Steptoe

Episode 237: I'd Like to Teach the World to Troll, in Perfect Harmony!

Stewart Baker: [00:00:03] Welcome to Episode 237 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking technology, security, privacy, and government. Today I'm joined for the guest interview by Dr. Dipayan Ghosh, who's the Pozen Fellow at Harvard's Shorenstein Center and co-author of a new report, "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet." And I agree with about half of his report, so should be an entertaining interview. For the News Roundup we've got Nate Jones, formerly with Justice and the National Security Council's counterterrorism office. Nate, welcome.

Nate Jones: [00:00:45] Thank you.

Stewart Baker: [00:00:45] And David Kris, also formerly with the Justice Department as the Assistant Attorney General in charge of the National Security Division. And there's plenty of stories that will call on his expertise. So David, great to have you.

David Kris: [00:00:57] Thanks, Stewart.

Stewart Baker: [00:00:58] And I'm your host, Stewart Baker, formerly with NSA and DHS and holder of the record for returning to Steptoe & Johnson to practice law more times than any other lawyer. Okay. Let's jump right into the stories. There's another indictment of another Russian for more election interference. But this time this round of elections. David, what do you make of the indictment?

David Kris: [00:01:27] This is a criminal complaint against a woman named Elena Khusyaynova, who was the chief accountant for the Internet Research Agency and

worked for Putin's chef, Mr. Prigozhin. She's a fascinating woman, lives in St. Petersburg. She describes herself on a YouTube video that she recorded as just a simple Russian woman, mother, and small accountant. She's very excited to have been accused of having such a major impact on our election.

Stewart Baker: [00:02:01] So you have to really admire the Russians for their shamelessness. This is just in-your-face trolling, isn't it?

David Kris: [00:02:12] It really is. It's remarkable how quickly they got it up, and for a simple woman who just knows how to cook fish and raise children as she described herself, it's amazing you know how quickly she was able to get onto YouTube with this rebuttal. It is about as persuasive as the claim of the GRU officers that they were in Salisbury to see the cathedral. She is charged in this complaint with conspiracy to defraud the United States, which is sort of becoming a more and more standard charge coming out of the Mueller investigation, and the claim is that she was the chief accountant in this fairly large Project Lakhta, which is named after a region of Russia and which is sort of the umbrella for all of Russia's election interference efforts since 2014. And the idea that the goal of this effort by the Russians, as it's described in this complaint, is to sow discord and exacerbate divisions and undermine faith in democratic institutions in the United States. You know if this were a more stable, unified, truth-oriented time in our national politics and culture, we might be more inclined to laugh this kind of thing off. But as it is, you know it's of concern, and the complaint really shows a couple of things. One, a fairly elaborate corporate structure and entity for funding and carrying out the mission, which is sort of interesting. The Russians really do seem to have adapted to capitalism. And number two, much more sophisticated and better tradecraft. They are learning how to do their jobs better. They're using better English. They are more sophisticated about sort of who to pretend to be in certain fora and who pretend to be in other fora depending on the target audience.

Stewart Baker: [00:04:09] And also their lines on American politicians are plausible from the point of view of could Americans believe this.

David Kris: [00:04:19] Yes. It's actually kind of fun to see some of their internal comms laid out because you know anybody who's been in the US Intelligence Community has at one time or another sort of wondered you know as we prepare profiles on various foreign leaders and try to understand their motivations, what are they preparing about us and how wrong or right would we think their assessments of our leadership and motivations would be. And so here you've got a sense of sort of the Russian assessment of the American political scene for whatever that's worth. And you know they are not wholly unsophisticated, obviously I'm not going to endorse everything they say. But it is an interesting spin on our politics and the way in which they can continue to undermine us and undermine faith in democratic institutions and rule of law. They have a big budget for this – relatively big budget for this – operation. You know it's tens of millions of dollars over a couple three-year period. They have multiple bank accounts. And they're attacking Bob Mueller now so of course you know as part of one of the strands of their activity. So they're getting more sophisticated, more aggressive. And you just see that they are continuing to do what works and an activity for which they've really not yet been punished in any way that would deter them. It's also notable I think in that this complaint's filed in the Eastern District of Virginia. It tells you something about Bob Mueller's strategy as the special counsel looking into all of this. He is effectively now acting like a startup incubator. And he is creating little spin out businesses that he sets up on their own. And so he's got EDVA [Eastern District of Virginia] doing this case, and NSD's [National Security Division of the Justice Department] got a case, and Southern District of New York has a case, and the District of Columbia US attorney's office has another case. So the business is proliferating, and it's not being centralized in the special counsel's office, which I think is a good strategy in the sense that he's diversified the portfolio and any one of these offices can now go forward and follow the evidence where it leads them.

Stewart Baker: [00:06:25] So one of the things that I was struck by is that Bob Mueller is running into a little bit of trouble with the claim that this kind of activity defrauds the United States by defrauding the Justice Department's FARA [Foreign Agents Registration Act] people or the Federal Election Commission. How serious do you think

that problem is, and are we going to see that here as well if these charges ever went to trial?

David Kris: [00:06:54] I don't know yet. I will say the charges you know sort of have a certain intuitive appeal in the sense that they're pretty broad, and conspiracy is of course the darling in the prosecutor's nursery and it allows them to bring in sort of one umbrella charge a lot of different strands of behavior. I'll also say, not to play too much inside baseball, you know Mueller has on his team Michael Dreeben, the former and actually current I think, criminal deputy in the solicitor general's office. And there is no better, smarter, more knowledgeable criminal lawyer that exists in America today. So I would say in the long run here my money is on these charges to survive.

Stewart Baker: [00:07:39] Okay, so there's another story that I'm just going to touch on. It's a fascinating story, but I have kind of promised Nick Weaver, who responded to my tweet about this by demonstrating a great interest in it, that we would hang onto this for next week when he is in the Roundup. China Telecom is very persuasively accused by a group of Israeli researchers of having essentially kidnapped months' worth of traffic, and instead of having it go to a South Korean government from the Canadian government, it just went first to Beijing and then it went to the South Korean government and the Beijing government was able to look at anything that wasn't encrypted for months at a time. And the way in which this was done and the implications for US and Chinese policy going forward are going to be pretty significant, I think.

Nate Jones: [00:08:45] Yeah. I don't want to take away from Nick, but I'll just say you know the way in which the world's telephone lines and other communications lines are laid out can be very significant. We saw a while back Brazil with its aspirations to create a direct cable to Europe, and the other interesting aspect of this I guess is whether it is just mirroring a fat pipe of communications for surveillance purposes or rather it could actually be used literally to interfere – that is, seize and block transmission or delay transmission or even potentially, if they're very sophisticated, mess with data and then change it and transmit it through. There's a lot of interesting possibilities here, and I will look forward to hearing Nick's thorough assessment of it.

Stewart Baker: [00:09:32] Sounds good. Sounds good. So there's a similar suggestion here in a story saying that President Trump keeps talking on his iPhone even though the Russians and the Chinese and probably other intelligence services are listening. Nate, is that really what the president's doing?

Nate Jones: [00:09:57] It seems so. I mean this story at a high level has been out there for quite some time obviously, and you know we'll leave the irony between this and his campaign's central focus on Hillary Clinton's email servers to the Twitter sphere to discuss. But you know I think we're continuing to see I guess two things emanating from this story that I think speak more broadly to the president's approach. One is his disdain or disregard for the advice and expertise of career professionals, including in the information security realm. And you know their deep concern about his behavior is once again now spilling out into the newspapers in this context. The other thing is you know he continues to sort of put his personal and political interests or creature comforts ahead of what some believe is the country's best interests. You know the only thing that's really new here is that there's a little bit of flavor for the fact that the Chinese may be having some success in accessing his communications with friends and colleagues and their effort to wage this influence campaign against the president himself. And whether that can work is I think still yet to be determined. But I think the bigger picture here is that's not the only reason to be concerned. There are a lot of reasons why even private communications between the president and close personal friends and colleagues could be useful or exploited by foreign governments to the detriment of this country. And it behooves the president to be a little bit more careful and circumspect in these conversations and in his use of his private iPhone.

Stewart Baker: [00:11:53] Yeah, when you're president you don't have any truly private conversations. Everybody you talk to, with very limited exceptions, wants something from the president of the United States. And if he's having private conversations with people who are also tied to business interests in other countries, those other countries are going to try to get those guys to say what is in those countries' interests. And now they have an ability to actually check up on their billionaires when they talk to Trump

and make sure that the messages that the billionaire claims to have delivered was actually the one delivered and also to judge how much of an impression it made. I think even if these are only private conversations in the president's view, he's crazy to be doing them in this fashion.

Nate Jones: [00:12:47] Yeah, and I think you know if anybody other than someone who was elected by the American public to lead the executive branch was engaging in this kind of behavior. I think you know we would see pretty swift and severe action taken against them if it posed these kinds of risks. And so you know at this point until he comes up for re-election he's sort of immune from those kinds of consequences. But I think you know it shows that he's being judged by a different standard than virtually anybody else in the executive branch would be if they engaged in similar behavior contrary to the advice of their security folks.

Stewart Baker: [00:13:28] So what I'm hearing is a very refined version of "lock him up" from you.

Nate Jones: [00:13:37] [Laughter]

David Kris: [00:13:37] [Laughter]

Stewart Baker: [00:13:37] And I have to say, giving credit where credit is due, if the YouTube video was Russia's demonstration that they've mastered trolling, the Chinese response to this was equally tongue in cheek. They said if the president's having a problem securing his iPhone conversations, maybe he should try a Huawei phone.

Nate Jones: [00:14:02] [Laughter]

Stewart Baker: [00:14:02] So Tim Cook. I won't spend too much time on this even though it is three things that usually set me off. Tim Cook, the EU, and privacy all in one story as Tim Cook goes to the EU and says, "Oh, we're such sad Americans. What we need to do is have a GDPR so that you can put my competitors out of business and I

can have all of the business because I'm privacy protective and they're not." I'm not sure this is all dog bites man. It's only the fact that Tim Cook keeps doing it and getting headlines for it may be due to the Apple reality distortion field that it even made it into the paper. Here's a story that is fascinating. FireEye put out a story that said that an intrusion that made the papers into Saudi – FireEye didn't say Saudi, but the *New York Times* did – into a Saudi petroleum facility and that could have caused fatal accidents was that the malware was actually designed in a Russian institution. And they offer some pretty persuasive evidence. Nate, this is kind of an interesting take on what we had previously thought was the Iranians' work.

Nate Jones: [00:15:29] Yeah, that's right. And to me there are a few things that are really interesting about this story. One is you know as we see more and more of these efforts by private entities and public ones to attribute cyberattacks like this, you really start to appreciate that despite the challenges associated with making those links and doing this analysis, it's hard for hackers not to leave some digital footprints that can be used to trace things back to them. And I think that you see this once again in FireEye's analysis. There are little tiny mistakes or you know pieces of tradecraft that are being used that are I think pretty persuasive. You know as we saw with the US government's analysis of the Russian efforts to influence our election, it does take time. It can take months if not years to fully appreciate all the different aspects of this and to dig up the evidence. But you know over time the truth does sort of come out eventually. The other thing that I find interesting is that these private companies, whether you know they're some of the major tech companies or these private security companies like FireEye, there's a limit to what they can tell you. Right? They only have access to certain information, and you know they were able to attribute this to the Russians, as you said, pretty persuasively in this case. But they can't tell you a whole lot about whether they were doing it on behalf of the Iranians, whether this was just the Russians' efforts. If so, what their motivations were, what their actual intentions were, and when you contrast it with some of the indictments we've seen coming out of not just Mueller but in the past with the US government, they were able to you know exploit other avenues of information gathering and intelligence collection to provide more color on the intentions and the motivations of these nation state actors and provide you a fuller picture of

what's going on. And we still don't really have that, in my opinion, in this case, although they do pretty persuasively point the finger at some level of Russian involvement in this.

Stewart Baker: [00:17:52] So I'm guessing this institute – it's the chemistry and the industry institute [Central Scientific Research Institute of Chemistry and Mechanics],it's been around since the revolution and before – got paid to do this. And they said, "This is terrific." It's like selling an F-35 after you've built it for yourself and you're just reducing the sunk cost that you had to cover by selling it off to other people knowing where it's going to be used and you don't care whether it affects the Saudis. Seems like a logical thing, but we may find that out hopefully in yet more indictments to come.

David Kris: [00:18:32] You know one of the interesting things about this, Stewart, there is developing more and more now a sort of state of the art around the attribution of cyber incidents. And you see, as Nate was saying, in these complaints and indictments and in the private-sector reporting on this various methods by which attribution is now undertaken, and it's a super important area of law for the world right now and policy. What I think you're also going to see is criminals and others becoming more sophisticated in trying to plant false information to lead people astray and cause them to believe it was somebody else. So the offense and defense on this is going to continue to escalate as the sophistication rises on both sides.

Stewart Baker: [00:19:17] So I have legal advice for the head of this institute: do not go to the Saudi embassy for a visa.

Nate Jones: [00:19:23] [Laughter]

David Kris: [00:19:26] [Laughter]

Stewart Baker: [00:19:26] Okay. Some very quick hits. Yahoo has finally settled from that massive breach that basically breached all of their accounts. And it follows the Baker Rule for just how cheap it is to settle class actions for breaches: $50 million to cover 200 million people who had three billion accounts. That comes out, even if you

estimate it by person, to about 25 cents a person. And in theory you could get up to $375 if you could prove that you spent many hours trying to deal with the fallout, but my guess is the important thing from the company's point of view is this was a dirt cheap settlement at the end of the day, at least when you look at the number of accounts that were compromised. Cambridge Analytica [Facebook] is paying the largest fine that could be imposed [in the UK]. Nate, I still am puzzled over this 'cause you can say that there was an improper application of the rules, but the fact is all of these alleged privacy abuses were people getting paid to hand over the information of other people that they were in contact with on Facebook. It's a questionable violation to my mind, especially one that would get the maximum. And my guess is really this is just revenge for the perception that Facebook helped elect Trump.

Nate Jones: [00:21:11] Yeah, I mean I guess to be slightly less cynical but still somewhat cynical, I think you know you could argue that this is the UK government you know on some level trying to figure out how to use the sticks at its disposal to try to influence private companies to be more aggressive in confronting efforts of all kinds to influence democratic elections or undermine confidence in those elections or in the rule of law. And you know ironically they're doing that by, as you point out, twisting the rule of law to a degree to achieve a particular end. But, as you said, you know there's a very good chance that Facebook will appeal this, and we'll see what that appellate process produces if they do. But I think there are some valid reasons for governments to be concerned about efforts like the Cambridge Analytica approach to influencing elections and trying to get ahead of that use what tools you have to try to get others to snuff that out.

Stewart Baker: [00:22:19] So the British commitment to privacy has some limits. Somebody hacked Belgacom, the big ISP in Belgium, and filled it full of spyware. And the Belgians are conducting a long investigation – have conducted – and they asked the British to help them track down the substantial evidence that GCHQ might have done this. And the British said, "Yeah, I don't think that would be consistent with our national security or our sovereignty. And besides, Brexit, Brexit, Brexit. We're not turning over

anything to you." And I think the investigators are about to give up the ghost because they are not getting anywhere.

David Kris: [00:23:09] Yeah, this is a little bit of kabuki theater as surely nobody is surprised by the other side's reaction to all this. Proximus, which is the new name of that entity in Belgium [Belgacom], was, according to some stuff leaked by Snowden, the victim of a watering hole attack that compromised a few employees who visited a fake LinkedIn site, and that apparently let GCHQ into their network where they moved all over the place laterally and otherwise to get a lot of juicy information. It's hard to imagine, particularly with Brexit going on, that the British government is going to cooperate with this investigation, but I suppose the Belgians had to ask. And as you say, it's gotten a little press recently, but it doesn't really look like it's going to go anywhere as a Belgian-British joint venture of investigation.

Stewart Baker: [00:24:06] And last story. We covered in some detail the Uber bug bounty / ransom payment to hackers who found a bunch of data, downloaded it, then went to the company and asked for ransom in a context where you could if you stretched said, "Well, I guess they're asking to participate in our bug bounty program and why don't we give them a $100,000 as a bug bounty and then we don't have to report it as a breach," which turned out to be a disaster for Uber and its management. And now it turns out a disaster for these hackers who having discovered this scam tried it out on a LinkedIn subsidiary and said, "We've already picked up nearly seven figures" – which is what I think low six fingers apparently translates to – "from another company. And we found a bunch of your stuff too. We'd like you to pay us as well as part of your bounty program." And instead they got indicted.

David Kris: [00:25:11] Does highlight the ethics of bug bounty extortion and the like and the sort of fine line between offering your assistance with making sure that no fire occurs in the building and other kinds of tactics which would be frowned upon through the vehicle of the criminal law.

Stewart Baker: [00:25:28] Yeah, it's too bad. These guys may have lived up to their promise to destroy the Uber data. But it's not that fine a line: either join the bug bounty program or you don't. And if you're hacking somebody and claiming it's a bug bounty, you need to be in compliance with their bug bounty rules.

David Kris: [00:25:52] It is a little bit of a post-hoc effort to put lipstick on the pig there, isn't it?

Stewart Baker: [00:25:56] Oink! Yes! Okay. Let's turn to our interview with Dr. Dipayan Ghosh, who with Ben Scott wrote the report, "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet." Okay. Our guest interview today is with Dr. Dipayan Ghosh, who's got a great resume already for somebody who's clearly pretty young. You were a Facebook privacy policy guy. Before that you were in the Obama White House, and now you're at the Harvard Kennedy School working with Tom Wheeler from the FCC on platform policy.

Dipayan Ghosh: [00:26:43] Yeah, it's so great to be here, Stewart. Thank you so much for having me. I'm honored as an avid listener. And it's great to be here.

Stewart Baker: [00:26:54] Okay, well we're going to talk about your report, which you did with Ben Scott, called “Digital Deceit II.” And it is... Well, let me ask you: what problem are you solving here?

Dipayan Ghosh: [00:27:07] Well, the problem we're trying to address is broadly the disinformation problem, and the first report which we put out in January is an attempt to analyze the way that this whole problem works, the way that misinformation spreads through online platforms, and the business model behind those online platforms that encourages its spread and the consumption of disinformation. And this second report that we released last month is a response to: okay now that we know that this is a problem and now that we understand that perhaps this business model is driving it, what are the policy measures that we should take to respond to it?

Stewart Baker: [00:27:49] Okay. So the idea is that the platforms' business model, advertising to people about whom you have a massive amount of data, is part of the problem at least of digital disinformation. Certainly it's the most salient one in the last 10 years because the platforms are new in the last 10 years. And so the question is: what can we as political actors do about the mismatched incentives? So let me ask you a question that isn't really in the report, but I haven't gone back to "Digital Deceit I": do you think that the bias of platforms against conservatives is a real problem?

Dipayan Ghosh: [00:28:33] Well, I think overtly, explicitly we can see that there maybe is some evidence to suggest that there is a problem here, but I actually don't think that – if the question is, is there an intentional bias against conservative thought and conservative perspectives and viewpoints that has been decided upon as the internal corporate position by company leaders –

Stewart Baker: [00:28:59] Of course they're not going to do that. Right? It's more a question of what are all the incentives inside the company and what are the assumptions inside the company about what's hate speech and what's not, what's acceptable speech, and what goes beyond the pale.

Dipayan Ghosh: [00:29:16] Well, this is a hard question to answer. I mean I do think that overtly again you could suggest that companies have taken corporate positions that aren't in alignment with conservative perspectives in certain cases, as you mentioned. Hate speech could be one; misinformation could be another. Again I don't think there's an intentional decision-making process behind this. But I think you could say that, at least on evidence, yes there is this bias.

Stewart Baker: [00:29:54] So I agree with you. Maybe I feel more strongly about it, about the evidence and about a sense that this is not so much intentional as it's the water in which they swim. Fish don't notice the water in which they swim, and the social media folks out in Silicon Valley really don't see their bias for anything other than you know *bien pensant* [orthodox] thought. But the concern among conservatives about platform bias ties to a degree to some of the issues you are raising because if you think

that there's bias there you might ask the question: well is there a regulatory solution? Is there an economic solution? Is there a competition solution? So this is by way of giving you a sense of the perspective I brought to some of the things you said because some of the things struck me as working toward solving the problem that I see and others were pretty orthogonal. So let's unpack what you had to say. You really boiled down your recommendations to three things. You want more transparency from the platforms, especially about ads and what they're doing with the data. You wanted a whole set of privacy rules. And you wanted new competition policy. So why don't we break it apart? 'Cause I thought the ad transparency was interesting but maybe pretty limited. You basically endorsed the Honest Ads Act and say that plus a little more is what we ought to try.

Dipayan Ghosh: [00:31:40] Absolutely. I think we have to look back at the business model here. Part of the business model is about concealment. That is for leading Internet platforms to hold information within and not expose it because doing so would reveal things that go against their commercial interests.

Stewart Baker: [00:32:05] So this is revealing their algorithms, revealing how they target ads, and the like.

Dipayan Ghosh: [00:32:10] Absolutely. That's part of it. So this is again – both reports written with Dr. Ben Scott, and Ben and I have been thinking a lot about this transparency problem. Our proposed suggestion is that we should have a regime for political ad transparency that brings the same kind of things that a consumer might expect for transparency in political ads on broadcast or radio to the digital world.

Stewart Baker: [00:32:46] That seems like sort of "Duh. Why would that not be the case?" My memory is that when he was up on the Hill, Zuckerberg said, "We recognize there's going to be regulation," more or less endorsed Honest Ads if I remember right. So Silicon Valley kind of sees this coming and is prepared to give way at least to the extent of the Honest Ads Act, which is not quite what you get on broadcast but close.

Dipayan Ghosh: [00:33:15] I think we've gotten to that point. I think for a long time Mark Warner and John McCain and Klobuchar (Senators in the US) were pushing for the Honest Ads Act for a long time throughout 2017. The industry wasn't really coming to the table, and then as soon as the Cambridge Analytica incident happened, we saw people like Mark Zuckerberg and Sheryl Sandberg flip overnight and say, "Oh, actually we," despite the fact that the industry's lobbyists were pushing against it behind closed doors –

Stewart Baker: [00:33:51] But the companies couldn't stand the heat.

Dipayan Ghosh: [00:33:53] They couldn't stand the heat, and they flipped. And they said, "Oh, we actually love the Honest Ads Act. We love the principles therein. And in fact, you don't even have to push that as law because we're going to take these steps voluntarily."

Stewart Baker: [00:34:05] And they have produced some transparency centers, which you know I have to say the idea of going to visit those just fills me with tedium. Is it worth going to their ad transparency pages?

Dipayan Ghosh: [00:34:20] I think it's worth going there if you're a certain kind of person like a journalist or a researcher or somebody who's trying to understand this from an academic point of view or just academically interested in these kinds of things. But for the most part, 99% of the American electorate is not going to go in and try to look at those sources.

Stewart Baker: [00:34:40] And so you make the argument that people shouldn't have to go look it up. It should be displayed with a mouse-over or something on the ad.

Dipayan Ghosh: [00:34:49] Absolutely.

Stewart Baker: [00:34:49] I was puzzled by why, first, how you limit this and why you limit it. Political ads – a political ad is defined, at least you suggested, as basically

dealing with a political issue that has national significance, and that could be almost anything. Right? And how do you decide – how are the platforms supposed to decide – well this is political and that is not?

Dipayan Ghosh: [00:35:18] Yeah, it's a conundrum, and of course a lot of press organizations and other kinds of organizations that aren't political, per se, but are pushing content that has to do with hate speech or with a Republican candidate or a Democratic candidate that their content is getting flagged as political.

Stewart Baker: [00:35:39] Why not just do it for all ads? What's wrong with just saying, "We don't fully understand how this is being used to affect the way we think about things. People can take their posts and elevate the posts' circulation by paying for it." That feels like an ad.

Dipayan Ghosh: [00:35:59] Well, let me be clear: I'm not against that. I think I'm all for more transparency in digital advertising, and I think we should know the provenance of the ad, the impact of the ad as in how many people have been attempted to be targeted, also the targeting parameters of the ad, and all that information should be in context.

Stewart Baker: [00:36:18] And the worry on the part of the platforms is that this will lead to a gaming of the system. Everybody will say, "What does it take to get Google juice? I'm going to do that." And every time the algorithm changes, they'll change their content to get maximum value out of it. And the companies won't be able to keep secret things that will be misused.

Dipayan Ghosh: [00:36:44] Absolutely. I think those are at least the explicit arguments that the industry makes. And I think also the industry is very worried about, as you say, revealing their intellectual property, their secret sauce behind their algorithms, because ad targeting and content curation are the thing that sets Facebook and Google apart from all their competitors. And whichever companies are able to target clients' ads most

effectively to the biggest audience is going to rise to the top of this industry and take it over.

Stewart Baker: [00:37:20] Right. Then they'll be able to show better click through and better results in stores, etc., etc. Okay. So the problem this addresses, though, at the end of the day I think is the problem of the Russians buying ads that you know we didn't know was Russians. Does it address Cambridge Analytica in a significant way?

Dipayan Ghosh: [00:37:47] I think it can to an extent. I think we have to get into privacy a little bit as well. But to an extent, it would because if we could follow the principle that the person seeing the ad should know the targeting parameters –

Stewart Baker: [00:38:04] Why did you see this ad, essentially.

Dipayan Ghosh: [00:38:05] Exactly. So Facebook, for example, is actually more transparent about that than Google is. So you can click into the down arrow in the top right of an ad and click "Why am I seeing this ad" and you'll get some high-level description of why.

Stewart Baker: [00:38:23] Not necessarily who bought it.

Dipayan Ghosh: [00:38:25] Not necessarily who bought it. None of that other context, especially for obviously an ad that's not political. I think we need to go a lot further, and this gets into the privacy argument as well. But yes I think if you're looking at the Cambridge Analytica problem, the 87 million people whose data that was accessible by Cambridge Analytica. Cambridge Analytica working for, let's say a political client, would have, if it was really doing everything that it could, would have started analyzing those 87 million people, started bucketing them into different categories, and for their clients engaged in a contingency-based advertising campaign to see what kinds of ads work for different constituencies and what gets the most re-shares and organic reach. And to be able to see that you were targeted for particular reasons, whether it's by Cambridge [Analytica] working for another political actor or some other PAC [political action

committee] or candidate, I think can go some way. But again, you already alluded to this, transparency is not going to solve this problem.

Stewart Baker: [00:39:51] But I do want to, before we move on, I do want to ask one more transparency question because one of the ways in which conservatives feel that their speech has been disfavored is it's been de-revenue-ized. And the platforms say, "Well, we had some users who didn't want their ads to appear next to this kind of content." But in some cases they just said, "You know we don't like you. Get out. We're not going to send money to your YouTube account no matter how many people look at it." Is that something about which there ought to be transparency, as well: decisions about which kind of content is being disfavored by which advertisers and which kinds of contact are being disfavored just by the platform?

Dipayan Ghosh: [00:40:36] For sure. Yeah. I'm thinking about the public interest here, and I see no way that having that level of transparency available to the public would harm the public.

Stewart Baker: [00:40:47] Right. Okay. So you also talk in here about bot disclosure. You know, "I am a bot. This Twitter account is not a real person." And that's rather similar to what I call the California Turing Test where California has said you cannot disguise the fact that you're a bot if at least you're trying to defraud someone, which is kind of a pretty limited disclosure requirement. Is this the beginning of implementation of your recommendation?

Dipayan Ghosh: [00:41:26] I think so. I think so. What we talk about in the report is the Blade Runner Law, and this is the idea that you know –

Stewart Baker: [00:41:35] It's just a cooler name than California Turing Test. [Laughter].

Dipayan Ghosh: [00:41:37] [Laughter] Right. As a political actor – or any actor that is running a robot account – to disclose that or have a requirement on the platforms that are able to detect that kind of activity to disclose that.

Stewart Baker: [00:41:57] So there doesn't strike me as any really good reason not to do this other than if you're a platform it means some of your subscriber account data will be reduced. But other than that, is there really a good policy reason on the other side for not having bot disclosure?

Dipayan Ghosh: [00:42:20] You know I can't think of one.

Stewart Baker: [00:42:23] Okay. I realize that's not your job. Okay. And then the thing I was puzzled by and skeptical of was disclosure of automatic algorithms used in serving ads I guess because I wasn't sure what problem was being solved there. And maybe you can tell me what it is you were trying to get at with that?

Dipayan Ghosh: [00:42:51] Well, the use of algorithms is going to increase in this space.

Stewart Baker: [00:42:57] For sure. That's the platform's answer to everything. "Oh, we'll have machine learning solve this problem!"

Dipayan Ghosh: [00:43:04] Right. Well, so machine learning is being used on both sides. It's being used by political actors to try to push their content in an effective way. That is, to be a little bit more specific, what political actors like I believe Brad Parscale, who managed the Trump campaign's activity, what they did is really test out all sorts of different configurations of ads and then run them against all different pockets of the country to see what fits.

Stewart Baker: [00:43:41] I got to ask because you were in the Obama Administration and we heard so much about how brilliantly the Obama Administration and the campaign had used social media. How could it possibly be that this guy who made his

money in real estate and you know only knows how to use Twitter could come up with a use of Facebook that was apparently so much more effective than the Clinton campaign's?

Dipayan Ghosh: [00:44:10] Well, look, I wouldn't attribute this necessarily to the president. I think Brad Parscale was very well trained in what's known as commercial marketing.

Stewart Baker: [00:44:21] But better than that entire team of digerati on the Clinton team? It just seems so weird.

Dipayan Ghosh: [00:44:28] I advised the Clinton team, as Ben [Scott] did. And so I can't claim any of their operations or to have decided anything, but what they would say is that "We had a principle that we didn't want to step over."

Stewart Baker: [00:44:49] So they think they were more moral than the Trump guys.

Dipayan Ghosh: [00:44:53] You could probably get them to say that, yes.

Stewart Baker: [00:44:55] That there were things they wouldn't do.

Dipayan Ghosh: [00:44:57] That's right.

Stewart Baker: [00:44:58] Okay. Interesting. Okay. Well, that fits, right, because it was my assumption that if she had won, she could have used all the same techniques and we'd be hearing about how wonderful and cool it was instead of how evil and manipulative it was. But okay.

Dipayan Ghosh: [00:45:17] Well, let me just say that I personally I don't think that anything that Brad Parscale, at least what has been revealed, I don't think anything there, at least as far as I've read, is evil. I think that he was just playing within the rules of what is allowable. And it was –

Stewart Baker: [00:45:40] Mostly just A/B testing at the micro level.

Dipayan Ghosh: [00:45:43] That's right. Yeah. I think it was all fair game. I mean you could make the argument that our Congress should pass laws against that kind of activity, and that would be a very hotly debated legislative proposal. But I don't see any problem with what has been reported about what he did.

Stewart Baker: [00:46:02] Okay. So that's your set of proposals, and we'll get to privacy in a second. But the problem solves clearly is not knowing who's doing things to you. Does it solve the problem of social media trying to divide us and put us in filter bubbles? Seems to me that – we may want to talk about that in privacy – but transparency doesn't really tell you you've been put into a filter bubble necessarily.

Dipayan Ghosh: [00:46:31] Not necessarily. I mean the closest you'd get to that is through the ad targeting parameters that could be revealed. But that doesn't really get you to the point where you could conclude that yes I've been put into the “support Kavanaugh” filter bubble or the “Pizzagate” filter bubble.

Stewart Baker: [00:46:51] So I know you want to talk about privacy, and since we are running low on time already, I want to tell you straight up: boy, that was the least persuasive part of your paper.

Dipayan Ghosh: [00:47:03] [Laughter]

Stewart Baker: [00:47:05] I felt like I should be playing Carly Rae Jepsen, "Call Me Maybe," in the background because it was like a period piece. I felt like you were saying, "You know the Obama Administration, when I was there, we came up with all these great ideas, and they're still great ideas!" But I don't see how giving platforms less data changes the ability to influence voters in significant ways. It might make it more of a black market for that data, but they're going to have the data. If they can't sell it, it just means you're going to reinforce the monopolies or duopolies that are there now. I

thought the idea of saying we should all be able to take our data away and really consent – these are the sort of prescriptions you gave – were interesting privacy policy but not really addressing the problem of disinformation. So tell me why I'm wrong.

Dipayan Ghosh: [00:48:05] Well, I think Ben [Scott] and I have concluded the disinformation problem is really driven by the collection of information about us. If we look at the business model, the business model is about creation of sticky services, the collection of data through those services, which contributes to these behavioral advertising profiles. Those profiles include –

Stewart Baker: [00:48:30] You know they want stickiness without regard to the data they're collecting from the stickiness. The stickiness allows them to serve more ads.

Dipayan Ghosh: [00:48:37] Absolutely. But the practice underlying it all is the development of these behavioral advertising profiles. Without that which allows the companies to infer your personal preferences and interests and beliefs and likes and dislikes, they're not able to piece together the last part of it which is the development of algorithms. And those algorithms that are built to do two things which is curate content and keep people coming back to these sticky services and target ads which contributes to their revenues directly.

Stewart Baker: [00:49:16] But in general, unless we are self-loathing, we should like the idea that they're giving us stuff that we want.

Dipayan Ghosh: [00:49:23] Absolutely.

Stewart Baker: [00:49:24] Although I'm familiar with the argument that says you know we all like pork rinds, but a steady diet of pork rinds is going to kill us. That seems to me is not really addressing the problem. The other is you're sort of saying, "The platforms have a business model. We don't like what the platforms are doing, so let's screw with their business model."

Dipayan Ghosh: [00:49:46] Well, I don't think we're saying we should screw with their business model. In other words, to be more explicit, I don't think we are saying that Chanel or Nike or the NBA shouldn't be allowed to engage in targeted advertising over Facebook. I think what we are saying is that the creation of this commercial regime for the service of Chanel or Nike or a traditional advertiser has been great. It's cut costs in this industry. It's allowed for more effective engagement. But it has created a system through which nefarious actors are able to infiltrate very easily fronting as legitimate businesses and legitimate political actors and so on and so forth. And they are part of this data regime as well. They are absolutely getting access to the types of inferences that Facebook has made or Google has made about us almost necessarily so without our consent.

Stewart Baker: [00:50:50] Yeah. So I guess I can't help thinking that this ship has sailed. The amount of data about us is going to continue to increase online. And the ads are going to be based on that. And efforts to stop that are a little like King Canute telling the tide to stop. It just doesn't feel like it's going to solve the problem. And you know giving people data portability, it just means that somebody you know some third party is going to say, "Hey, port all that data over to me so I can use it to serve ads for you, and I'll give you a free toaster too." And so we're not really going to end the trade in data. We just might cut the consumer in on a little more of the payoff.

Dipayan Ghosh: [00:51:38] Well, you know I think I'd push back a little bit and say that data about us becomes less and less relevant each day that it exists out there. And that's why the leading companies in this sector are collecting data continuously about us over time because our behavioral advertising profile changes by the day.

Stewart Baker: [00:52:03] Right. Once we bought the car we're not interested in the ads for other cars.

Dipayan Ghosh: [00:52:05] Of course. And our interests and preferences change over time. And so the more recent that can be, the more current that can be, the more valuable it is, which is why these companies are so valuable because they engage with

us every day. So I think that the value of data in this sense in the digital advertising ecosystem falls off pretty quickly. And so if we are able to institute solid privacy regimes, they would still have a lot of meaning. If we are able to institute a regime by which a user is able to consent and really say –

Stewart Baker: [00:52:49] Well, we consent all the time. And I don't want the solution to be "Oh, now you have to read it before you consent," because nobody is going to do that. It's just a roadblock. Alright. I think the most promising idea in this space is to say if you think you're abused by the platforms and the platforms have a monopoly or duopoly or an enormous network effect, why don't we go at the monopoly? Why don't we go at the network effect so that you can have the Fox News of platforms as well as the CNN or MSNBC of platforms? And there I thought your suggestions for changes were you know in the right neighborhood but a little thin.

Dipayan Ghosh: [00:53:45] Yeah, I think this is definitely an area that deserves more scholarship and more investigation. I think a lot of people these days are talking about antitrust reform. I don't think the answer necessarily stops there. You mentioned the network effect. Part of the reason that these companies are so valuable is because more and more people come to them, are attracted to them, and they have these global platforms that engage and help people engage in communication. That's something that's tremendously valuable and to just to break it up using antitrust authority might not be the right –

Stewart Baker: [00:54:26] Yeah, 16 little network effects just isn't going to make it. Is that what you're saying? You can't just break up the company by saying there will be four social media companies.

Dipayan Ghosh: [00:54:38] Right. You could say that you know let's split off the different services into different companies, and I think that argument definitely has some more validity to it because the only value that they add to each other is the sharing of data across those services. And I think you could very easily make the argument that,

no, that shouldn't happen, or at least these types of mergers and acquisitions should have far greater scrutiny than they do. And that's where we start. I think we –

Stewart Baker: [00:55:11] Or you could say the solution is to go in and take apart some of these acquisitions from the past where we can still see different social graphs. But I agree with you thinking about it from a consumer point of view. You may only have 20 people that you want to share stuff with, but they have 20 people and it's not the same 20 people and before you know it, everything has been interlinked and splitting it up is really hard to do. But you could say, "Well, fine. We've got a picture sharing service, and that is separate from our social media or separate from our messaging system." So you could still probably break them up, but my guess is that's going to turn out to be harder than one would like.

Dipayan Ghosh: [00:55:56] Absolutely. Absolutely. Which is why we suggest, yes, scrutiny over mergers and acquisitions but also beyond antitrust reform a whole set of competition policy reforms that can really bring our regulatory authority to bear in other ways, specifically through more narrow restrictions on what the industry can and can't do in different respects.

Stewart Baker: [00:56:23] Yeah. So this is sort of conditions on the acquisition, on the merger, which always struck me as kind of a toll for creating a monopoly. It's not an enormous structural solution. It's just saying, "Well, I've got a couple of good ideas, and I want you to do this, and then I'm going to let you buy this company."

Dipayan Ghosh: [00:56:42] Well, if we agree that the network effect is something that's natural and contributes to society, then we have to surrender. We have to surrender some way. I'm not saying that's the right solution. It's really a suggestion from us. But I think cutting through all of that, we also suggest data portability, a radical proposal for portability that really can bring about greater competition in the sector.

Stewart Baker: [00:57:12] And how is that? I thought I saw it was a very detailed proposal, looked like you'd worked on it in the past as well. But basically it says

consumers should own their data and they should be able to demand it all in a format that is easily manipulable and searchable and then presumably give it to somebody else who says, "I'll pay you for it."

Dipayan Ghosh: [00:57:33] What consumers have lost in the face of this industry is their autonomy. If we want to give them their autonomy back, what we have to do is not just allow them to download your information through the Facebook tool or download your data through the Google tool because that's just explicit data that you've shared with those platforms and you could easily share with anybody else. Those companies are not providing anything really through that. What is really valuable are the inferences about your behavioral profile that those companies have compiled over time –

Stewart Baker: [00:58:07] And that you think should be portable as well.

Dipayan Ghosh: [00:58:09] Well, that's the meat of the industry.

Stewart Baker: [00:58:11] And isn't that then going to just create a secondary market? So I guess what this turns out is it allows you to say that the big social platforms will have all this data, but they won't be able to use it in an anti-competitive way because a dozen other companies will be created that also want the pipe full of transactional personal data so that they can serve ads without worrying about the dominant ad servers. So it's not trying to get at the social network effect. It's trying to get at the way in which advertising reinforces the duopoly.

Dipayan Ghosh: [00:59:03] Absolutely, and it does because if we look at the digital advertising market, it's dominated by these two companies. And the profit margins that they're making off of that are really tremendous. I mean these companies are essentially websites where you see an ad and they collect lots of margin over the relative costs, and in creating this regime whereby they have these very marketable and sticky services, they're the only ones that are able to collect data through those services and have bought up all these other companies in the advertising ecosystem to reach into third-party websites and get your data through that way and to oppressively send you

updates over your phone to try to get your location data and other data through your phone in that way. And then finally to use that infrastructure more and more explicitly in the advertising sector they have absolutely engaged in certain anti-competitive behaviors, and yet our government doesn't really have any way of solving any of those issues.

Stewart Baker: [01:00:22] So this is interesting, and if you worry as I do about anti-conservative bias in ads, having multiple ad companies who are basically living off of the data portability stream means that you're much less likely to be discriminated against in the distribution of ads because the people who distribute them can't afford to do things that are economically foolish but ideologically satisfying.

Dipayan Ghosh: [01:00:55] Absolutely. Yes. And I think that, look, we need more diversity in political viewpoints on these platforms. I think if you talk to the platforms – and I'm not advocating this – but if you talk to them, they will say that, look, it's not the political perspective, but it's rather the perpetuation of misinformation or let's say – I don't want to attribute anything in particular – but they will they will argue that there are these very clear lines against our hate speech policy or our misinformation internal corporate policy.

Stewart Baker: [01:01:33] Oh that's preposterous. They have no idea what disinformation is, and they barely know what hate speech is. Somebody got de-platformed the other day for using the wrong pronoun, and of course that's hate speech because it's you know anti-LGBT. But I don't think that the platforms themselves can say, "We know exactly what we're enforcing, and it's clear."

Dipayan Ghosh: [01:02:00] I think they can say that.

Stewart Baker: [01:02:02] Well, they can say it. [Chuckle]

Dipayan Ghosh: [01:02:03] They can say it right now, and there is no stick against them for saying that, which is why I say and Ben [Scott] says we need to have a whole new regulatory regime that applies to this sector.

Stewart Baker: [01:02:16] So I'm not sure about regulation, but I like the idea of saying if the problem is that people are extracting psychic income from imposing their social views on others because they make so much money that you know why not, that the idea of saying well maybe they need more competition and rather than going at it by looking at the free services, we should look at the underlying ad market that supports it and say, "What can we do to build more competition in that market?" Very interesting approach and one that might attract conservatives as well as the more standard reformers. Well, Dipayan, this was terrific. And I usually ask our guests if they have upcoming events, speeches, additional reports. Are we going to see "Digital Deceit III" soon? Anything that our listeners should be watching for because this has been a great conversation?

Dipayan Ghosh: [01:03:19] Well, thank you so much, Stewart. Again it's just a pleasure to be here. At the Harvard Shorenstein Center at the Kennedy School we're launching the Platform Accountability Project and are hoping to put out a lot of content and research through that vehicle and are organizing a big event in February for congressional staff.

Stewart Baker: [01:03:45] Good. Well, put Glenn Reynolds on your advisory board. He has an endless stream of stories about Silicon Valley abusing conservatives.

Dipayan Ghosh: [01:03:55] [Laughter]

Stewart Baker: [01:03:55] I'm sure he would be glad to repeat for you. Okay. Thanks to Dipayan Ghosh. Thanks to David Kris and Nate Jones for joining us for the News Roundup. This has been Episode 237 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Just a reminder: please send us ideas for guest interviews at CyberlawPodcast@Steptoe.com. Watch my Twitter feed, @StewartBaker, for stories

that we will be covering in the future. Leave a rating for us on iTunes or Google Play or Stitcher or Pocketcasts, wherever you get your podcasts. And I have not forgotten that I promised to read the most entertainingly abusive reviews, so get them in soon. Finally, show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio engineer; Michael Beaver's our intern; I'm Stewart Baker, your host. Please join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.