Steptoe

# Episode 233: Outing the GRU

**Stewart Baker:** [00:00:04] Welcome to Episode 233 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us in our new studio with hopefully our improved sound quality. We're lawyers talking about technology, security, privacy, and government. Today there won't be an interview, but I'm joined for the News Roundup by Evan Abrams, who's an associate in our blockchain and cryptocurrency group, and by Nick Weaver, senior researcher at the International Computer Science Institute and a lecturer in Berkeley's computer science department. Hi, Evan.

**Evan Abrams:** [00:00:39] Hey, good morning.

**Stewart Baker:** [00:00:39] And hi, Nick.

**Nick Weaver:** [00:00:42] Hello.

**Stewart Baker:** [00:00:42] And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. Jumping right in. Uber is going to pay $148 million to all the state AGs to settle their 2016 data breach case. This is the one in which somebody wrote to them and said, "Hi, I've got all these names and other credentials. And I think you should give me $100,000." And they said, "How would you like to be part of our hacker bounty program? And you just have to sign up to it and agree to destroy the data." And so retroactively they made it a bounty payment rather than a breach. And then when that emerged, all hell broke loose, and they've been sued, including by all the AGs. And they've now settled that case for $148 million, which I have to say is like $140 million more than you would ordinarily expect to settle a case with the AGs for. So surprisingly big number. Nick, I don't know if you looked at this, but my impression is that there's never been any unfavorable consequence to any user of Uber from that

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

breach, that the guy who found the stuff apparently did destroy it as requested when he got his $100,000 bounty payment.

**Nick Weaver:** [00:02:10] I think so. I haven't heard of anything.

**Stewart Baker:** [00:02:13] So this is really expensive for a breach that caused no known harm. And I think it's basically a special deal for companies called "Uber" who have thumbed their nose at government for so long. And they're going to pay this partly because they have that reputation and partly because they've got completely new management and they're trying to live down that reputation.

**Nick Weaver:** [00:02:37] And I think partially because the cover up was worse than the crime.

**Stewart Baker:** [00:02:41] Yeah, you know I think it was a close call. I think it was creative lawyering, and there are times when creative lawyering is a bad idea. It was close. The guy did ask for $100,000, and you could have squeezed that into the bounty program with a shoehorn. And that's what they did. But they didn't really have any assurance that he had destroyed the data other than waiting to see if it showed up someplace. So understandable that it was treated as a cover up. I'm not sure that's completely fair to the people who made that call. Alright. Speaking of being fair to people. Bellingcat. God bless them. They have tracked down the true identity of one of the two guys who went to the UK to carry out the nerve agent attack on the Russian defector. They've written a very persuasive analysis suggesting that he is in fact a Colonel Chepiga, I think, in the GRU who's been decorated in the past for unknown exploits in eastern Ukraine – or we suspect eastern Ukraine – and is now completely outed as a guy who grew up in Siberia and is in his I think 30s and really will never be able to live this one down.

**Nick Weaver:** [00:04:13] Yeah. Bellingcat does amazing work. One of the little tells was finding this officer's name on a list from the military school he went to for having gotten the Order of Russia award, which is basically hand delivered by Putin, and yet not in the

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

public record. And all sorts of things. It's a really persuasive dossier, and the amount of open source work that Bellingcat does is just astonishingly good.

**Stewart Baker:** [00:04:51] Yeah. And it's an indication of just how hard it is to hide in the new digital world that we all inhabit. Even people who are old enough to remember before there was a social media world and who know they should be hiding but can't keep others from bragging about them essentially.

**Nick Weaver:** [00:05:15] Yep. That it isn't just your data but data about you provided by others.

**Stewart Baker:** [00:05:22] So here's a question I'll ask you, although there's no reason why you have to answer. Would MI6 be justified in going out and killing this guy?

**Nick Weaver:** [00:05:32] I dunno.

**Stewart Baker:** [00:05:32] I mean he's killed somebody on UK soil. And if you want to establish a rule that you don't do that, you kind of have to respond in kind, don't you?

**Nick Weaver:** [00:05:43] I don't know. I'd be worried about living out *Assassin's Creed* of dueling assassins might be a bit escalatory. I don't know.

**Stewart Baker:** [00:05:54] I'm not sure it's escalatory to return the favor, but yes, that is always the worry. But as I've said in other contexts, I'd just as soon the Russians had to stare into that pit for a while instead of us always saying, "Oh, we will be the responsible ones." Anyway. So that's just a question. Everything is coming together in Washington in the last week or two for significant action on privacy. But it's too late for this Congress. Least that's how I see it. The Trump Administration has now put out a kind of think piece, very general, asking for people to give them comments before they start thinking about what their detailed proposal on privacy might be. But their think piece reads like an FTC fair information practices rule more or less written into statute. And so if the Trump Administration is there and Republicans are there – John Thune has

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

written an op-ed that there needs to be some kind of approach to privacy that's better than what we have now – and you know Silicon Valley has basically said, "Oh my God, if we don't get federal legislation that preempts California, we'll have to live with the California rules," so they're actually lobbying for a federal law. And so if there was 12 months left in this Congress, there probably would be one. Since there isn't and you have to assume that there'll be a Democratic House, I'm guessing that that means that the fight over preemption will make it much harder to get legislation at the federal level.

**Nick Weaver:** [00:07:43] I imagine so because we in California like our privacy legislations, even though we're the land of Facebook and Google. Close exposure means we don't trust them.

**Stewart Baker:** [00:07:58] Yeah, I can see that. And of course no one knows what the final California legislation is going to look like because this was a stalking horse designed to be amended over the next year. And so the real question will be when Silicon Valley goes to Sacramento, what will Sacramento do with the placeholder bill that they adopted? Alright. I want to ask Nick about the Pho – that's not in the sense of false, but in the sense of P-H-O – one of the packrats, the NSA packrats, who was indicted and is now being sentenced. There was a sentencing report that was you know a little bit personal with Mike Rogers writing a fairly unhappy letter about Pho's impact. And one of the questions that has arisen is: was this guy who took home massive amounts of stuff, then connected it to the Internet, and used apparently Kaspersky software to guarantee its security, is he the source of a lot of the stuff that the Russians have released as Guccifer 2.0 or as Shadow Brokers? What do you think?

**Nick Weaver:** [00:09:17] I don't think so. So let's remember what the Shadow Brokers dumps were. There were three dumps of tools and one dump of a workstation's working set. For three of the four dumps, two of the tool dumps and the Windows workstation, these were personalized. These were working sets of individual operators. So a data packrat wouldn't get those particular instances. So like a data packrat might get the router tools or the mail server tools but wouldn't get the router tools as being used in a particular campaign targeting particular IP addresses with the notes files on how my

targeting is going and what my progress is. So what I suspect happened is both this guy and [Harold] Martin were data packrats that were caught up when the NSA went, "Oh, crud," and started basically doing an overall revamp of the security among the TAO [Tailored Access Operations] side and found these two. I think reading Mike Rogers' sentencing statement that Pho did result in the compromise of hacking tools on the Kaspersky incident and that caused the NSA to have to retrench a large number of tools. I think how serious it is is saying that this is somebody who is pleading out to a single count of mishandling classified information. And I think he's going to face a sentence greater than Reality Winner did.

**Stewart Baker:** [00:11:08] And probably deserves it. Right? I mean he didn't have intent.

**Nick Weaver:** [00:11:12] Oh, yeah!

**Stewart Baker:** [00:11:12] But the impact of his mistake is just really dramatic.

**Nick Weaver:** [00:11:16] Yes. Although the other interesting thing is the judge himself flagged the rules for the peons are different from rules for the rulers in that David Petraeus pled guilty to the same charge and got a literal "ouch that hurt" slap on the wrist.

**Stewart Baker:** [00:11:36] Well, because the woman he allowed to read his diaries also had a clearance and, as far as we know, didn't compromise in any way that had an impact on the government, which is fair. He cautioned her about the sensitivity of that data in a way that she seems to have taken to heart. I think it's easy to say, "Oh, well he's a big shot, and he got a good deal because of that." And maybe he did, but I think they are different cases.

**Nick Weaver:** [00:12:04] Oh, agreed. But it also shows the problem of having given him such a good deal is that it makes it harder to sentence people like Pho who really do

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

deserve the several years in prison because it's very easy for the lawyers on the defense – and the judge, even – to make the comparison.

**Stewart Baker:** [00:12:29] So you know I agree with that. But I will say when I was at NSA we had people who took stuff home usually for the best of motives, and this guy seems to have had the best of motives, as well. He thought he was not living up to the standards of the team and that he had to get better, and he wanted to practice and he wanted to study. And so he took it home for those purposes. And so it was a dumb mistake. It's just that the consequences of a dumb mistake when I was general counsel were that you had a bunch of stuff sitting around your study and if the Russians knew enough about you to break into your study, they could steal your stuff, but probably they didn't. Whereas once you put it on the Internet, they can find you, and they will find you, and they'll steal the stuff and all the consequences will flow. So he deserves a much tougher sentence than the people that we caught taking stuff home who mostly just lost their clearances and sometimes ended up with a misdemeanor. But I do sort of feel sorry for the guy. He's like 70 years old, and he's doing his best to improve himself. And he's walked into a buzz saw.

**Nick Weaver:** [00:13:51] Yep.

**Stewart Baker:** [00:13:51] Okay. Speaking of buzz saws, the New York attorney general has written a report on virtual markets and cryptocurrency. It's pretty detailed, and there's some interesting aspects to it. I'm going to ask Evan to give us an overview.

**Evan Abrams:** [00:14:10] It is pretty detailed. It's 40-something pages, and it originated starting back in April when the attorney general sent out a questionnaire to the 13 probably largest cryptocurrency exchanges out there depending on how you measure it, nine of whom chose to participate. Four exchanges declined to participate and said that they don't do any business in New York and therefore they did not feel the need to respond to the attorney general's office. The report's really aimed at kind of your average mom and pop crypto investor, if you will, and tries to kind of lay out risks and considerations that people should be focused on when using these exchange platforms

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

and particularly some of the differences between kind of your average investor and your professional investor who's using you know automated trading and things of that nature.

**Stewart Baker:** [00:15:08] So essentially they said if these crypto exchanges were the New York Stock Exchange, what would they be doing differently from what the crypto exchanges are doing and tagged all of the conflict of interest issues and the like – auditability problems – essentially treating them as though they were a pretty sophisticated exchange.

**Evan Abrams:** [00:15:33] Exactly. Throughout the report in a number of places they compare these exchanges to the New York Stock Exchange or Nasdaq and the varying levels of regulation between those entities. The report summarizes kind of three major concerns or takeaways, although there's obviously more than that throughout, but the three "key findings," as the report calls them, have to do with potential conflicts of interest on the platform. So that relates to both entities trading on the platform, employees of these entities trading on the platform, and then also concerns around if they're receiving consideration for listing certain currencies or tokens. The other two key findings were concerns around abusive trading or market manipulation and what the report cites as lack of effective controls around that issue. And then concerns about protection of customer funds with regard to issues of hacking. Obviously there's been a number of major exchanges that have been hacked in the last couple of years. And the report points out that there's no insurance for these exchanges like there is for many of your traditional financial institutions or banks where you would typically hold your funds. There's no FDIC or other similar type of insurance.

**Stewart Baker:** [00:16:48] Well, you know the FDIC is like a federal program. So I can't get insurance for what I buy on the Nasdaq, can I? So it's a little bit unfair to say, "How come you don't have...?"

**Nick Weaver:** [00:16:59] Actually, yes you do.

**Stewart Baker:** [00:17:00] Really?

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

**Nick Weaver:** [00:17:00] You have SIPC [Securities Investor Protection Corporation].

**Stewart Baker:** [00:17:02] Oh, okay. Well there you go. Goes to show I never buy anything on the Nasdaq. [Laughter]

**Evan Abrams:** [00:17:07] A number of exchanges I think have made the point and would make the point that they're not ready insurance products for most of these exchanges that they can just go out there to an insurance provider and get something like this. And it would probably be quite expensive if there were a kind of tailored crypto exchange insurance.

**Stewart Baker:** [00:17:27] But overall you know as cryptocurrencies and crypto exchanges become more mainstream and make more money, this reads like an agenda for regulating those currency exchanges so as to make them equivalent to Nasdaq and the New York Stock Exchange.

**Evan Abrams:** [00:17:49] It does definitely have a flavor of that, and it's worth pointing out that New York has probably the most detailed and complex regime at the state level for governing cryptocurrency business activity there. They have the New York BitLicense regime which...

**Stewart Baker:** [00:18:02] Oh, yeah. Which got panned by a lot of cryptocurrency companies, didn't it?

**Evan Abrams:** [00:18:09] So a lot of companies decided that it was going to be too difficult to obtain a license or that the regulations they felt were going to be too burdensome. So a lot of companies left New York altogether after the BitLicense came out. Recently there's been a few more companies that have been moving back to New York or applying for the BitLicense, but there are still not many companies that have received a BitLicense. Can't recall what the exact number is right now, but it's less than

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

10. It's a pretty small amount. So most companies have chosen to avoid the state. And one of the interesting...

**Stewart Baker:** [00:18:40] Well, you know some of them are going to get dragged kicking and screaming back to the state. Right?

**Evan Abrams:** [00:18:44] Yes. Well, one of the interesting takeaways from the report is that three of the four exchanges who declined to participate said, "We don't have anything to do with New York." The New York attorney general actually referred three of those four exchanges to the New York Department of Financial Services, who's the entity that issues and oversees the BitLicense. And presumably the State of New York intends to argue that those exchanges were engaged in some sort of virtual currency business activity within New York. So we'll have to see how that...

**Stewart Baker:** [00:19:17] Knowing how New York defines what it takes to owe taxes in New York, wouldn't surprise me. Nick, you've been critical of the industry. Is this sort of form of pretty aggressive look like the New York Stock Exchange regulation where we're going to end up?

**Nick Weaver:** [00:19:36] I think so, but I think this is actually way too light touch. So the problem is the cryptocurrencies are actually incompatible with modern finance because of the irreversibility. So this is why you can't get good insurance for cryptocurrency. There's also liability shifting. So with Coinbase, for example, if your account gets hacked, somebody steals your money, Coinbase's response is, "Sorry for your loss." But if your bank account or...

**Stewart Baker:** [00:20:08] So what you're saying is all these things are designed to kind of close the transaction right away and not allow you to pull it back, whereas if it were the New York Stock Exchange, everybody would know where the money went, where the stock went, and could say, "That transaction's got to be reversed."

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

**Nick Weaver:** [00:20:28] Yes. And reversibility is the key tenant for modern electronic finance because reversibility enables fraud mitigation, the ability to go, "Oops, undo," and at least for a limited period of time undo it.

**Stewart Baker:** [00:20:43] Alright.

**Nick Weaver:** [00:20:44] You don't have that with cryptocurrency, so that's why the exchanges get hacked all the time.

**Stewart Baker:** [00:20:49] So let me ask another blockchain question because blockchain's reputation for security is also being used to justify voting on mobile phones in West Virginia.

**Nick Weaver:** [00:21:06] Oh...

**Stewart Baker:** [00:21:06] [Stifled laughter] I'm not going to laugh. West Virginia has allowed 24 counties to experiment with vote by mobile phone. And it's all secure because it's on the blockchain.

**Nick Weaver:** [00:21:15] Pfft! First of all, this is not a blockchain project. It's the same as the Walmart thing. You're calling it a blockchain when you have a limited number of authenticated writers. Basically it's called a brain-damaged git archive being sold to upper management with the magic word that causes people to shove money at you.

**Stewart Baker:** [00:21:39] So let me push on that. It is a way – and people have put a lot of money into making blockchain easy and relatively standardized, like IBM, and so taking advantage of that – I mean the Internet is just a way of trading data between computers, but the fact that it was a protocol, the fact that was easy, enabled the Internet economy. Aren't we going to see something like that? The blockchain is just a well-developed technology for keeping track of transactions in a ledger?

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

**Nick Weaver:** [00:22:13] No. Because the thing is is anything that could have benefited from an append-only ledger with a limited set of writers – all these private or permissioned blockchain business – that's 20-30 year old technology. We've known how to build it for decades, which means all these private or permissioned blockchain projects are one of two things. It's either internal where I've got to clean up data formats, state exchanges, etc. But if I say "blockchain," management will actually fund the necessary upgrades. Or it's consultants from IBM or whatever using the magic word "blockchain," which causes upper management's eyes to glaze over and throw more money at the consultant.

**Stewart Baker:** [00:22:57] Alright. So I take it then you think that not only does blockchain not solve the security problem here but that even saying blockchain is relevant here is a bit of a misrepresentation. And so why is West Virginia doing this?

**Nick Weaver:** [00:23:19] Because they want a vote-by-phone system for overseas military. That as much as I hate the notion of Internet-connected voting because of potential fraud issues, that's actually an okay-ish objective in the very limited context of you're only using it for overseas military personnel in lieu of paper ballots. But what's wrong with paper ballots?

**Stewart Baker:** [00:23:50] Yeah, it's a fine cause. We can stipulate that it's a good thing if we could do it, and neither the military nor the election boards have really covered themselves in glory in enabling folks who are a long way away and maybe under fire to vote. But this strikes me as ultimately going to end in tears.

**Nick Weaver:** [00:24:17] I agree.

**Evan Abrams:** [00:24:18] There was a statistic that came out on this: something like half of the military absentee ballots that came in from overseas in West Virginia came in too late in the past election.

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

**Stewart Baker:** [00:24:29] That's partly because the military has been slow to deliver them and partly because the secretary of state is slow to fix the ballot so that it can be sent out.

**Evan Abrams:** [00:24:39] Right. So yeah, I mean I think it's...

**Nick Weaver:** [00:24:42] Partially what makes me think might be able to improve the process is a bit more common infrastructure. So a way where any local municipality can submit a PDF of the ballot. It gets printed out at the military installation and scanned there. And yeah, you keep a copy of the paper ballot, but you count the scan for convenience.

**Stewart Baker:** [00:25:11] Yeah, you could do that. You're right. People are overthinking this, I suspect, and we'll regret it, but eventually hopefully it will settle out. Quick set of topics. There was a story suggesting that the GRU had developed tools that were persistent even when you reinstalled your operating system. That obviously is the "P" APT, the persistence. I wasn't sure that was all that new a development.

**Nick Weaver:** [00:25:45] No it isn't. The NSA has been doing that for years. They've got a couple of software implants that actually go into the disk controller rather than the BIOS.

**Stewart Baker:** [00:26:00] Oh, that's even deeper. And I take it you're relying on leaked material that might not have been Snowden leaked but was leaked as part of the Snowden era by Jacob Appelbaum.

**Nick Weaver:** [00:26:14] Yep. And the problem is once that was leaked, two different groups developed two separate versions targeting two separate disk controllers just for the heck of it within six months.

**Stewart Baker:** [00:26:27] Yeah. Alright. Other topics. A content moderator who works for a contractor to Facebook says that looking at all those beheadings and child porn

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

videos gave her PTSD, and she wants to hold Facebook liable. I don't at all doubt you can get PTSD from looking at that stuff. It's horrible. I used to know people who were responsible for some of that, and their favorite technique was to take a big yellow Stickie and put it in the middle of their screen so they couldn't see the most horrible parts of the video but they could still figure out what was going on. But I'm guessing 20% or less chance that a lawsuit like this will succeed because essentially they have to say that Facebook was negligent in not figuring out a way to prevent PTSD, and I'm not sure there is a way. India's Supreme Court has upheld the Aadhaar program that we talked about recently that had been kind of hacked by people who wanted to create identities. And the Supreme Court said, "Yes, this 1.2 billion person database is fine, along with the credentials that go with it. But we're not going to let you authorize banks to demand it as well as government services," although there is an expectation that maybe new legislation would allow that. So Aadhaar is here forever, and it's time for them to figure out how to make it more secure. Facebook got hit for 50 million accounts compromised and then realized a little later that the compromise – which I suspect is going to end up like Uber. It's not clear that anything bad happened as a result of this, but 50 million is a big number. And then 40 million more for people who use Facebook as their login credentials. So if you say, "Yes, log me in using Facebook," well, there were 40 million accounts that were apparently compromised that way, which is actually kind of more the worry. I don't know. Nick, do you agree?

**Nick Weaver:** [00:28:41] Yeah, and it's also unclear whether that 50 million is actual deliberate compromise or just the condition that could have resulted in compromise.

**Stewart Baker:** [00:28:56] Ah, yeah. Yeah.

**Nick Weaver:** [00:28:56] Because it was with the "view as other person" mode.

**Stewart Baker:** [00:29:00] So the problem Facebook had here – and we're going to see this over and over again. This is law an action, folks! The GDPR says you must disclose your compromises within 72 hours. It looks like Facebook kind of did that and having done that had to keep investigating after it had made the disclosure, which is probably

why it went from 50 million to the additional 40 million. Alright. Trump has accused China of interfering in midterm elections on the theory that why should the Democrats have all the fun. And I thought it was interesting. His example was an Iowa newspaper insert that the Chinese had written. This is a pretty common thing for foreign governments to do: to write a little insert that slides into the paper that tells you how wonderful it is to invest in their country. But the Chinese apparently devoted big chunks of it to explaining why President Trump's trade war was bad for Iowa farmers. And Trump thinks that's fake news and it's interfering in our election, and he's not completely wrong, so you know it's close enough for a tweet.

**Nick Weaver:** [00:30:15] And of course, whether or not it's actually true is kind of relevant. You just call it fake news and rant at it anyway.

**Stewart Baker:** [00:30:22] Well, you know maybe it is bad for Iowa farmers, but I'm not sure that we should feel comfortable having the Chinese weigh in on who should be elected for Congress from Iowa. Okay. Bunch of reports that came out. I'll just bang through them. The Europeans reported that they have gotten most of Silicon Valley to agree to nuke disinformation on their services. Lots and lots of stuff about what all these services are going to do. What's missing is a definition of “disinformation.” Why do I think that's important? Because I think the Europeans believe that disinformation is anything that is tweeted by Donald J. Trump, but they don't want to say so, so they're not going to define it. So we're going to see information taken off of American media services to satisfy European notions of disinformation. Just saying. DOJ has put out a report. I went to a long meeting at the Justice Department with lawyers for people who suffer breaches. And they then encouraged us to take home their report, which is not bad. It's kind of best practices for what to do if you've had a breach. It's worth reading. They've done better best practices papers, but this is not terrible. But for one thing – well, maybe two. They throw regulators under the bus, saying, "It is worth noting that the Justice Department does not have a regulatory role in regard to data breaches. Accordingly, reporting a cyber incident to the Department or to federal criminal investigators will not lead to regulatory enforcement action by the Department for the incident." Basically saying you can tell us. We won't tell the rest of the federal

government about what happened to you, which you know shows just how hard they're having to work to get people to show up and disclose. And then you know very sadly CCIPS [Computer Crime and Intellectual Property Section of DOJ] has persuaded yet another administration to double down on the idea that hacking back is a terrible thing and they say you know, "Victim organizations should not unilaterally respond to an incident by accessing, modifying, or damaging a computer it does not own or operate, even if the computer appears to have been involved in an attack or intrusion." I talked to Justice officials about that. They do have new and better stories about why it's a bad idea. We're not going to delve into them today, but I'll get them on to have that argument and move it a little forward. But I'm guessing that Representative Graves if you were hoping that this administration was going to endorse the ACDC [Active Cyber Defense Certainty] Act, don't count on it. And the Australian Strategic Policy Institute says China is back and stealing our stuff, that they never really gave up on stealing commercial data. They just gave up on the idea that they might get caught, and so they are doing it much more subtly and more selectively. That's an analysis of several countries. I think the Council on Foreign Relations contributed to that for the US, if I remember right. And Nick, I'll ask you: does that sound right to you?

**Nick Weaver:** [00:34:02] Yeah. Sounds about right.

**Stewart Baker:** [00:34:05] Yeah, that's kind of... And look, let's not forget that's a deal we would have taken. We indict these guys, which costs us relatively little, and we scare them into not going into systems without lots of controls and back out options and double blinds designed to make sure that they don't get caught, which makes them less efficient at stealing stuff that you know if all you have to do a smash the window and grab everything, you're going to get a lot more than if you have to you know *Topkapi* style come in through the ceiling. And now they are much more in cat burglar mode than smash and grab mode, and you know that's better than nothing. Federal CIO says we need more cloud. House has a report on artificial intelligence that is nice for its bipartisanship, but the bipartisanship means it's pretty anodyne. And NIST has a new set of IoT standards because why should they be the only ones who don't have IoT standards for people to suggest. So lots of reports out there, and if you don't have time

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*

to read them, we've read them for you. Okay. Nick, Evan, thank you for joining us. That's going to end our program because we don't have an interview today. This has been Episode 233 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Don't forget: send us names for guest interviewees, and we will send you one of our highly coveted Cyberlaw Podcast mugs. If you want to send those suggestions, get them to CyberlawPodcast@steptoe.com. I have not gone back to my practice of trying to tweet the stories we're going to cover in advance, but I'll start doing that at @StewartBaker on Twitter and LinkedIn. Please do go and rate our show. You've heard the pitch. You've heard it from everybody. So if you like the show, please do that. If you like the quality of the audio, go back and say, "Hey, the audio is much improved!" Coming up we've got Suzanne Schwartz, who's going to tell us why we shouldn't worry about hackers taking over our heart implants – or why we should. The general counsel of the UK's version of NSA – GCHQ – is going to be on. It's very exciting. First guest we've had where we couldn't actually use his last name. And Chris Krebs is going to explain to us why West Virginia's system isn't so bad – or maybe it is so bad – and what DHS is doing about the security of election systems. He'll be on before the election, so we'll get to hear about that. Not sure he's going to cover Iowa newspapers. And finally show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett's our audio engineer; Mike Beaver is our intern; Stewart Baker is your host. We hope you'll join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.*