates Facebook. Most of them hate Facebook because Facebook let the Russians do things in 2016, but now it turns out the Russians hate Facebook too because of what they're trying to do to make up for their mistake. This is a lawsuit by the Federal Agency of News [FAN], home of the trolling accountant that we talked about a couple of episodes ago, which has now filed a trolling lawsuit – what looks to me like a trolling lawsuit against Facebook. Is there any hope that this lawsuit is going to go anywhere?

David Kris: [00:08:49] Well, I don't know. It's going to generate some laughs if it does go anywhere. A jury trial has been demanded, and I'm sure it'll be fun to play this out in front of the jury. Technically, this the public accommodations and breach of contract case because FAN claims that the US government has more or less bullied Facebook into discriminating against Russians, including FAN itself. I mean, you know as to whether there's anybody left who favors you know sort of speech controls, look, subject to the same caveats as I made earlier, everybody thinks, I believe, that you know child pornography and so forth outside of the First Amendment oughtta come off these platforms and the government has passed laws requiring companies to report it in. Then there's a second group of speech involving non-First Amendment, but a lot of these platforms, for example, forbid adult nudity even though it wouldn't fit the First Amendment exceptions there. So this is a kind of a field where it may be easier to talk

about sex than violence, I guess. And I don't think even you, Stewart, sort of doubt that these platforms have an ability, pursuant to their terms of service, to knock off that kind of content and keep it out. The hard thing, I think, is the third bucket of speech which is stuff that isn't maybe in that second group but it's still icky and people don't like it – at least some people don't like it – and we're going to inevitably disagree on what the lines are and where they should be drawn and then we're also going to disagree about any particular application of those lines. Nominally, that's what's going on in this case. They're basically claiming, "We're innocent. We didn't do anything wrong. We're not part of the Internet Research Agency or any Russian governmental entity. We're just innocent Russian users who got swept up in this anti-Russian madness here."

Stewart Baker: [00:10:39] Under US law, do you get to sue over that? I mean, when I complain about discrimination against conservative speech, everybody rushes to assure me that the First Amendment doesn't apply to private platforms like Twitter and Facebook.

David Kris: [00:10:54] Yeah, and they're bringing a public accommodations and breach of contract case. They say they complied with the terms of service. They didn't do anything wrong. The fact that they're ethnic Russians whose audience is Russian users or people of Russian descent is not a basis. And they've complied with the contract. Facebook oughtta comply with the contract. And they can't be kicked off. So we'll just see about what discovery is like in this case, among other things, if it actually moves forward and see what the facts are.

Stewart Baker: [00:11:27] So yes. But you know if they really want to get to the "social justice warriors" of Silicon Valley, they should say, "Why this is discrimination on the basis of our national origin. This is racism straight up against Russians!"

David Kris: [00:11:41] They are more or less saying that through their public accommodations. And so you know this will be a fun one to watch.

Stewart Baker: [00:11:51] This will be entertaining. Yeah. Meanwhile, the Russians – they're such good trolls, they really are good – they've opened a civil case against Google for not censoring news in accordance with Russian law. And they're planning to amend their law, in modest imitation of the European Union, to say, "And if you don't do what we say, we're going to charge you 1% of your global revenue," which is a good deal because the Europeans are charging 4%. Maury?

Maury Shenk: [00:12:23] It's the flipside of what David was talking about. It's in his bucket of stuff that we think is illegal. This is an increasing thing we're seeing around the world is governments will have lists of illegal content which have to be taken down, and Google failed to sign up for the list. And under existing law, they can be fined something like $10,000 for that. So the Russians are trying to adopt a new law, as you said, but it's only 1% of Russian turnover, so it's really fairly gentle compared to the EU's 4% of global turnover.

Stewart Baker: [00:12:52] Oh! It's a bargain! Putin, you piker! Alright. They are also planning privacy legislation. They're going to protect the private information of all those GRU officers who were stupid enough to take Uber straight from GRU headquarters to the airport. Maury, is this just a standard privacy law turned into data protection for Putin's cronies?

Maury Shenk: [00:13:24] I think the Russians, like everybody else, think that they're legislating in a principled way. But you know we talk a lot about Europeans passing legislation that's anti-US tech firms. Sure, Putin does a lot to protect his cronies. So I'd say it's a mix.

Stewart Baker: [00:13:40] Well, so if the Europeans were passing GDPR in the hopes of protecting their adtech industry, it sure looks as though they, as I've said in other contexts, aiming at America and hit themselves square in the foot because European adtech firms, according to the press, are taking a big market share hit. And, Michael, since you know a lot about adtech, I'm going to ask you: This is what the press is

reporting, that there's been an enormous drop in European market share as a result of GDPR compliance costs. Does that sound right to you?

Michael Tiffany: [00:14:18] Yeah, it does. And you know I can think of two reasons, only one of which I'm cynical about. First, you just have classic regulatory capture phenomena. Really complex piece of legislation creates a complex landscape, so who's going to win in that environment? It's going to be the people with hiring power. Right? So it's literally going to favor the powerful. The less cynical explanation is that the really big platforms are and have been more heavily scrutinized, which means that they're just ahead of the game. They've been thinking about privacy and navigating through some super sticky situations for literally years now, and the effect of GDPR is to force a bunch of smaller players to catch up who hadn't had to grapple with this before.

Stewart Baker: [00:15:06] I would suggest a third possibility which is if you're buying or using adtech and you're suddenly worried that it could create liability for you, you're much more likely to want to buy from somebody you've heard of before than somebody you don't know well.

Michael Tiffany: [00:15:26] Yeah. So there's a flight to safety effect.

Maury Shenk: [00:15:28] We're certainly seeing this with our clients, moderate-sized companies, that need advice from us on GDPR while the big guys have in-house privacy lawyers who've been looking at it for years and percentage-wise, in terms of their turnover, it's much slower. I do think however that if these big fines, like the 4% of global turnover, some of the big guys could face serious pain under GDPR like they have with some of the competition fines against Google, for example.

Stewart Baker: [00:15:58] Yeah, but that's – somebody once described the FCC as in the business of nudging monopolists to do the right thing. That's my guess. Even 4% of global turnover would hurt, but it's not going to change your market position is my guess. This is actually a really interesting thing that will change ransomware's market position. The US has indicted some Iranians for ransomware, the usual yada yada. I

don't think they caught anybody, but what they did do is they persuaded Treasury to freeze the bitcoin. So what does that mean? Everybody who takes bitcoin in the future is on notice that if it comes from this address, it's tainted?

Dr. Megan Reiss: [00:16:45] That's my understanding. It's kind of an interesting way, and whether or not it works is a question. But it puts a lot of people on notice that if you are engaging with known violators of law – I mean, these are nasty guys who targeted hospitals with ransomware attacks. These are bad people.

Stewart Baker: [00:17:06] Those are the people who can't afford to be down for five hours.

Dr. Megan Reiss: [00:17:08] Yes. And then they pay the ransom. If you engage in transactions with folks known to be doing stuff like this, you're on notice from the US Treasury. And that's fantastic. Whether or not it works in this underground world where people have bought into this idea that we don't need to know who people are in order to engage in financial transactions, there's the question of whether or not it will be easy. But the fact that we're at the point saying we need to do this, I think is a really good move.

Stewart Baker: [00:17:40] Shoutout to Sigal Mandelker, who has done some really interesting stuff with Treasury sanctions.

Dr. Megan Reiss: [00:17:47] Treasury in general. Good job, Treasury, on a lot of stuff this year.

Stewart Baker: [00:17:50] Yeah. And actually, I think NSD plays a role in this because they also got Commerce to do some creative things with sanctions on companies saying, "Don't do business with this company because they're tied to espionage." David, you were at NSD. Do you credit this more to the regulatory agencies or more to NSD prodding them to do new things?

David Kris: [00:18:16] Oh, I'm going to give you the politically correct answer and say I'm sure it was a joint effort and all the best elements of federal power were brought to bear in a coordinated fashion.

Stewart Baker: [00:18:27] So can I then attribute this for the first time to you actually saying something nice about the coordinated effects of the Trump Administration?

David Kris: [00:18:38] Okay! Put me down for "good on coordinated, regardless of who's in the White House."

Stewart Baker: [00:18:42] Alright. Okay. So David, while I've got you, I have to ask you about this story about the guy who was heading down 101 drunk and passed out asleep in his Tesla on autopilot. And the cops drive alongside, and there he is snoozing away. And they have to figure out how to stop him. If I understand it, they had one guy behind, zigzagging across the highway to slow down 101, which is really hard to do. And then one guy pulled in front of him and said, "Well, the Tesla won't hit me," he thought, "If I slow down, it will slow down behind me. And then we can stop this car." My question for you David is: Is there any interesting Fourth Amendment issue in that entire scenario?

David Kris: [00:19:36] I'd like to say that I think probably not. It feels to me like an interesting technological question, an interesting methodological question about how they achieved a traffic stop. But it does sound like a Fourth Amendment seizure stop effectuated through the magnificent technology brought to us by Elon Musk. And I will say I would file this under the "don't try it at home" department because the technology of this autopilot is not yet advanced to the point where you can get drunk, pass out, just program your home address, and hope for the best.

Dr. Megan Reiss: [00:20:09] Well, you can.

Stewart Baker: [00:20:12] Yes, that's right! That's right. Yes, the Darwin Award!

David Kris: [00:20:17] It might be a little bit of an IQ test, but I mean, the police have in the past, for example, thrown tacks or spikes on the road to stop cars that won't stop. This feels like a more kinder, gentler way of doing it. And I think it was rather creative policing, and nobody got hurt and that's all good. And I believe he was seized as of the moment they started to block in his car. They're lucky that, as you said earlier, that the Tesla didn't change lanes and try to accelerate and pass.

Stewart Baker: [00:20:48] Yeah! Don't you think that's kind of a failing in the software? If I'm driving down 101 and all the lanes are open and the guy in front of me slows down, I want my car to change lanes!

David Kris: [00:20:59] Yeah.

Michael Tiffany: [00:21:00] Well, I have that car. It asks for confirmation from you before changing into a better lane.

Stewart Baker: [00:21:06] So here's my other question: Don't you have to hold on to it to keep the autopilot? What, was he handcuffed to the wheel?

Dr. Megan Reiss: [00:21:12] He was really – he didn't wake up during the seven minute interdiction!

Michael Tiffany: [00:21:16] He must've been leaning on the wheel.

Stewart Baker: [00:21:20] Oh, that's it.

Dr. Megan Reiss: [00:21:21] Oh! Wow.

Stewart Baker: [00:21:26] Snoozing on the wheel! Okay. Alright. Last question, just a question for Megan. What kind of internal debate do you think there is going on – and maybe external debate – at Twitter and Facebook about how to handle the Yellow Vest protests in France where there is violence, there's legitimate protest. There must be

enormous pressure from the Macron Administration to treat these guys as quasi-terrorists and threats that they shouldn't be allowed to organize. How do you think that's playing out? Is this Arab Spring or is this 2016 American election?

Dr. Megan Reiss: [00:22:04] My guess is they're treating it more like an American or European protest event where they're not going to try to shut it down just because there is a criminal element, although it's going to get harder and harder as they continue doing things like lighting things on fire, attacking the Arc de Triomphe, attacking an Apple Store which is kind of absurd.

Stewart Baker: [00:22:31] Oh, my God! No! Sacrilegious!

Dr. Megan Reiss: [00:22:31] It will be interesting to see what pressure comes to bear.

Stewart Baker: [00:22:35] Alright. Well, thank you all. We're going to turn now to our interview with Michael Tiffany, who is the co-founder and president of White Ops, which is one of the premiere firms that does security work on ads, basically aimed at stopping ad fraud. Michael, welcome.

Michael Tiffany: [00:22:56] Thank you.

Stewart Baker: [00:22:58] So I guess I think we should start by explaining how adtech works so that we can figure out how adtech fraud works. Because you know in the ordinary ad world, Procter & Gamble just says, "We'd like to run an ad in the *Wall Street Journal*, so we'll just go to the *Wall Street Journal* or maybe our advertising firm will go to them and say, 'We'd like to buy us an ad.'" That is nothing like what happens online where it's all multiple intermediaries. Can you explain the structure of the industry?

Michael Tiffany: [00:23:32] Yeah, with pleasure. So in that earlier model, depending on what you wanted to advertise, you found what shows or what magazines were popular with a particular demographic and then you placed your ads in those publications, hoping that the right people viewed it. Well, online ad sales still work on the basis of

circulation. If more people see your ad, then you pay more money. But instead of trying to reach people through particular publications as a proxy for the audience that you want to reach, now there are extraordinarily sophisticated targeting mechanisms such that when you load a Web page, an auction happens in the background while the browser is pulling down all the content that is a multi-party auction deciding what ads to show you. And the ads that you end up seeing are a function, of course, of what website you're at but also a function of your cookies and device IDs and a bunch of guesswork about what sort of person you are.

Stewart Baker: [00:24:34] So they know, instead of guessing the *Wall Street Journal* usually has rich people, you actually know this is a rich person – or at least they behave like a rich person online. And instead of the *Wall Street Journal* selling it, you get to sell your ad to somebody who has figured out what the characteristics of this, some intermediary who says, "Now I know who Stewart Baker is. I think he's a lawyer, and I think he's got money so I'm going to give him this ad."

Michael Tiffany: [00:25:03] That's right. So the exact market opportunity that led to these intermediaries is this: “P&G, I can give you the exact same guy who later in the day is going to be reading the *Wall Street Journal*, but you can reach him on this blog at a lower price. And you know what? That might even be a better time to reach him because you want to catch his attention not when he's reading the news but instead when he's reading about his hobbies.”

Stewart Baker: [00:25:29] Right. Okay. And the way this works, there are still publishers. They still have websites – *Wall Street Journal* or SkatingOnStilts.com. So there's a hole there for an ad.

Michael Tiffany: [00:25:42] That's right.

Stewart Baker: [00:25:42] And the person who actually decides what goes in that hole is a supply-side provider. This is a platform that says, "We have a hole. We have a

supply of holes. And as people come to the site, we will fill that hole with an ad that gets the highest bid in the auction."

Michael Tiffany: [00:26:09] That's exactly right. So that has led to, of course, amazing democratization because now you can target exactly what you feel like is the right audience across vast swaths of websites, which is wonderful. And it's presumably better for publishers because it means that the creators of content can open up those advertising holes to a much wider array of advertisers than their sales forces could possibly have reached by themselves.

Stewart Baker: [00:26:40] People that you would never run into, would never find advertisers who may pay a lot of money for a particular kind of reader, but they'll never come to the *Wall Street Journal* because you're charging a lot of money to reach a very wide audience instead of an even greater amount of money to reach a particular person.

Michael Tiffany: [00:27:01] Yeah. So the economic incentives for participating in these global auctions schemes is really quite large for both advertisers and for sellers. So as a result, in a very short period of time, the majority now of ad spending is spent online in these auctions.

Stewart Baker: [00:27:22] And you only pay if somebody clicks on your ad or if somebody goes to see your ad.

Michael Tiffany: [00:27:27] If someone views your ad. That's right.

Stewart Baker: [00:27:29] Okay. And so here's a highly instrumented environment in which lots of stuff happens very quickly. You can validate a lot of information about the people who are getting on your site, and yet it's full of fraud that depends on you not knowing some of those things. And that seems to be what this case that we're talking about today – the 3ve case –

Michael Tiffany: [00:27:57] That's right.

Stewart Baker: [00:27:58] Was getting at, that the people, mainly Russians who were engaged in that, had figured out a way to game the system. What were they doing to game the system?

Michael Tiffany: [00:28:08] Well, fundamentally ads are charged again based on essentially circulation. If more people view ads, the more money changes hands. So that means that if you can manufacture an audience that appears to be looking at a lot of ads, then you can make a lot of money. In fact, you can make more money doing ad fraud than you can from all the ransomware in the world, all of the spam campaigns in the world, really all of the banking account takeover attacks in the world because if you compromise real people's computers and you make them view more ads, you can make money this month and next month and the month thereafter.

Stewart Baker: [00:28:53] Forever because they really are real people.

Michael Tiffany: [00:28:57] That's right. That's right. Now this is an environment that, as we said, is very sophisticated, where everyone is trying to serve the right ad to the right person at the right time. Obviously, a robot is never the right person. So that leads to the question: Okay, so how can an industry that is hiring maybe the best data scientists in the world – there are few people working on self-driving cars, the rest are working on making advertising better – how can an industry filled with those kinds of ultra-smart people be duped by fraud? And the answer is that since this scheme makes so much money, it's attracted literally the best cybercriminals. I mean, if you're the best black hats in the world, you do the most profitable thing. Right?

Stewart Baker: [00:29:43] So I looked at this. They busted these guys. They say they made $7 million with this scheme with massive amounts of bots. Didn't seem like a lot of money.

Michael Tiffany: [00:29:53] I feel like a better way to put this is that the prosecution is ready to prove to a jury that at least $7 million was made. Like just because Al Capone went down for tax evasion doesn't mean he wasn't a bootlegger and murderer. In this case, the crime scaled really rather well, and the malware perpetrating the crime is actually really well-studied. Kovter, for instance, which was used by the 3ve operators –

Stewart Baker: [00:30:22] This is one of the malwares.

Michael Tiffany: [00:30:24] That's right. It's been around for years! Not only that, but Proofpoint, one of the partners in what we called Operation Eversion to take this operation down, had studied some of the threat actors behind 3ve. They called them Kov Core G and put together a timeline stretching back something like six years. What's really new here is consequences. See, for the most part, antivirus companies – really, all the good guys, as a global community we're cleaning up malware infections or trying to take down botnets, but most of the time it's just superficial. You can't make consequences happen for the operators behind the scheme because it's really hard to deanonymize them. Well if you catch them in the act, you can answer the question: Who benefits? And then law enforcement can follow the money, which they're extraordinarily good at, and that combination is pretty new in this world. And that's why even people in countries you don't ordinarily think about facing consequences for cybercrime were caught this time.

Stewart Baker: [00:31:36] So I was reading the indictment, and they clearly had wiretap orders on some of these guys because they knew what they were searching. So they said, "This guy was asked to solve a problem, and he immediately went out and did some Google searches and then brought back a solution." So there must have been intense coordination with law enforcement on this.

Michael Tiffany: [00:32:03] That's right. I'm told that this is the broadest, largest takedown to date. The working group is extremely large, and the nature of the way that both cybercriminal rings were dismantled – there was 3ve and also another scheme called Methbot – was really quite pervasive. So it wasn't just about taking down parts of

the infrastructure but actually really trying to unwind the networks. I don't know of any example that was this extensive.

Stewart Baker: [00:32:39] So one of the things that was interesting is that the fraudsters had spread their infrastructure. Some of the fake views were coming from compromised computers that had been infected with a variety of viral bot software.

Michael Tiffany: [00:33:00] That's right.

Stewart Baker: [00:33:00] And they'd been pretty careful there. They actually wouldn't run it if somebody else had already compromised the machine, if I remember right, or if they were running antivirus. So they were trying to stay under the radar.

Michael Tiffany: [00:33:16] To the extent that the malware had evolved to this level of sophistication, if they downloaded a website that had cryptojacking code, it would actually get intercepted and disabled because the cryptojacking code can increase the CPU on infected computer –

Stewart Baker: [00:33:35] Right, and your machine starts to run slow?

Michael Tiffany: [00:33:35] Which might tip off the victim! Exactly. So they would disable all of that so the ad fraud could keep running stealthily in the background.

Stewart Baker: [00:33:45] So really they were doing the user a big favor. It cost the user nothing to go to these sites and pretend to read them. From the user's point of view – the people who have the bad security – there's really not much risk in having these guys on your system, is there?

Michael Tiffany: [00:34:04] Our theory – the reason why we're spending so much time on ad fraud – is that there are only so many cybercrimes that really scale.

Stewart Baker: [00:34:14] Right.

Michael Tiffany: [00:34:14] Ad fraud is one of them. And the money that's made from ad fraud forms the buy side to malware innovation. This is the money that is spent on developing Kovter, on developing new rootkits, new bootkits. This money isn't going to just rainbows and puppies. And so if we can cut off the scalability of this crime, even though it might feel benign, it'll actually have a far-reaching effect on the pseudonymous criminal underground that pays for innovation.

Stewart Baker: [00:34:46] Right. Trying to take away the incentive to develop really sophisticated new attacks.

Michael Tiffany: [00:34:51] That's right.

Stewart Baker: [00:34:53] And part of that is to reduce the payoff, and the other part is to increase the penalties.

Michael Tiffany: [00:35:00] That's exactly right. What winning means is that we push down the payoff so far that a rational actor – because we're talking about super rational, honestly brilliant people – looks at the potential payout versus the cost and risk and they think, "You know, I'm going to pick a different game."

Stewart Baker: [00:35:18] So the other thing they did that I thought was interesting – well, they did multiple other things – they got a data center and registered hundreds of thousands of IP addresses and then used all the virtual machines in the data center to fake being users online or to fake being sites that had inventory – that is to say ad holes to fill.

Michael Tiffany: [00:35:46] That's right.

Stewart Baker: [00:35:47] And then other fake machines would come in and read the inventory while it was on the fake machine from the fake publisher. And so the only

people who are real in the whole transaction were the guys who were paying for the impressions.

Michael Tiffany: [00:36:03] That's right. The Methbot operators were running the whole scheme out of just a few data centers.

Stewart Baker: [00:36:12] So why did they pick a US data center? That strikes me as dangerous.

Michael Tiffany: [00:36:15] Right? Well, certainly there's some hubris involved here, but they covered their tracks in an extraordinary way that we had never seen before where they divided up all of the IP addresses they had under their control – over 650,000 addresses, that's an asset that by itself is worth millions of dollars – they broke it up into small blocks and forged entries into one of the root systems of the Internet.

Stewart Baker: [00:36:46] The BGP [Border Gateway Protocol]?

Michael Tiffany: [00:36:47] The RIRs. These are the Regional Internet Registries that keep track of who owns what IP addresses. Well, what they did is they made these small blocks look as if they were owned by ISPs across Middle America.

Stewart Baker: [00:37:04] And these were blocks that nobody cared about because they hadn't been used yet.

Michael Tiffany: [00:37:07] That's exactly right.

Stewart Baker: [00:37:07] Like HP used to have 1/16th of all the Internet addresses in the planet, and so they're obviously not using them all. And so they could they could pretend to be those guys for years without anybody noticing.

Michael Tiffany: [00:37:21] That's exactly right. So that was not a fast attack. They had to build that inventory up over time. First of all, it was breathtaking, but it was also a

source of fragility since they weren't using infected real people, since it was all synthetic, what we were able to do is simply publish the list of every address that they used, which blew them off the Internet the same day.

Stewart Baker: [00:37:49] Plus it's a trademark violation, which you know Microsoft has gotten a lot of traction out of saying, "If malware says 'Microsoft.dll' or has 'Microsoft' in it, that's trademark violation, and we can seize it and take away your ability to use it." So it seems to me, given the many ways in which they were supporting this, that taking it down must have required a lot of coordination. And indeed coordination with arrests.

Michael Tiffany: [00:38:25] That's right.

Stewart Baker: [00:38:28] Were you sitting there waiting to take it down for a week or two while they kind of made sure that everybody that they wanted to arrest was in a jurisdiction where they could arrest them?

Michael Tiffany: [00:38:39] Right, well, from the White Ops perspective, we're actually stopping bots doing ad fraud all the time, every day. Obviously the DOJ is not putting out press releases every day, and their timeline was totally outside of our control. But there was a particular day when it was time to dismantle all the infrastructure, and I believe that the trigger event was one of the arrests. So as far as law enforcement was able to dig in and ultimately get to attribution down to named individuals, then I think they were looking for certain movements and saw an opportunity to move. And at that time, multiple parts of Operation Eversion, including Symantec and Proofpoint and Shadowserver and multiple ISPs, all moved into action to take control of the C2 (command and control).

Stewart Baker: [00:39:42] Which I assume was all over the world, right?

Michael Tiffany: [00:39:44] That's right.

Stewart Baker: [00:39:44] Which meant that they needed cooperation either from big ISPs but more likely also government agencies.

Michael Tiffany: [00:39:52] That's right. Because the government is technically seizing those assets, and then once they're seized, then the name servers can be redirected.

Stewart Baker: [00:40:00] So as a legal matter, did the Germans recognize US seizure of this, or did they seize this stuff on their own? Do you know?

Michael Tiffany: [00:40:07] No, that's going over my head.

Stewart Baker: [00:40:09] Okay. Because it's easy for the US government to say, "We're seizing this asset." And maybe the Germans just go along because they know it's all for the good of the Internet, but I would have thought if the US government tried to seize an asset that was located in Germany, the German government would usually say, "Excuse me. That's our job."

Michael Tiffany: [00:40:31] Well, there was an extraordinary amount of international cooperation also evident in the arrests. The people indicted were from Russia, Ukraine, and Kazakhstan, but the arrests were in Bulgaria, Malaysia, and Estonia. And then assets, of course, in North America and Europe.

Stewart Baker: [00:40:53] So let me ask you the broad question to sort of put a bow on this: What does this tell us about the future of ad fraud, adtech fraud? Is this a sign that we're starting to get a handle on it, or is this us lifting a rock and saying, "Oh, my God! Look at that!" and spraying it with Raid but not necessarily solving the problem?

Michael Tiffany: [00:41:17] Well, when White Ops first started looking into this problem, we really did feel as though the victims had no idea that they were being victimized. So this was a crime that succeeds by going unnoticed and was hugely unnoticed. That's no longer the case. Now advertisers are aware of the risks of ad fraud, but the world was still light on consequences. So I believe this is a real turning point. As I said, what

winning looks like is when the profits are no longer attractive relative to the cost and the risk. And this is the first time we're seeing really major costs and risks at this level. And I don't think that this is an end so much as the beginning. An end certainly to 3ve and Methbot, but I think we're going to see more of this.

Stewart Baker: [00:42:09] So my guess on this is that the people who are most technically sophisticated about how the whole market worked weren't really hurt by ad fraud. Right? If you're selling clicks or you're running auctions and you're collecting fees, the fact that they're fraudulent transactions is bad for your reputation, but you still get paid for each of those transactions.

Michael Tiffany: [00:42:33] There's actually a subtle economic principle here that it's hard to see but is extremely powerful. Google was our principal partner on fighting 3ve, and one of the reasons why this is so very much in the vested interest of Google is that all this fraud has the effect of making it look as though there are more people watching ads on the Internet than there really are, which creates artificial oversupply. So if you've gone to all the trouble to get real human engagement, it actually sucks to be competing against fake because fake is cheaper.

Stewart Baker: [00:43:09] Right.

Michael Tiffany: [00:43:10] So if we can eliminate all the fraud, then literally billions of dollars go to the clean, honest players left standing.

Stewart Baker: [00:43:21] Right.

Michael Tiffany: [00:43:21] And so that's how we've been able to build such a coalition for the complete elimination because everyone who wants to live in that fraud-free future, because they believe they'd make even more money in that future, are allies with us in this fight.

Stewart Baker: [00:43:32] So it reminds me of the old saying by people like Procter & Gamble said, "Half of my advertising budget is wasted. I just don't know which half." With luck you'll be able to say, "Half of it is fraud, but I know which half and I can eliminate it."

Michael Tiffany: [00:43:48] That's how we'll win.

Stewart Baker: [00:43:50] Alright. So a quick question about White Ops: Are you going to have any more reports or events or speeches, or are there resources for people who want to know more about this that you'd recommend?

Michael Tiffany: [00:44:04] Yeah. We set up a landing page sharing an extraordinary amount of technical detail as well as partner materials at WhiteOps.com/3ve. By the way, "eve" is stylized as "3ve." There were three parts to it. So if you visit there, there's a lot of free pointers.

Stewart Baker: [00:44:22] I have to say, in my head I was saying "threeve" for the longest time. But yes it is "eve," but the first "e" is a three. Leetspeak, unfortunately.

Michael Tiffany: [00:44:34] We're hackers. What can I say?

Stewart Baker: [00:44:37] Yes, exactly. Alright. Michael Tiffany, this was terrific. Thank you so much for coming in.

Michael Tiffany: [00:44:42] The pleasure's mine.

Stewart Baker: [00:44:42] And it's a great introduction to really the darkest corner of cybercrime but one that if we could clean it up would give those guys in Russia an opportunity to find a better use for all those brains.

Michael Tiffany: [00:45:00] That's right.

Stewart Baker: [00:45:00] Thank you very much. Okay. That's Michael Tiffany, Maury Shenk, Dr. Megan Reiss, and David Kris. Thanks to all of them for joining us. This has been Episode 242 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Be sure to suggest a guest interviewee, and we'll give you a highly coveted Cyberlaw Podcast mug. Since I suggested Michael Tiffany, I'm going to give him the highly coveted Cyberlaw Podcast mug. And send those suggestions to CyberlawPodcast@Steptoe.com. You can watch our thinking about what's going to be on the next show by following @StewartBaker on Twitter for as long as Twitter lets me stay up, which God knows how long that will be. Please do leave ratings for the show and engage with the other reviewers. We're always looking for entertainingly abusive reviews. I'm hoping Jim Langevin, who is likely to be in charge of the House Armed Services Committee Subcommittee on Emerging Threats, which will have a lot of high-tech Defense Department policy, we're hoping that he will be on as the chair of that subcommittee, and if we're lucky and the Congress grinds to a halt on Thursday, I'll go and interview him. You usually can't lose money in this town betting that Congress will grind to a halt. Also Denise Howell, who had me on This Week in Law, which is the granddaddy of legal podcasts – I think they must be on episode 400 or 500 by now – she's going to join us, so we'll start talking about some of the topics that she usually covers on what is generally called TWiL. And after that, the Blockchain is going to take over the podcast again on December 17, so if you're sick of listening to me, you only have one more episode before the Blockchain takes over. And then we're gonna go take two weeks off for our usual Christmas break. There's a foot of snow on the Middlebury Snow Bowl. I will be there. If you're looking for me, I will be the guy wearing a jacket that I was once stopped by TSA by a woman who said, "Excuse me, sir. Did you buy this jacket in 1992?" and I had to admit that I did. So you'll recognize me right away. Finally, show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio engineer; Michael Beaver's our increasingly indispensable intern; and 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.