Steptoe

Episode 227: Defending against deep fakes with lifelogs, watermarks … and tatts?

Stewart Baker: [00:00:04] Welcome to Episode 227 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government. And today I'm joined by our guest interviewee Bobby Chesney, who is a law professor at the University of Texas School of Law, who co-hosts the National Security Law Podcast where he does battle every — it's very civil battle, but battle nonetheless — every week with Steve Vladeck, also of UT, and a founder of Lawfare. Bobby, welcome.

Bobby Chesney: [00:00:41] Thanks, great to be on the show.

Stewart Baker: [00:00:42] Yep, we're going to be talking about deep fakes with Bobby and maybe a little also the FISA document dump that came out over the weekend. Other participants include Maury Shenk, who is a lawyer and adviser on European technology and cybersecurity issues in London. Nick Weaver, a perennial favorite teaching at UC Berkeley. Welcome, Nick.

Nick Weaver: [00:01:04] Thank you.

Stewart Baker: [00:01:05] And Patt Cannaday, who's a Steptoe summer associate in our Washington office. Patt, welcome.

Patt Cannaday: [00:01:14] Good to be here.

Stewart Baker: [00:01:14] Okay, and I'm Stewart Baker, back from the wilderness more or less in one piece, formerly with NSA and DHS and hosting today's podcast. Maury, I

want to start out talking about what was certainly the biggest dollar news of the week, which is the $5 billion-plus fine that the European Union imposed on Google for its abuse of a dominant position in the Android operating system. We got some comments from people on Twitter. The president of course tweeted that he thought that this was evidence of Europe trying to take advantage of the United States and that it needed to stop. And a couple of other people: Saad Gul said well really maybe that's not such a good analysis considering this looks a lot like the Microsoft case, and Chain Security weighed in to say it's kind of ironic that President Trump is defending Google. So this has gotten a lot of commentary, maybe not so much deep law — probably because as far as I can see, the European Union's legal analysis so far consists of a two page press release — but Maury, did you dig into this in any detail?

Maury Shenk: [00:02:45] I think we're waiting to hear more, but the basic analysis does indeed seem very similar to what the Europeans did with Microsoft where it was about bundling Explorer with Microsoft Windows. Here it's about bundling Chrome and the Google search app with Google Play. One feels that in this case, like the Microsoft case, the Commission's a little bit behind the market, which is already — the market tends to discipline these kind of monopolies as it did for Microsoft. You know whether you think they're after the US, I think it depends upon where you sit. If you're Google, maybe. If you're President Trump, or dare I say Stewart Baker, you tend to have that reaction. Google's competitors like this, though. Many US competitors — and frankly there aren't that many big EU technology companies to go after about this.

Stewart Baker: [00:03:38] Well that's certainly true. If the EU was trying to help European technology companies, they'd have to have some first. Increasingly they don't. Like you, this feels like nostalgia for the Microsoft case and misplaced nostalgia at that. In the Microsoft case, you really couldn't as a practical matter use a PC without the operating system Microsoft supplied. And yet the EU says, "Oh yeah, there's that Apple thing, but that's completely irrelevant. We don't want to talk about it. We don't want to think about it. It has nothing to do with market share or dominance. We're going to define this case as a case in which you are monopolizing the Android operating system and other operating systems for phones that don't integrate the phone and the operating

system, therefore putting Apple outside of the relevant market." That struck me as artificial in the extreme.

Maury Shenk: [00:04:49] Yeah, I think so. Although, the FTC looked at conduct like this from Google in 2012 during the Obama administration and had similar concerns about this. Google does have a very big market share in the search market. And you know a lot of the competitors are concerned. There are other ways that people are — you know Facebook is starting to play a big role for search. This all may look very outdated — at risk of repeating myself — a few years down the road.

Stewart Baker: [00:05:27] Yeah, that would be my guess too. Although, $5 billion dollars? That's a lot on the top of the $2+ billion they hit Google with for — what was it — privacy last time, right?

Maury Shenk: [00:05:43] Yeah, we'll see. Google will be appealing for sure.

Stewart Baker: [00:05:47] Well, that's right. This fine is basically for having contested the EU's initial judgment. Basically the European Commission is saying, "You should have done it when we told you we thought it was a violation. You should have fixed it then. Because you didn't, we're going to charge you $5 billion," which is not exactly due process.

Maury Shenk: [00:06:12] Well, you know this is one of the areas where the EU I think is learning from the US with big fines. We've done it in areas like sanctions, and as we'll be talking about later in the podcast, ZTE was another case where big penalties was US practice, and I think the Europeans have taken a leaf out of our book.

Stewart Baker: [00:06:30] I think that's entirely true. The question then is: if you were President Trump — I realize this is going to be a bit of a strain on your imagination — but if you were President Trump and you really didn't like this, what would you do to prevent Europe from enthusiastically embracing this kind of fine-based regulation of US companies in the future?

Maury Shenk: [00:06:54] Well, I don't think President Trump's criticism of it as being improper targeting of US companies is the wrong way to go. I mean whether or not you agree with it, if you're trying — if you want to defend Google — our commenter from Chain Security said that seems a little strange for Trump to do it — but if you want to defend Google, I think he probably took a reasonable tack.

Stewart Baker: [00:07:16] Well, but that's just naming and shaming. That's not actually doing anything. So he's going to have to find something other than just tweeting to deter the European Union from this. I'm not sure...

Maury Shenk: [00:07:31] He does seem reticent about trade actions, so I'm sure he can think up something if he wants to do that.

Stewart Baker: [00:07:37] Alright, well maybe that's it. It will get rolled into the negotiations over automobile tariffs and the like. Okay. So one of the other things that happened this week, actually it happened at Aspen — I was there for it — was Rod Rosenstein announced the results of the Cyber Digital Task Force at the Justice Department. Patt, what would you say was the most significant part of that endless report — probably 150 pages?

Patt Cannaday: [00:08:12] So I think the entire first chapter sort of deals with the most pressing issue and something that's been on our TVs for a long time now. But basically it's entitled, "Countering Malign Foreign Influence Operations," but basically it boils down to Russia interfering in the elections and how to prevent this in the future. So that's basically the whole first part of the report and the most important part.

Stewart Baker: [00:08:41] I think that the rest of it struck me as predictable: Justice Department worries about technology, encryption, and the like. So the news: the new policy is the Russia election interference stuff. And if I'm reading this right, what really is new here is a policy about when the Justice Department will out foreign nations for interference. And some of the stuff is pretty obvious and would have happened anyway.

When we have to make an arrest, we have to explain why we're arresting these people. And we'll name foreign governments, if that happens. I thought the most interesting one on the list... Well first, they go out of their way to say, "We want to do this in a way that will not interfere with, will not be perceived as partisan, which is why we're setting limits around when we will and won't talk about who's doing this." But they seem to suggest — it's a little unclear — that they're going to go to the tech companies, especially social media platforms, Google, Facebook, Twitter, and tell them when they think they see some interference by foreign governments. And I get the sense that we're probably going to tell them quietly and not publicly and give them information that they weren't giving to the rest of the public so that Facebook and Google and Twitter could go push the bots and the fake profiles out of their platforms.

Patt Cannaday: [00:10:36] Right. That is absolutely what it looks like, and they have a whole bullet about alerting technology companies when they believe there's been some interference. I didn't see this maybe as groundbreaking, especially later they talk about the things that they've been doing all along — so the private industry notifications, the FBI liaison alert system — that are targeted already at private companies. So to me, this is sort of status quo, but...

Stewart Baker: [00:11:07] I think it implies a level of cooperation in trying to make sure that the private efforts to keep foreign governments out of election issues are reinforced by what the Justice Department is seeing through intelligence and law enforcement discovery. I don't see anything really groundbreaking here, other than that they now have a policy. And presumably these will be the Rosenstein principles for the next 15 years when people ask who can we talk to about this apparent the government interference. So the one question I have for the Justice Department is: if they're going to tell social media platforms we think there are some Russian bots or Russian actors, the expectation presumably is that the social media platforms are going to take that down, kick those guys out, and that's great as long as they aren't kicking out actual Americans. And I don't have a lot of confidence that social media is going to be evenhanded in the way they apply their policies because they have such a bad record of being evenhanded in US politics already. And so one question would be: if the Justice

Department is going to provide privileged access to this information, maybe they should say to the social media platforms, "We want to see how you're using this. We want to make sure that you are actually using this in the evenhanded way in which we're providing it to you."

Patt Cannaday: [00:12:49] Right. This doesn't go as far as to say as to constrict the companies themselves to follow sort of the same nonpartisan behavior.

Stewart Baker: [00:13:00] Yeah, it doesn't. And you know this is tricky because you can't tell private citizens what to say in this country. On the other hand, if you're going to give them something that you don't give the rest of the public, it's not unfair to ask how they're using it. Okay. So Nick, I'm going to ask you a question because I genuinely don't know the answer, but it feels serious. We've seen over the past six months or a year increasing number of hacks that are aimed at the deep structure of Intel and other AMD ARM chips which have gotten a lot of value, a lot of speed out of doing speculative execution, which is basically saying, "I don't know if you're going to actually need this, but I'm going to start on it anyway because I've got extra pieces of my silicon that aren't being used." And there's been a recent announcement that suggests that all of the fixes that people are trying to implement for those kinds of attacks are starting to fail. And I wonder if you could tell us: is that really true, and how bad is it?

Nick Weaver: [00:14:16] It's sort of true. So these are all side-channel attacks. So what happens is two programs running on the same computer, one tries to figure out some secret from the other. And what it comes down to is: switching between programs, we keep trying to make it cheaper and cheaper because we do that a lot, but it doesn't interact well with the speculative execution features. And so what you need to do is just do expensive operations every time you switch programs. And programs can be things like a Web page itself. And so we've seen this with Chrome. Chrome now actually has a really robust set of defenses that they just rolled out. And what it involves is really running every single Web domain as a separate program and using these very heavyweight operations, and it's part of the reason why Chrome takes up so much CPU, but you have to in order to get the isolation. What we've come to the conclusion is that

any sort of, any sort of history, any sort of speculation cannot cross programs. And so this means that every time you switch programs, you've got to empty out all your caches, all these little hidden caches like the branch buffer and everything else. And so for normal people, it's basically run Chrome and accept that your performance is going to go down for a little bit. But for us computer geeks, it's really fun to watch us tap dance madly on the lip of the volcano.

Stewart Baker: [00:15:55] Okay. So you're predicting that we'll be tap dancing there a long time and there'll be at least occasional eruptions.

Nick Weaver: [00:16:03] Oh, yeah. I think it's basically Fissure 8 at Kilauea right now.

Stewart Baker: [00:16:10] Oh, great. Okay. Alright. So we'll watch this space, and this looks like a big challenge for chip makers in particular, as some of the tools they've used to boost performance suddenly look as though they have to be cured by reducing performance.

Nick Weaver: [00:16:30] Yep.

Stewart Baker: [00:16:31] Okay. Let me ask you about a different topic. The House and Senate have been negotiating with the Trump administration over what to do with ZTE. As you all remember, ZTE had persuaded President Trump that it ought to be allowed back into business if it paid a big enough fine, a billion dollars plus something, and fired its board, fired some of its management, or reorganized its operations. The purpose of that all was designed by the Commerce Department in response to an export control violation where the company seemed to have been deliberately flouting US controls to sell US equipment into proscribed countries like Iran and North Korea. The Commerce Department came down hard on them, and it looked like it might put them out of business. They said you can't ever sell US company — or you can't sell, for the next five years, US equipment, and that meant they were just done. The president said, "No, let them pay the fine and undertake some of these other constraints, and they can stay in business. They can keep selling US products," which of course was good for the US

products as well. Congress had said bravely it was going to overturn that compromise. It looks as though Congress is not going to overturn that compromise. What Congress is going to do, is they're going to say, "If you do business with the United States, we don't want you to use ZTE — or Huawei for that matter — equipment," so they're going to regulate telcos — big telcos — indirectly. Looks like a pretty substantial climb down for the people who said, "No, we're going to get tough with ZTE." I don't know you're thinking about what the final impact of this will be.

Nick Weaver: [00:18:43] Well there's two things. There's the sales to ZTE, and I think the resolution is good. I'm in the camp of "let's sell to them all they want buy from us." The problem is this was — the sales to ZTE part was just totally blatant political grandstanding. And in fact it actually — the Senate language wasn't actually going to undo the death sentence. All it would do is force Trump to basically sign a statement saying ZTE has behaved in the past year, and they have in the past year. But we also know how well Trump likes signing certifications, even when they're true. As for the supply chain, that's essential. And I think it's perfectly reasonable for the US government to use its market power and say, "If you want to sell to us, include this stuff."

Stewart Baker: [00:19:42] Alright. Well it's going to be — this debate is not over, is my prediction. I want to talk — Bobby, I want to talk about FISA, but let's do two quick stories first. Maury, the EU and Japan have mutually agreed that each other's data protection law is adequate. This strikes me a pretty big deal because it means that data can move between the EU and Japan quite freely. And the real question will be whether Japan's law gets challenged in the European Court of Justice the way US law has been challenged in the past and probably in the future.

Maury Shenk: [00:20:28] Yeah, I think it's a pretty big deal. The number of countries that have this kind of deal with the EU is pretty short. The number of big countries is even shorter. It's Canada. I think Argentina. And you know it's a broader deal than the US has on the Privacy Shield, which is a smaller version of the same thing, but I think less likely to be challenged because Japan I think has a more of a national consensus

on data protection than there is in the US, and the Europeans are more likely to be happier about Japanese law than they are about US law.

Stewart Baker: [00:21:05] Yeah, that's probably right. Nick, I saw that finally all 50 states that were offered funding to improve the security of their election systems have finally taken the money. Does that mean we can relax?

Nick Weaver: [00:21:20] No, I'm really worried about the election in 2018, especially voter registration systems. That if I was Russia, I would take every contested House seat, get all the most Republican-leaning precincts, and just randomly de-register about 10% of the voters. That chaos would be horrifically spectacular, throwing the entire election's legitimacy into doubt. If I was an election official right now, I would be really worried.

Stewart Baker: [00:21:55] I think you're right that they could do stuff like that. It is also possible to come up with mechanisms for avoid — for at least countering that. You can have provisional ballots. Ten percent of the electorate casting provisional ballots would be really painful, but it certainly is doable if the state officials who are responsible for the election actually do their job. And that's really the question. They took the money. The question now is if they can do the planning that they need to do to make sure stuff like this doesn't in the end have an effect on the vote.

Nick Weaver: [00:22:34] Agreed.

Stewart Baker: [00:22:35] Alright, Bobby. The FISA document dump. It's basically three or four applications — maybe the first we've ever seen — applications for a FISA wiretap aimed at Carter Page, who was at least briefly associated with the Trump campaign and who according to the documents was believed by the Justice Department to be acting as an agent of the Russian government. Did you look those over, and if so, what conclusions would you draw from them?

Bobby Chesney: [00:23:18] I did look at them, and Stewart, I got to say you know I'm used to sparring every week on National Security Law Podcast with Steve, who comes at me from the Left, so I'm counting on you to play that same role here.

Stewart Baker: [00:23:30] Don't count on it!

Bobby Chesney: [00:23:34] Yeah, so I looked at it. Look, as you say, maybe the most remarkable thing about this is the very fact that we're reading five affidavits. FISA Title I applications you know normally never see the light of day. As I understand it, these were forced to be disclosed by court order through FOIA litigation that basically was premised on the idea that the Nunes memo — the HPSCI majority memo — had made sufficient disclosures to prevent the government from being able to withhold the stuff. So the government resisted and resisted, but finally it was the end of the period for disclosing it, so they produced it. And naturally everyone's focused on the political context for all of it. That's the nature of this story, unfortunately. I think that the most important takeaway, from my perspective, is something that doesn't surprise me at all and that is that the attempt by the HPSCI majority report from Nunes to make it seem as if the FBI had effectively defrauded the court by not disclosing that one of their primary sources — Christopher Steele information — was a bunch of opposition research paid for by the Democrats. We already knew from the HPSCI minority response to the Nunes report that probably there was some disclosure. There was a reference to it being in a footnote. Now you can see in the document that there's pretty extensive disclosure, maybe not quite as robust as it ought to have been in an excess of caution. But it's pretty clearly disclosed, so that's confirmed. It's a pretty big black mark on the HPSCI majority report. But there's other stuff. There's a lot of kerfuffle out there about the fact that there are a couple of references to some Yahoo News article where the source for the news article was also Christopher Steele. And if you look on pages 22 and 23 of the first FISA application in this batch of documents, you'll see in the unredacted portions some of what was going on there. And there's no question that there is a footnote that references back to source number one, but it's not clear in the text — I think it's not sufficiently clear in the text that source number one and the source in the article are one and the same, so that's something that should have been done clearer. That said,

there's a big chunk of redaction where maybe there was such disclosure, and that's the problem with trying to draw conclusions from this entire document. I mean there are huge swaths of redaction. We don't know what other stuff was put forward by the FBI to build their probable cause case. Clearly the Steele dossier is a big part of it, but there may well have been a lot of other stuff, and you just can't tell.

Stewart Baker: [00:26:14] Yeah. As far as its implications for Nunes, I agree with you. The Isikoff-Yahoo News thing is a little ambiguous. I have to say I think the mainstream press has been doing a sack dance over Nunes saying this shows that his presentation wasn't accurate. It's not that it wasn't accurate. It's that it was lawyerly in maybe the not entirely reputable sense of that word. Everything he said was true. It might have left impressions that weren't true which were corrected by the reply brief of the Democrats on the committee. But I didn't see anything in here where you could say this shows that what Nunes says wasn't true. It's just that the impression he left might have been overdone.

Bobby Chesney: [00:27:10] I guess it boils down to the intent. I think the intent of the impression he left was very much to make it seem the FBI was engaged in your proverbial "witch hunt," etc., and I just don't think the facts bear it out. But I guess the real problem, the larger public policy problem, is that we count on the Senate and House Committees on Intelligence to be these proxies for the public overseeing the intelligence community, and in order for that to work at all, there does need to be some degree of trust that they're carrying it out in a nonpartisan way. And once we're into a conversation about how the majority is going to report and then there's litigation-like reply, and there's sort of these two efforts to spin things. I think HPSCI's in tons of trouble. And the contrast with the Senate Select Committee which has I think behaved itself quite admirably is quite striking.

Stewart Baker: [00:27:57] Yeah, absolutely. I guess I will say one thing that bothered me about this — or a couple of things. One, the amount of reliance on ordinary press reports — quite striking how often they just said well this is what is in the media. You know it's hard. They can't ignore that, but they can't be absolutely sure it's true, and they

certainly can't sure it isn't spun. Every one of these for a period of about a year included that story about how the Republican platform was changed to be more Russia friendly as a result of the intervention of Trump forces, which is a story that's highly contested and probably wrong. There were some changes, but there were changes to somebody else's proposed amendment, and they were modest and ambiguous. What I find striking is that having run that report, they never corrected it. They never said that it's been contested in any way. And since the question — you know it was only in there to show that maybe Russian efforts to influence the Trump campaign were succeeding. The fact that maybe it turned out not to be true should have been part of later submissions to the court.

Bobby Chesney: [00:29:29] Yeah, I wouldn't disagree with that. I would say that that's probably — if there's a weakest spot, that may well be it right there. I also think it's a very tiny piece of the much larger puzzle, even if we don't account for all the redacted stuff.

Stewart Baker: [00:29:42] Yes.

Bobby Chesney: [00:29:42] One of the things that's sort of striking because we get this — it's a set of four total applications, so you've got the original and three renewals, and they grow by leaps and bounds as time passes. Now, who knows what that reflects? It's all redacted. We don't know, but I think it's a reasonably safe inference to what's going on is that once the tap is in place and they're collecting on him, they're getting stuff that they think is relevant enough to put into the next round of renewal application. It's my surmise that you know by time you're into this, whatever influence that initial reliance on a news story, for whatever marginal impact may have had, is pretty well drowned out, I suspect.

Stewart Baker: [00:30:20] I think you're right. You can't tell much because what he says on the phone when he's being tapped is an increasing piece of this. I do also have this feeling that if this had been a proposal to wiretap the ACLU or somebody who was active in the ACLU as opposed to somebody who was active in the Republican Party, I

think alarms would have gone off at the top of the political elements of the intelligence community, and they would have pressed questions like: is there any bias in that article? Or really, you're right. They disclosed that the FBI speculated that there was a partisan motive for the information being collected, but they were not exactly pushing that forward so that the court understood just how much risk there was that they were being utilized in a partisan fashion. And I think it's a blind spot on the part of Obama Justice Department and intelligence community leadership not to have really said, "This could be very bad if we are asking the court to do something that could be later portrayed as partisan, and we need to scrub and disclose anything that might suggest a partisan motivation." And that just does not seem to have occurred to them. They just let the process grind out in its usual way, and it produced that footnote in which you have to already know the facts to understand it. Nobody who read that without understanding what was going on already would understand all of the identified persons and the speculation and the like. You will only get a kind of vague impression. You don't get the sense that this was research paid for by the other party.

Bobby Chesney: [00:32:32] Hey, maybe this is the much improved version. Maybe there was an earlier draft that wasn't as cautious as this.

Stewart Baker: [00:32:39] Could be. Could be. Well Steve Vladeck, we miss you. We know you're listening, and we know it's just driving you crazy not to be able to respond. I will come on the National Security Podcast sometime, and you can have at me.

Bobby Chesney: [00:32:56] Oh, that is so true.

Stewart Baker: [00:32:58] Alright, well let's move right into our interview and talk to you about deep fakes. You've got a great paper, very thoughtful, a little too law-y for my taste, but you wrote it with Danielle Citron. It's on deep fakes. I, of course, was attracted to this topic because traditionally we try to find any element of sex that might be associated with national security law or cyberlaw, and we've discovered that deep fakes, which are were originally people putting famous faces on folks engaged in a variety of porn activities for — I didn't even know this was a thing, but apparently people

like to see famous people going at it. And that has led you to a much more thoughtful discussion of what deep fake technology might mean more broadly, so why don't you tell us in a couple minutes what the basic theme of the paper is.

Bobby Chesney: [00:34:05] Great. Happy to do it. You know, as you said, this is coauthored with Danielle Citron from University of Maryland, who's just amazing, and I'm sorry she wasn't able to join us for the call, but it very much reflects both her ideas and mine. Danielle comes from a privacy perspective, and a lot of her work is focused on the impact of technology on women online, in particular harmful impacts in a variety of respects. And then of course I come at things from a national security perspective. And at some point back in the winter, we were comparing notes on disruptive technology trends and what they meant in our two areas. And we saw the intersection here with deep fake technology. So let me explain what we do in the paper — and by the way, for listeners who actually want to read the paper, it's easy to find if you Google for "SSRN deep fake," you'll find it. SSRN's an acronym for a paper repository, and it's freely available there and we welcome comments.

Stewart Baker: [00:34:58] And it really may be the second-most loathsome paper repository on the Web. It's just almost impossible to use easily.

Bobby Chesney: [00:35:08] It really is a pain, isn't it?

Stewart Baker: [00:35:10] It's unbelievable.

Bobby Chesney: [00:35:11] If you go there, don't be deterred by Stewart's very fair description. There's an orange button for "Download Paper," and you can get it for free there. So we make a set of claims. We make three sets of claims. First, pretty I think non-controversial descriptive claim. We simply describe the disruptive technology at issue here: altering audio or video content digitally to advance a lie, to make a fake appearance that someone said or did something they never said or did. And more specifically, since that capacity in general has been around a long time, we talk about how there have been specific recent advances to make this possible to do in a much

more persuasive and compelling and harder to detect kind of way. Okay, so that's the first claim. Second claim is a set of predictions. We predict first of all that this capacity, both the lower end and the higher end capacity to make deep fakes, is going to diffuse rapidly. And then we predict that this use — there will be some beneficial uses, yes, some artistic and political expression, for example — but there will be this whole slew of harmful uses, and that's the heart of the paper where we provide sort of a rogue's gallery, a parade of horribles of things that might happen at the individual, organizational, and societal, indeed international relations level, in harmful ways. So you've got harms to democracy, to national security, international relations, but also exploitation and abuse of individuals, sabotage of business rivals, sabotage of personal rivals, the whole thing. Some of this depends on the magnifying and distorting effect of social and broadcast media, but not all of it does. Some of the worst harms we anticipate will involve very private and discreet targeted distribution of a fake, and then others will depend on the social media magnifying lens and cognitive biases and the way people pass around information that's not reliable. So then those are our first two claims. The third and last claim is really a survey of the various tools from technology, law, behavioral, or business innovations that might be brought to bear — or in some cases we predict will be brought to bear — to mitigate some of these harms as they start to emerge. And we conclude on a pretty negative note that there is no silver bullet solution. We have some ideas about things we think could be done and some things that we think will be done that there we're not sure should be done, and we leave it all there to start a conversation.

Stewart Baker: [00:38:47] Alright, well let's start the conversation with a confession. I almost moved this entire field of technology forward by about four or five years because when I was in government, which was about 10 years ago now, if you remember, bin Laden was releasing these videos from time to time inspiring the troops — was very low tech compared to what ISIS was able to do, but it was a big problem — and we didn't have a good way to stop it or counter it. And I tried to get my staff to agree that we should offer a $50,000 prize for people who could send us bin Laden videos, and that we would give the $50,000 to the most persuasive one. And the way that we would

know it was a fake is that three-quarters of the way through, he needed to use the word "kumquat."

Bobby Chesney: [00:37:39] Did you get any good ones?

Stewart Baker: [00:38:50] My staff persuaded me that that was maybe not the best idea, and probably it wasn't because then I would own all these deep fakes. It would be my policy decision that brought it on them, and so you know I at least survive with my reputation, such as it is, intact. But it was clear even then that there were going to be opportunities to do this and that there would be — if we could do it in certain circumstances, it would be great for us — and in many other circumstances, it would be really bad for us. So I agree with you completely. Nobody is going to feel sorry for bin Laden if he ends up looking like a kumquat fan. But it's easy to imagine this being used by foreign governments in ways that are devastating to the US politically and in terms of international reputation. So that takes it I think pretty quickly to the question of what should we do about it. And you're right. Your list of ideas for what to do about it, especially the law ones, strike me as you know working pretty hard to drag law in. The real problem with bringing law into it is we aren't going to know who did it, and if we don't know who did it, it's kind of hard to bring legal consequences.

Bobby Chesney: [00:40:21] No, that's right. I think that one thing that's important to emphasize is it's not like some of the most malicious uses would be legal uses as things currently stand. I mean there's all sorts of state common law torts...

Stewart Baker: [00:40:33] Oh, yeah.

Bobby Chesney: [00:40:35] ...intentional infliction of emotional distress and all sorts of — all sorts of ways to police this. And the real challenge: if who you want to target and suppress is the creator of a really malicious and harmful deep fake, you've got the tools, you just aren't likely to catch that person. I mean in some cases, you will. It will be possible just as it is now, but for some of the things that we really want to be concerned with — you know the things that are of interest to you and I, Stewart, like national

security concerns, the way that you might deploy this for covert action purposes if you're hostile to the United States — state tort law is probably not the tool that you need to turn to. Now as you point out, this stuff's been around for a while. I want to emphasize what's different now because I imagine some listeners are thinking, "Hey, Photoshop's been around forever. Alteration of image and audio? That's nothing new. Just get an impersonator, etc." So perhaps a quick word on the technology advance underlying all this, and it has to do with the application of deep learning techniques to existing ideas about using neural network pattern recognition algorithms. What it boils down to is increases in computing power and in the algorithms associated with neural network processing have both created a much more robust capacity to create a neural network that can sort data and produce coherent patterns and then reproduce and then alter and reproduce those patterns, and then best of all — or worst of all, depending on your perspective on this — the idea of pitting two of these against one another so that they just iterate rapidly back and forth with one creating an image or video or sound and the other attempting to detect it and then going another round to improve from there. So they call that generative adversarial network, or GAN, methods. That's a 2014 paper from Ian Goodfellow and others that pioneered this idea, and a ton of academics and private sector entities have taken this, and they're running with it and making pretty rapid strides in creating a high-end, very difficult to detect, very persuasive looking set of fakes that's beginning to match what previously you'd have to go to a Hollywood studio to achieve.

Stewart Baker: [00:42:45] So it makes perfect sense. It's evolutionary in a sense. You create the fake, and then you say, "Let's use our most sophisticated techniques to find out whether it's fake." If we find it's fake, then it's up to the program that created it to find a way to fuzz all of the telltale clues. And then you send your attacker back in to try to figure out whether it's a fake and how to prove it. And each time the ability to identify the fake depends on you know fewer and more tenuous handholds on the topic.

Bobby Chesney: [00:43:24] Exactly. And even though obviously most of us can't deploy the GAN, or generative adversarial network, approach yet, we argue in the paper this is gonna diffuse, and it will diffuse. It'll diffuse pretty rapidly, and over time there'll be

a spectrum of tools out there that people can get their hands on to try to use this stuff and people you can hire to do it for you. Some of it will be better than others, but at the high end, it will be difficult to detect.

Stewart Baker: [00:43:49] So let's talk about what could be done. I thought there were two interesting approaches that you touched on. One is reputable sources will begin to say, "This is from me, and you can tell because at the end of the video I've hashed the video and signed it with my private key and therefore you can be sure — as long as you want to look up my public key — you can be sure that this is the product of my studio, my camera."

Bobby Chesney: [00:44:25] Yeah, you can guard against somebody sort of usurping your brand — the Louis Vuitton problem, if you will — with that sort of thing because if you're a sufficiently well-resourced generator of content — whether it's you know a national political campaign or somebody in business — you can do just what you said and create sort of indicia of digital provenance that are pretty reliable. And there's this whole booming industry, by the way, of people creating private sector solutions to mark digital provenance in various ways.

Stewart Baker: [00:44:55] Yeah.

Bobby Chesney: [00:44:55] Digital watermarking. Metadata. That sort of thing.

Stewart Baker: [00:44:58] And that's what bin Laden would have done if I'd gotten my grant out because he could have just used a private key and started signing his videos, if he'd thought of it in time. So if you're a source who's afraid of being spoofed, you can do this. But, of course, you can't go online these days without finding a video that was made by some ordinary person who happened to be in the right place at the right time and just their phone up.

Bobby Chesney: [00:45:32] Right.

Stewart Baker: [00:45:33] And those folks aren't a brand, but we certainly don't want to be fooled by fake videos that purport to be individuals. In those circumstances though, isn't there a substantial incentive for the camera makers to also start hashing and watermarking and otherwise signing the product of a particular camera?

Bobby Chesney: [00:45:58] So there is, but we have a — what I'm describing as a VHS versus Betamax — problem here. Right? There's going to be a lot of different solutions and a lot of platforms. Cameras are on all sorts of devices. Now obviously, we would consider iPhones and the like to be the primary devices of concern, but if we really want to get our arms around this problem, such that you would consider it unreliable to see a video or an image that doesn't have the digital watermark of choice whatever it may be, you're going to get your hands around a lot of different devices, a lot of different ways of capturing that content. And it seems unlikely to me, as things currently stand, that any time in the near future we're going to have the kind of uniformity of uptake of the technology — let's stipulate that the technology is even there already — that we'll have the kind of uniformity of uptake that would enable us to really immediately doubt things that don't come with that watermark already. Maybe we'll get there. Then we'll have the sort of variety problem. I'm a little skeptical that we're going to solve that one anytime soon. The interesting question is: what about if you avoid the problem of the multiplicity of cameras and image takers and instead go to a larger choke point? Go to the platforms and say, "Alright, if you have a major social media platform and you allow users to upload content, it's going to have to bear certain watermarks, certain digital hallmarks of authenticity and provenance." In theory, you could go to a handful of entities and capture a lot of where information flows.

Stewart Baker: [00:47:31] Yeah.

Bobby Chesney: [00:47:31] The interesting question is: would they do that? Would they be willing to do it, and would it come with that technology and that filtering come with the kind of disruption delay and inefficiency that might alter the user experience in a somewhat negative way and therefore drive people away from that particular platform

and to some other platform, some new thing that may not even exist yet? It's easier, and it's just a little bit freer. People might go there.

Stewart Baker: [00:47:54] Actually I am going to be more optimistic. I realize that's not in character. But if you're YouTube, you don't want to be known a place where a lot of fake videos that produce riots are displayed, and you don't have to — there doesn't have to be a law. It's bad for your brand in the long run. And you don't even have to say you can't upload it if you have some dumb old camera or we don't recognize the format by which you're authenticating your data. They could simply say, "Well, fine. We're not going to monetize it, or we're gonna have a warning label saying this is authenticated and therefore needs to be taken with a grain of salt." There's a variety of things that you can do if are a platform that aren't legal — which aren't driven by law — but which have a pretty substantial impact on this kind of thing.

Bobby Chesney: [00:48:57] There's also a definitional challenge, though. So I agree with you that YouTube and anyone who wants to have a brand that's known for reliability is going to be interested in this to some point. There's all sorts of perfectly legitimate manipulation of video that may go on, both for clarity or for stylistic effect or because it's political satire. And of course there's going to be margin cases where it's a bit hard to draw that line. And I think I know from listening to past episodes of this very show that you know you've got a concern, I think for good reason, that sometimes there's a political inflection to how that sort of filtering and screening might take place, and this could become a new avenue in which that issue becomes a difficult one for the big social media companies.

Stewart Baker: [00:49:36] Yeah. So I've engaged in self-help. I've gone out and gotten a small tattoo in a rarely seen part of my body, so that anybody who takes the video of me participating in an unusual or inappropriate acts had better know where that tattoo is.

Bobby Chesney: [00:49:58] We need a Twitter poll to vote on what people think Stewart's hidden tattoo is. Where it is and whose image is it?

Stewart Baker: [00:50:06] I think that's right. I think that's right. Can I come up with something more entertaining than George Schultz's tattoo? He famously had a Princeton Tiger on his butt.

Bobby Chesney: [00:50:21] I know you can out-do that. I'm sure you've already out-done that.

Stewart Baker: [00:50:24] So the other self-help thing that I think is attractive and potentially part of the solution is life logging essentially. Keeping a record — and frankly, I think politicians are going to have to start doing this soon — keeping a record of where you are and what you do. And so that you can say, "I wasn't there, and I can prove it." And there are a lot of reasons why that might fail in certain circumstances. But my guess is that that's where people are going to go just as a matter of self-protection.

Bobby Chesney: [00:51:06] Yeah, we argue that. We think that the thing that's most likely to happen for whom reputational sabotage is an especially acute concern — so politicians, people running for office, major public figures of various kinds, anyone who's got a fragile reputation — either all the time — you know your celebrity perhaps it's all the time, if you're a chief of police perhaps it's all the time — or at least at acute moments. So during an election. You're going to see more and more life logging. Now, a lot of this already kind of takes place. Whenever there's a controversial event on campus, you can bet that there's people with cameras up from the beginning, both because — you know whichever side of the controversy you might be on, everyone's trying to record things because everyone wants to have their record what's going on, and maybe one side is trying to inflect that record a little bit to make it look like things happen the other way, and the other side is hoping to capture a more honest record. You'll see an expansion to that, and that could take all sorts of forms, and we can look to police body cams as a sort of a variance of the technology or application that you might then begin to see with some of these figures. And you might see employers insisting upon it for certain categories of employees, and in fact police body cams is an example of that from a certain point of view, although it's not the employer necessarily in

that case insisting upon it, So that could well be the solution. You can even imagine — and we anticipate — there will be commercial service providers that try to establish an especially trustworthy brand as the repository for this type of content. And if they intersect technologically with the social media platforms in the right sort of way, they might be able to set up a system in which there's very quick and rapid basically alibi checking that's reliable goes on.

Stewart Baker: [00:52:51] Yeah.

Bobby Chesney: [00:52:52] But we also really worry about what this means for a world in which you increasingly have sort of omnipresent surveillance just because all the people around you are life logging everything happening to them.

Stewart Baker: [00:53:02] Yeah, well, I think — you know look, we've crossed that Rubicon, and it's just a question of when we realize that — in fact, we're being life logged as we speak. If you have ever gone to get the description and maps of things that Google knows about you, if you're an Android user, they know where you were every minute of the day for the last five years, and they can show you on a map.

Bobby Chesney: [00:53:35] And now they can start charging for the service. You realize it's actually a benefit.

Stewart Baker: [00:53:37] Exactly. Persuading people that they're getting a great benefit from it. Well actually, what I suspect is going to happen is a lot of people are going to want to have this under their control, pull it back, encrypt it, sign it, put it in the blockchain — because everything has to go on the blockchain — and then...

Bobby Chesney: [00:53:58] Exactly.

Stewart Baker: [00:53:59] ...be able to recapture it, but only on their terms, only if they agree. And of course, then there'll be questions about when you can override the encryption with a search warrant which will be entertaining.

Bobby Chesney: [00:54:11] Exactly. *Carpenter* questions for sure.

Stewart Baker: [00:54:13] Yes. At which point you kind of say, "Well, okay, maybe there's not a third-party doctrine, but for God's sake there ought to be a first-party doctrine! You recorded it!" Alright. So I want to borrow from the National Security Law Podcast the idea of frivolity at the end.

Bobby Chesney: [00:54:31] Yes.

Stewart Baker: [00:54:33] First, you should tell us if there is some event coming up that — you did have a great event with Senator Rubio talking about deep fakes. Any other events where you or Danielle are going to be holding forth on these topics?

Bobby Chesney: [00:54:47] We're going to give a talk. So I'm going to talk for some student audiences at Hastings in September and also for the — I think it's the — World Affairs Council out there. You can get the video of our talk last week with Senator Rubio at Heritage on the Heritage site, which I want to put in a plug for Klon Kitchen who's now running the new tech policy program at Heritage, and I think it's a fascinating and important move for Heritage and similar institutions to start engaging more in tech policy. So do I get a free mug if you invite Klon on the show?

Stewart Baker: [00:55:17] Yes, yes you will. You absolutely will, and I'll put in a plug. I listened to that as though it were a podcast, and if you are not familiar with Huff Duff and Huff Duff Video, you need to Google those things and put their little icons in your bookmark column because any video — or at least any YouTube video and many other videos — can just be turned into a[n] audio file and sent to your podcast aggregator.

Bobby Chesney: [00:55:55] Oh, nice. Huff Duff?

Stewart Baker: [00:55:56] Huff Duff. And then Huff Duff Video.

Bobby Chesney: [00:55:59] That's great. I've actually long wanted that service, so that's good to hear.

Stewart Baker: [00:56:02] Yes.

Bobby Chesney: [00:56:02] The other thing that I'll be working on is — you know the Fall semester is looming, and as you know we've got a sort of an emerging cybersecurity program at UT that includes me and Matt Tait (@PwnAllTheThings) teaches with us here. And I'm continuing to fine tune my course which is about the legal and institutional and policy aspects of cybersecurity matters, and Matt does the mirror image and he teaches the technology to the law and policy students. So we'll be really busy with that coming up soon.

Stewart Baker: [00:56:27] Yeah, that's terrific. He's great. So frivolity. I was reportedly out of the podcast because I was lost in the wilderness last week, and it is true. I went to Aspen for the security forum and a homeland security meeting. But I walked. Started at Snowmass and hiked into Snowmass Lake and then over about a 12,500 foot pass and down into Aspen using a whole bunch of new technology that I'm becoming enthusiastic about. I'm sort of finally catching up to the ultralight revolution. So instead of a tent I just took a bivy sack and a poncho that I wore when it rained and set up as a kind of tarp when I when I made camp and a little metal stove where you burn wood — which really I have to say appeals to me because you can set it up in a completely denuded camp site and people have been pulling down trees all around you and chopping them up, and the stuff they leave behind, the little bits of wood that they leave behind, are exactly the right size for sticking into this tiny stove, so you can build a wood fire in a stove and feel as though you're ecologically pure at the same time. So that's my frivolity.

Bobby Chesney: [00:57:59] That's fantastic. Let me tell you that you're bringing me back to hiking in Big Bend when I was younger, just out of college. Big group of us. We were such idiots. Most of us packed almost no food. We did bring drinks, and it wasn't water. But one guy had a little field stove, and he had some dehydrated spaghetti with meatballs, and he poured some of our scarce remaining water into it and cooked this

thing up while the rest of us were splitting a Pop-Tart, and it was nearly the Donner party. I mean when he started cooking that thing... So lesson learned there.

Stewart Baker: [00:58:33] Yeah. Well, and I will say one time in Yellowstone with this stove, my son and I cooked an entire meal using deer poop, which smelled like grass burning. It was terrific.

Bobby Chesney: [00:58:50] That's fantastic.

Stewart Baker: [00:58:52] So you can do all kinds of stuff. Yes. Alright.

Bobby Chesney: [00:58:55] I knew there was a Green inside you.

Stewart Baker: [00:58:58] Alright. Thanks to Bobby Chesney. Thanks also to Maury Shenk, Nick Weaver, and Patt Cannaday for joining me. This has been Episode 227 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. I should probably do a few credits and notes. You heard Bobby, if you suggest successfully that we invite somebody to the podcast, you can get a highly coveted Cyberlaw Podcast mug. Send those suggestions to cyberlawpodcast@steptoe.com. Watch us. I've started you know irregularly putting up topics that I think we might cover the next Monday on Twitter and LinkedIn and Facebook just asking people for comments, and we're getting comments. I actually find the feedback kind of useful, so watch for @StewartBaker on Twitter, and my LinkedIn account and Facebook accounts are similarly obvious. Please send us some ratings. Go on iTunes and Google Play and Stitcher and give us a review. That's how we get noticed. Upcoming — you know coming up with enthusiasm is our August hiatus. There's some suggestion that we ought to put out favorite interviews from the past. So I'll be glad to take comments on that idea — of course, you don't have to listen to them, so maybe we'll just do it and see if anybody downloads — but before we go on hiatus, Noah Phillips, who's an FTC commissioner, formerly a Cornyn aide, and formerly a Steptoe associate who worked with me, very bright guy, will be on next week talking about a whole host of FTC issues including privacy and the European Union. Show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio

engineer; Michael Beaver is our intern; and I'm Stewart Baker, your host. We hope you'll join us again next week, for the last time in four weeks, as we once again provide insights into the latest events in technology, security, privacy, and government.