Steptoe

Episode 231: Ah, September, when Europe unleashes a summer's worth of crazy

Stewart Baker: [00:00:04] Welcome to Episode 231 The Cyberlaw Podcast brought to you by Steptoe & Johnson. Thank you for joining us. We are here in the new studio that we are just furbishing. It's not complete, but it's pretty good. We'll send pictures around from the event. We're lawyers talking about technology, security, privacy, and government, as you know. And we've got a great panel today. For our guest interview and hopefully weighing in on some of the news items, Michael Chertoff, co-founder and executive chairman of the Chertoff Group, formerly my boss [as] Secretary of Homeland Security, and the author of *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*. Welcome, Secretary Chertoff.

Michael Chertoff: [00:00:52] Thank you.

Stewart Baker: [00:00:54] And speaking of people who worked for Michael Chertoff, Paul Rosenzweig, the founder of Red Branch Consulting and senior fellow at the R Street Institute, former Deputy Assistant Secretary for Policy at DHS. Welcome, Paul.

Paul Rosenzweig: [00:01:09] Thanks for having me, Stewart.

Stewart Baker: [00:01:11] And Matthew Heiman is here. Visiting scholar from George Mason University's National Security Institute, formerly with the National Security Division at the Justice Department. Matthew, it's great to have you.

Matthew Heiman: [00:01:22] Pleasure to be here.

Stewart Baker: [00:01:23] And Gus Hurwitz on Skype. Associate professor of law because he's got tenure and co-director of the Space, Cyber, and Telecom Program at the University of Nebraska. And for those students and law professors who are listening to the program and who have been impressed by Gus's contributions, he's now poachable. Your law school could try to hire him away, at least as a visiting professor. Welcome, Gus.

Gus Hurwitz: [00:01:54] Now you're really just trying to get me in trouble, Stewart.

Stewart Baker: [00:01:57] [Laughter] You can deny it. Feel free.

Gus Hurwitz: [00:01:59] And I will, in case my dean is listening.

Stewart Baker: [00:02:01] Alright. And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. Let's jump right in. The National Academy, Paul, has a report out on securing the vote. You took a pretty good look at that. What did you think?

Paul Rosenzweig: [00:02:16] I think like most National Academy reports, it is pretty solid technically. And the real question is whether or not there is political will to implement it. It has a series of recommendations, as such National Academies reports have, the most salient of which are: at least have paper backups...

Stewart Baker: [00:02:37] Right.

Paul Rosenzweig: [00:02:38] ... and do risk-based auditing of results, which is different from how we do recounting now everywhere except in Colorado, who's only done it for a couple years now. And there are others. You know like most reports there are 26 recommendations or something like that.

Stewart Baker: [00:02:53] The big ones are: you should use paper; forget machines.

Paul Rosenzweig: [00:02:56] Or at least have paper backup. Right? There's only five states that still have DRE, direct recorded elections, without any paper backup, and in fact there's a hearing going on in Georgia as we speak about whether or not the court there is going to order Georgia to close down its direct recorded election system and reinstitute some form of paper backup 50 days before the election. So I really wouldn't want to be the election commissioner in Georgia if he was ordered to make a change.

Stewart Baker: [00:03:26] That would be tough.

Paul Rosenzweig: [00:03:26] Yeah. Very hard. I mean I...

Stewart Baker: [00:03:28] Luckily we're probably not at risk of running out of paper.

Paul Rosenzweig: [00:03:31] That's true. I do think it is the right answer, which is that we have to take risk-limiting, risk-mitigating steps to secure the election infrastructure in the same way that we've spent the last 10 years kind of hardening the electric grid or the transportation grid.

Stewart Baker: [00:03:48] Yeah, although this is what's interesting about this is that we're going full Luddite. We're just throwing the computers out.

Paul Rosenzweig: [00:03:55] Well, you know I mean there was a report about five years ago in the Air Force, and they're keeping about a quarter of their systems that do the nuclear missiles in analog precisely for the same reason, which does make it seem a little silly that we have to be Luddites in order to be effective, but it's the reality of where we are.

Stewart Baker: [00:04:14] Okay. Audits? That's not something we do now. It makes all sense in the world that you would want to make sure that your systems are actually doing what you think they're doing. But that's been surprisingly controversial. The effort to require states to do that has led to legislation at the federal level getting stalled.

Paul Rosenzweig: [00:04:36] Yeah, well, I think that the resistance in the states is as much know political prerogative and all that.

Stewart Baker: [00:04:42] Oh, yeah.

Paul Rosenzweig: [00:04:43] There's also a cost factor, which is it's clearly one of those typical federal mandates without any backup payment. On the other hand, you know the ability to actually do statistically significant audits and give you confidence that the result reported is the result that was produced is I think a really valuable way of cross-checking ourselves and should be considered by any state that has enough funds to pay for it, even if the feds didn't order you to do it.

Stewart Baker: [00:05:17] Alright. Let's change gears and locations. Boy, you know September 1 comes and the Europeans just...

Paul Rosenzweig: [00:05:27] [Laughter]

Stewart Baker: [00:05:27] They all come back, and they have the craziest ideas. It's just amazing how much news they've made in the last week and a half. And Gus, one of the news stories was a European Court of Human Rights [ECHR] ruling on GCHQ's mass collection of intelligence, essentially telecommunications en masse that could be searched later, and ECHR actually didn't say it was a bad thing. They just said it needed some constraints. Is that right?

Gus Hurwitz: [00:06:12] It kind of is. This is a puzzling opinion and a fascinating one, and I really look forward to seeing what comes next. So the basic holding of the ECHR was that there were inadequate safeguards to protect bulk data collection including in particular related data sort of collection. And this was on the collection side of things, not the subsequent searching side of things, but as you note, the court expressly seems to say that bulk data collection isn't inherently problematic. It just needs to be done with adequate safeguards to comply with the Convention on Human Rights. Now it's unclear to me how you actually implement that. If you need to know what data you're going to

be collecting beforehand in order to implement these safeguards but you need to have the data collected in bulk in order to know what the data you're going to need to be able to search, it's really hard to know how you implement that. But the fascinating thing I think here is – I'm going to speculate and say pretty much all the major European countries are doing things like this. And one of the notable things the commentary has said about the GCHQ program is it's very similar to what we in the United States were doing. And it's really easy to play politics when the concern is about the United States violating these European protections. But this is starting to force the gaze inward, and something's got to give. Either the EU is going to need say, "Okay, we need to stop doing our collection entirely," or they're going to need to say, "Okay, those standards we've been holding the US to in these political talks and the failed Safe Harbor and Privacy Shield negotiations? Maybe we need to give a little there because we can't hold the US to higher standards than we're going to hold ourselves."

Stewart Baker: [00:08:18] So I think it's significant that this is the European Court of Human Rights, and it has pretty consistently seemed more sensible on this issue than the European Court of Justice, which has mostly seen these cases in the context of beating up the United States. And it has done it with an enthusiasm and irresponsibility that is staggering, whereas the European Court of Human Rights actually has kind of thought carefully about this and has essentially said, "Of course we're not going to stop bulk collection. Terrorism is a serious problem, and this is the only answer we have to it." Let me actually see if I can get Secretary Chertoff to jump in on this because this is – the European Court of Human Rights opinion at a high level is not so different from what you say about the future of data protection from government data programs going forward in the world that we're going to be facing.

Michael Chertoff: [00:09:22] That's right because I think what it recognizes is there's a tension between two impulses that you can only reconcile if you unpack really what is involved in surveillance. On the one hand, if you say you don't collect the data, when you do come across a relevant data point, you have nothing to compare to. You've lost the trail, so therefore you miss opportunities that would be justified to do searching. On the other hand, I think we all understand you don't want to have willy-nilly huge amounts

of data being rifled through by the government looking for whatever they're looking for. So one way to reconcile these is to say collection under a relatively relaxed standard is okay, but you can only hold it and not look at it until you have some more specific predication. So that reconciles two arguably inconsistent but necessary facets of surveillance.

Stewart Baker: [00:10:15] Yeah, and that is sort of what the ECHR said here. Well, I want to get through the full European wackiness. The copyright bill. Matthew, there's a copyright bill that is not quite done, but it's 90% done. And my guess is that there aren't going to be big changes because there are lobbies both sides of the issues. It is an astonishingly aggressive enforcement of intellectual property rights, isn't it?

Matthew Heiman: [00:10:52] Yes, and it's also an astonishingly protectionist piece of legislation that falls right in line with what Europe is doing when it comes to major tech platforms. So the upshot of the bill is that if someone posts copyrighted material on YouTube, which is owned by Alphabet/Google, or Facebook or anywhere else, those platforms become responsible for getting rid of it, and if they don't get rid of it, they're at risk.

Stewart Baker: [00:11:17] And they need the automated protocols for doing that, which means you know hashes and stuff that will almost certainly interfere with fair use at a minimum as well as being over-protective generally.

Matthew Heiman: [00:11:31] Exactly. And the thing that's striking to me about this is if you look at the winners and losers as a result of this legislation, the losers are the major tech platforms which tend to be US companies. The winners are newspapers and magazines. There's lots of those in Europe. And the other winner[s] are sports franchises because the other part of the bill talks about the fact that if you're at a stadium watching Liverpool play Manchester United and you take photos or you've got a video and you post it to Twitter, the sports franchises can force that to be taken off. So it's striking to me that the bill protects sports franchises, and we know Europe has some of the most valuable sports franchises in the form of soccer and Formula One race

teams. So being very cynical and jaded about a lot of European legislation, I think this is just another pot shot at US tech firms.

Stewart Baker: [00:12:20] Plus it keeps all of the dark money flowing to FIFA.

Matthew Heiman: [00:12:24] Exactly.

Stewart Baker: [00:12:25] Okay, so that's not the only anti-Silicon Valley measure that they're pursuing.

Matthew Heiman: [00:12:34] Right.

Stewart Baker: [00:12:35] Paul, they told the tech companies they have to take down terrorist messages within an hour?

Paul Rosenzweig: [00:12:43] Yeah, they did.

Stewart Baker: [00:12:45] Okay!

Paul Rosenzweig: [00:12:45] And if wishes were fishes, we'd all never starve. This is one of those you know the tech companies need to "magic harder."

Stewart Baker: [00:12:59] Nerd harder.

Paul Rosenzweig: [00:13:02] Nerd harder. Okay, not magic harder. It's obviously a completely unreasonable request. And what it really reflects – and this is kind of a slightly deeper point than Matthew's protectionism, with which I agree – it's discretionary. It's devolving everything to the discretionary judgment of European regulators. Right? Because everybody's going to violate this, so who gets fined will be at the whim and judgment of you know some privacy protection data DPA [data protection agency] in Sweden.

Stewart Baker: [00:13:44] I used to compare it to French parking regulations. Everybody parks on the sidewalk, but only the people who don't tug their forelocks for the cops have to pay.

Paul Rosenzweig: [00:13:52] Exactly. And frankly this is true of a lot of how Europe is developing its privacy regulations these days. The GDPR is essentially a formula for privacy rule by unaccountable, unelected DPAs in Europe that they hope to globalize. And then this is just part and parcel of that.

Stewart Baker: [00:14:14] So what should we make of the fact that in the right to be forgotten case, Europe is divided? Some are saying – the French are saying, I think the Austrians are saying – "Yeah, we're going to impose this censorship regime on anybody anywhere, and Americans shouldn't be able to read stuff about Europeans who want to be forgotten." And the European Commission has said, "Well, not so fast. Maybe we should be more cautious than that."

Paul Rosenzweig: [00:14:44] I would make of it that the European Commission recognizes that going too far down this road is sauce for the goose, sauce for the gander, very much like what Gus was saying about the inconsistency of holding GCHQ to the standards that had heretofore been imposed only upon those evil Americans.

Michael Chertoff: [00:15:02] Yeah, also if you're going to allow the exporting of a rule like this, what's to stop the Chinese from saying, "Well, you know what? We're going to punish you if you run anything by the Uyghurs or anybody who doesn't agree with Xi Jinping." I think there may be a dose of reality that's moderated here.

Stewart Baker: [00:15:19] Or criticizing Erdogan from Turkey. There's plenty of laws in Turkey that say that you can't do that, and they'd be happy to say you can't do it anywhere in the world. But that is where we're going, I suspect. I want to move through a bunch of these cases.

[00:15:39] [Laughter]

Stewart Baker: [00:15:39] I know. Social media bias. I actually got to play in this sandbox briefly. I saw somebody claiming that he had linked to Alex Jones's Info Wars. I'm not a big fan of Alex Jones, but I thought well it cannot be the case that you would be banned from Facebook for linking to an Info Wars site. So I took my social media status in hand and put it at risk and actually linked to him to see if Facebook would take me down, and they did not. And in fact they have later said that it was a mistake to have taken down this guy's account for the link. The lesson I draw from this is it's almost impossible to tell or to get ground truth on what kind of bias is being exhibited by social media platforms because they have so many ways to tailor what they do to individuals that you think you've tested whether they're doing something and it may just be that they're not stupid enough to take down an account that isn't obviously on the margins. Let me ask Gus to talk a little bit about one of the efforts to deal with fake news and to do so in an unbiased way. *The Weekly Standard* has been asked to do accuracy checks on stories. This was a surprise to me because they're obviously right leaning, and most of the fact checkers lean left. What's the story there?

Gus Hurwitz: [00:17:40] Yeah, so this is a counter-example perhaps to the lack of transparency on how social media is trying to police bias, and it's perhaps a cautionary lesson for what happens when social media is upfront about what they're doing. So Facebook has brought on board five agencies: the Associated Press, Politifact, Snopes, FactCheck.org, and as you note *The Weekly Standard*. And basically all five of them have a veto. Any one of those five can look at a story and say this is factually inaccurate. And Facebook takes that to mean a major or significant fact in this story whether or not that is inaccurate. And if any one of them says, "Yeah, this story has a problem," the article when it is run on Facebook, it will have a warning sign on it. And also it's demoted in their feed. So they lose about 80% of their viewership, which obviously in our ad-driven market can be quite a big loss for news or non-news agencies. So Think Progress had a story about the Brett Kavanaugh hearings with the headline saying Brett Kavanaugh "will kill *Roe v. Wade*." And this was frankly a terrible misinterpretation or misrepresentation of his comments about *Glucksberg* and the sort of thing that only someone who knows very little about the law but enough to be

dangerous could come up with and draw some connections to. And *The Weekly Standard* called it out and said, "No, that's not what he said. You're drawing some inferences." And Think Progress threw a fit. They said, "We've got no way to appeal this. We're losing tons of traffic as a result of this. Why does *The Weekly Standard* – this political organization, right-wing partisan, and all of this terrible stuff that the press doesn't like to have in it – why do they get to veto our coverage?" And to their credit, Slate wrote a story covering this saying, "Hey, Think Progress, you're on the wrong side here. Your headline is factually inaccurate." So good on you, Slate, and you get some factual accuracy points there, but there are a lot of I think really interesting questions in this case. First, Facebook, their general perspective – and this sounds familiar for most social media – is our hands are tied. These are our fact checkers. We're not going to second guess them. You can hear echoes of Section 230 through this, but *The Weekly Standard*, they're a news organization. They get to call out factually inaccurate stuff just as much as Snopes. But there are interesting institutional structure questions here. Should it be a single vote? Should Facebook have a formal appeal process? Is the penalty too high? I think it's really interesting that Facebook is experimenting with this. I think it's laudable that they have *The Weekly Standard* included, and perhaps they're the wrong organization. Perhaps – I won't pick on *The Weekly Standard* – perhaps Politifact will have a run of four or five bad calls at which point maybe Facebook then should say, "Okay, you've had a bite at the apple and a second and a third bite at the apple. We're going to cycle you out of our fact check group. Or we're going to bring some others in. Or we're going to switch this to require two organizations to throw flags, per se." But it's been a bit of a mess for Facebook. And I think it's at least better than the Twitter scenario that you described, Stewart, where we don't know what's going on. At least here we do so we can talk about it.

Stewart Baker: [00:21:49] So fake news is one way by which the platforms decide who can speak and who can't. Hate speech is another. And, Paul, Twitter has a new definition of hate speech or a new example of hate speech as I understand it. Now if you talk about illegal aliens, you're engaging in hate speech?

Paul Rosenzweig: [00:22:17] Well, that seems to be the case. I suspect we're in the middle of the story that your example with Info Wars will get us to the end of, which is to say I suspect that won't be the case for too long because it's a pretty silly position especially since it's a phrase that has found its way into Supreme Court opinions and has a legal provenance as well. But it does show both the dangers of asking social media to be content moderators and also the virtues of making it a private company that does it. At least it's not the government calling it hate speech. And if you don't like Twitter, you can get off the medium and start a separate one. Yeah. If we're going to ask social media to do any content moderation at all – and we're going to because at least you know child pornography, Nazi speech, we're going to – they're going to make mistakes, and this seems clearly like one of them.

Stewart Baker: [00:23:26] So okay, I want to move on. The meltdown of security on the Aadhaar identity database in India is a fascinating story, but I don't think we have time to talk about it, and its policy implications are kind of minimal. Same thing is true. There was an endless story about how IBM had developed technology to go through CCTV footage, and one of the ways you could search it if you were doing face recognition is by skin color. And the 12-page story basically seems to say, "Well, that's got to be shocking. Who's responsible for asking that?" I can't understand why you would not want to be able to say if they tell you that the suspect was Caucasian, you could say, "Okay, go through this crowd and eliminate the people who aren't Caucasian so we can start looking for the suspect." But apparently just the idea that would recognize that there are different skin colors is too much for some of the reporters. I want to skip those and go right to a bill that's gotten almost no attention and which the California governor's probably about to sign. And that is the IoT security bill. The bill is pretty modest in some respects. It basically says you have to have reasonable security, and by that we mean – if you're selling IoT devices – we mean you either force people to change the password or you have a unique password for every single device you sell – it's probably pasted on the device – which sounds like you know not a bad idea but a little incomplete. Thoughts?

Matthew Heiman: [00:25:41] This struck me as the California attorney general hunting license bill.

Stewart Baker: [00:25:46] That's for sure because there's no private right of action.

Matthew Heiman: [00:25:49] There's no private right of action.

Stewart Baker: [00:25:49] The California attorney general is going to be almost as important as the European Commission.

Matthew Heiman: [00:25:56] Well, or a mini-FTC, right, where when you're trying to figure out what exactly you're supposed to do as a device manufacturer, it's got to be appropriate and reasonable according the language of the bill and have the password option. But otherwise it's really in the attorney general's hands to figure out what appropriate and reasonable is. And it strikes me that we're going to have all these manufacturers bear those costs of creating this password issue, but I'm not sure that solves the issue of IoT security.

Stewart Baker: [00:26:25] No, they have to be updatable at a minimum.

Matthew Heiman: [00:26:27] Exactly.

Paul Rosenzweig: [00:26:28] It's a protection against like the rarest, stupidest bruteforce attack and nothing more. I'm going to echo a couple of security researchers who I've spoken to and read about this and you know it's the "magic bullet" of adding a security feature instead of going back to the beginning and fixing the security flaw in the first instance. And you know leaving completely aside the absurdity of the litigation uncertainty that it creates, it's just not going to make anybody safer, at least not much.

Stewart Baker: [00:27:04] A little bit, maybe.

Michael Chertoff: [00:27:05] I disagree. I think it's not complete. It solves one problem. There are other problems. But the point is it opens the door to what I think is important, which is you've got to build into these multiplying devices some reasonable level of security recognizing you're not going to necessarily defeat the most adept attackers. But I think what's emerged in the last year or so is that getting a poorly protected device and connecting it your network is not just a problem for you as the consumer, but it's a problem for everybody else when they get taken over and become part of a giant botnet. So at that point it's not enough to say buyer beware. You've got to tell the manufacturer you own some of the responsibility.

Stewart Baker: [00:27:49] I think that does make sense. Gus, go ahead.

Gus Hurwitz: [00:27:52] I want to hop in with two things. First, I'm going to agree and disagree with the previous comments. I think this is a good step for some problems, but I just really look forward to the California AG trying to bring a suit against a couple hundred, a couple thousand Chinese IoT device manufacturers since a lot of the problem is low-cost, cheap imported devices. And as I read the legislation, it doesn't have any provision in it that expressly disclaims the ability to go after the people selling these devices, electronic marketplaces for instance. The other thing: I just look at this legislation, and I think the D-Link case, the FTC's attempt to bring an unfairness complaint against D-Link for having said it's problematic to say, “To secure your device, change the password.” And this legislation basically says, "To secure your device, make sure you require the users to change the password." So there's a nice conflation or conflict there between the FTC's and the California legislature's understanding of what security requires.

Stewart Baker: [00:29:03] So you know you may be right. I think the California attorney general can sue those manufacturers, can say you must recall these, and if you don't recall it we're going to take this order against you and take it to the ISPs that service your IoT and tell them to turn your IoT off. And when users complain that their device is not working, they will get a notice from the California attorney general allowing them to join a class action against the manufacturer.

Paul Rosenzweig: [00:29:35] I'll make one final point, Stewart, which is to pair this with California's recent new privacy regulations. And what we've seen systematically at the federal level is an inability or an unwillingness to act, and California's doing in this context exactly what it did years ago in terms of car safety and car pollution, air pollution, which is they're trying to use their space as the largest economy in the country to drive a regulatory decision making when Washington is at an impasse. And we've already seen in the privacy sector that that's had a second order impact. The NIST [National Institute of Standards and Technology] is going to issue an RFP for privacy protective technology. There's increased interest in global generalized privacy regulation coming out of Congress maybe or out of the FTC. And I think that this is going to drive the exact same thing in the IoT whether we like it or not. And so it matters to get it right.

Stewart Baker: [00:30:36] So my prediction: 10 more states will adopt this in the next year.

Paul Rosenzweig: [00:30:41] Exactly.

Stewart Baker: [00:30:41] Unless it ends up in litigation challenging its constitutionality, which I think is unlikely. It's going to spread across New York and Massachusetts and Nevada and a whole bunch of states. So, yeah, we are going to live with it, and maybe that's not so bad. We'll talk with Secretary Chertoff about that. Okay.

Gus Hurwitz: [00:31:04] Stewart, I just want to put a quick pin in the idea you mentioned that the California attorney general could go to court and get an injunction requiring ISPs to shut off IoT devices. We'll need to come back to that at some point. Fascinating, controversial, problematic, hard, really good, terrible idea. So there's a lot there.

Stewart Baker: [00:31:26] [Laughter] Yes. That's my specialty. Okay. Thanks to Matthew, to Paul, and to Gus. I want to turn to our interview with Michael Chertoff.

Remember his book is *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*. Great book. I spent a lot of time with it in August and over the weekend. And you know I heard in it echoes of things that you and I worked on when we – and Paul – when we were at DHS, but clearly you've spent a lot of time thinking about these issues since you left government. And you basically have said I think that the kind of data that we collect, the amount that is available, changes everything about privacy and our expectations for government and the private sector. So I thought maybe you could just give us a little overview of why you think that and where you believe that change in the nature of what we collect is driving us.

Michael Chertoff: [00:32:40] I mean in the 10 years since I was in government, I've become familiar with the volume of data we generate, not even intentionally, just by third parties or by things that automatically generate data. And I'm not just talking about you smart device. I'm talking about the fact you go into the grocery store you get a discount if you use your loyalty fob. Use your credit card you have locational data. Use your Fitbit. All of this is stuff that actually occurred after I left. And what I realized was in trying to focus on privacy as hiding your data or keeping confidential, we were chasing after a will-o'-the-wisp because you're not going to be able to do that anymore unless you so radically took yourself off the grid that it becomes almost impossible. One example, one way to be off the grid is to pay cash. I've now walked by stores where they said, "We don't carry cash anymore. You've got to use your credit card."

Stewart Baker: [00:33:35] And it makes a lot of sense for them not to take cash because cash just attracts robbers, pilfering. So you can see why they would just not do that.

Michael Chertoff: [00:33:44] Sure. But it also means you're generating now data, information about every single purchase you make.

Stewart Baker: [00:33:50] Yes.

Michael Chertoff: [00:33:51] And then of course with the advent of the cloud, it's no longer kept in silos, but it can be aggregated. And what struck me was people were complaining after Snowden about the government, but actually the private sector was collecting and using vastly more data and not in order to protect your life but to sell you stuff.

Stewart Baker: [00:34:12] Right.

Michael Chertoff: [00:34:12] Or worse yet as we saw recently to try to coerce you or manipulate you into doing certain things.

Stewart Baker: [00:34:19] Yeah, I always thought that some of the reaction to Snowden and the general Silicon Valley attack on government collection is they see it as a competitor or maybe more fairly they think that concerns about what the government will do with this data slop over and lead to concerns about whether they should be collecting it at all. And so they're happy to say, "Don't worry. The government can't get at it, so you can stop worrying about it and just give it all to us."

Michael Chertoff: [00:34:48] And I think also you know there is a bit of a myth, maybe a kind of self-perpetuating myth, that the government can do much worse things to you than the private sector. But the reality is, for the government or at least for democratic government to do worse things, it's got to be visible and transparent. If you wind up not getting a job because someone doesn't like your eating and sleeping habits, you're not going to know about that, at least under the current state of the law.

Stewart Baker: [00:35:15] Right.

Michael Chertoff: [00:35:16] And therefore that could be a very serious consequence visited upon you with no transparency.

Stewart Baker: [00:35:22] Yeah, I remember that Lyft or Uber or maybe both of them announced that they weren't going to give rides to people who we're going to rallies for

the Proud Boys or some of these groups that are white identity groups. And I'm confident they didn't tell them, "By the way, we hate you, so we're not giving you the service." They just weren't available. There was nobody on the street when you asked for the ride.

Michael Chertoff: [00:35:51] Right.

Stewart Baker: [00:35:51] And you couldn't tell why that was unless you had aggregated the data of 300 of your associates.

Michael Chertoff: [00:36:01] Right. So I think that what I'm really arguing now is we have to move away from thinking we can conceal our data or keep it hidden and recognize it's going to be out there. But now the question is do you have a right to control it? And that happens to be something Europeans have moved towards, and although I'm not always a reflexive fan of what they do, I have to say in this case, putting aside the details, they have a point. And I'll give you an example from our own history when photography was invented. You know the famous story about a young woman whose picture was taken by her boyfriend, who sold it to a flour company that pasted on the side of the bags of flour. And she sued, and her argument was you shouldn't be able to use my image even though it wasn't taken unlawfully and it's not pornographic. And initially the courts said, "No, you have no right to sue because you haven't been defamed." Eventually they said, "You know, there actually is an interest here worth protecting. You shouldn't be commercially exploited or have your image commercially exploited without permission." That's an early example of control over data that the courts came to, and I think we're going to head there more and more.

Stewart Baker: [00:37:11] So I know the same story, and I've drawn a completely different lesson from that. That was at the heart of Louis Brandeis's complaint in the iconic much cited and little read article about the right to privacy in which he says, "It's just shocking that people can take my picture without my permission. You know if I wanted my portrait, I'd pay somebody to paint it." And the idea that somebody could take your picture without your permission was so disturbing to him, he came up with this

whole idea of the right to privacy. And in the end, none of us has protection against having people take our picture. This has turned from a privacy right into a commercial exploitation.

Michael Chertoff: [00:37:58] But actually we do. So here's an example. There is now case law, like in a case like *Carpenter*, that puts a limit on the ability of the government to get access to your locational data, which tracks you every moment, without getting a warrant – a warrant being kind of the baseline for where permission is. And you also have the *Jones* case which involves surveillance admittedly using an attached device, but if you read the opinions, you see issue is broader than that. Where we're headed – and I think this is interesting and correct – is for the court to say, "You know, it is true that when you're in public you don't have a right not to be seen, but at some point if the technology gives the government the ability to ubiquitously observe you 24/7 indefinitely, we're going to require some kind of permission for that." And that's an example of the court now basically saying there is not a limitless right to observe you.

Stewart Baker: [00:38:53] Fair enough, although the idea that individuals can't take my picture is preposterous. You know I'd love to be able to enforce it, but I can't. And no one thinks the government is prohibited from taking your picture because they've been doing that for many years, especially when they're dealing with organized crime. So my sense on this is that what happened is Brandeis was shocked enough and prestigious enough to get the courts to start recognizing a right to protect your picture, but that while that was happening people were getting used to their picture being taken. And by the time the two things came together, no one could justify having a real right to privacy. And it turned into this right of commercial exploitation.

Michael Chertoff: [00:39:42] And that may be the case with respect to the data we generate now, which is you're not going to basically make it impossible to generate the data because people do like the convenience, but you will give them some say into what's done with it. Can it be sold? Can it be used for a purpose other than intrinsic to the particular purpose you've given your data up?

Stewart Baker: [00:40:05] And surely that's right. As people discover bad ways in which their data can be used, they will object to it. Revenge porn laws, for example. And that is, from an American perspective, a more appropriate way to regulate than to say you have rights-of-man right to control your data, whatever that means. Because that leads to you know the French parking situation where you're always in violation of law. The question is whether you're going to be punished.

Michael Chertoff: [00:40:36] And obviously we're not going to I mean adopt certain European implementation of this kind of thing. But I do think here's an example of where I think we could be headed, which I talk about in the book, and you see it now. There's auto insurance companies that will give you a "discount" if you put a device on your car that records how you drive. And that doesn't mean if you break the law. It means if you're driving in an erratic way. Are you accelerating quickly, stopping quickly, et cetera? Now one man's discount is another man's penalty.

Stewart Baker: [00:41:06] Right.

Michael Chertoff: [00:41:06] So essentially what they're saying is, "If you let us monitor everything you do in the car, we'll give you a discount or we'll penalize you." What happens when your health insurer does that and says, "Well, you know I really want to see your Fitbit data. I'm going to look at what you buy, what you eat, do you go to a restaurant before you drive. And I'm going to adjust your premiums up and down depending on whether you are living a healthy lifestyle"? Now the Chinese are already onto this with their social credit score, which they're trying to develop, which basically says, "If you're a good citizen, as determined by our ubiquitous monitoring of what you do, what you eat, where you go, and who your friends are, then you'll get better schooling, better jobs."

Stewart Baker: [00:41:47] You'll get first-class train tickets, which you can't get if your social credit is too low.

Michael Chertoff: [00:41:53] Right. And you could easily see that migrating into a democratic country or a country like the US not because the government necessarily is going to do it but because the private sector will do it. That would easily turn into a situation which – what I call Big Nanny, instead of Big Brother – someone's always telling you essentially you can't do this, you have to do this.

Stewart Baker: [00:42:16] And I assume that one of the things that you think to be part of regulation of this is to understand what people are doing with the data because one of the things that makes the social credit score in China effective and what makes some of the social media censorship regimes effective is you don't know exactly where the line is, you don't know when they're hurting you and when they aren't, and so you just get cautious about what you do, even if it is not formally prohibited.

Michael Chertoff: [00:42:48] Exactly. Basically you self-police. And the idea is that it inhibits you and you're taught over time in much the same way as you might teach a dog to stay away from certain things because they may generate a problem. And in a way that's a much more powerful way of conditioning behavior and coercing it than having a lot of laws that are only intermittently enforced.

Stewart Baker: [00:43:12] What about you talk about the idea that maybe there should be more restrictions, more consent, maybe prohibitions on sharing this data with third parties, that it's collected for one purpose and they may tell you, "We share it with our partners to improve your experience," but you don't know exactly what's being done with that data. I see the reason why people might want to do that. But one of the countervailing considerations has been, well, if you don't allow sharing with third parties, you're essentially locking in the biggest collectors of data today who can use it for any purpose and start a new business based on the data. But other people who might want to start a business based on that data are prohibited from getting it.

Michael Chertoff: [00:44:01] Well actually, I think you know it's not to me what's more important than whether it's shared with a third party or whether you use it for a third purpose other than the original purpose is, is it being repurposed? I mean that's the

critical issue. I kind of divide the data situation into three categories. There are uses of the data that are obviously intrinsic to what it is you signed up to do. If you use Google Maps, giving your location is necessary in order to have it work. Then there is usage of data that are not intrinsic. When whether they do it themselves or they sell it to a third party, if it's used to market by sending you ads as you walk by a store, that's to me a distinct purpose you should have to agree to. The third issue is what do you do when people make use of your data that you didn't turn over? So you know someone takes photos of you. They mention you in Facebook. They do all kinds of things without your consent or knowledge, and it's all aggregated. The cloud provider can collect it all. And now it's used to target you for certain things, and you never agreed to anything at all. And in my view that is the area where you deserve the most right to control the use of data.

Stewart Baker: [00:45:15] That's interesting. But the most obvious example is when other people say something about you. Right? They tag you in a photo. They characterize your politics. Whatever. That is data about you, but it wasn't anything you provided. It was something provided by your friend. In many cases, the friend got a benefit. I remember that's how Cambridge Analytica worked.

Michael Chertoff: [00:45:43] Right.

Stewart Baker: [00:45:44] You provided this data, and you gave the names of all your friends. And that was the crucial data that they utilized. What about the argument that says, "Well, this is the right of the other party to say what he thinks and to provide information that he knows. You've already lost control of that data."

Michael Chertoff: [00:46:08] But here's where *Carpenter* comes back. One of the kind of observations I make in the book is that the scale of what's done now is your data changes the substance in the sense that, yes in the old days if someone wants to say something about you, they can do that, but implicit in that is the idea that it's not all being collected in one place. So it's basically fragmented. That's what I call information friction. And the assumption that you can say what's public, you know you have no right

to, is built upon what was for centuries this information friction. Now imagine all these millions of users of social media platforms, each individually have something to say about you or are photographing you, but now it's all collected and you have essentially almost a 24/7 view of you because in the aggregate the collector's able to draw that inference. That to me is the lesson of *Carpenter*, where *Carpenter* says at some point the scale actually changes the substance.

Stewart Baker: [00:47:08] So let's just quickly ask about *Carpenter*. I should point out: not only were you Secretary of Homeland Security, but you were a Third Circuit appellate judge and you were head of the Criminal Division at the Justice Department. How do you think the head of the Criminal Division is going to adjust and how much are they going to like the new sorts of rules that you are laying out for government?

Michael Chertoff: [00:47:37] You know actually when I was in Europe I had some people kind of raised this you know in a kind of semi-critical way. I'm actually advocating less of a change in the way we deal with government than I am with the private sector because the government already operates under fairly stringent and familiar rules, and it's just a question of adapting those rules again to scale when that changes substance. And, in fact, as we said a bit earlier, to me I'm actually willing to be fairly relaxed on collection because I think the value of collected data is not usually evident until after the fact. And so I counterbalance that by imposing stronger restrictions on when you get to search it, similar to what we do in the physical world. You know stop-and-frisk is a lower level of judicial requirement than an actual search or an arrest or a conviction. So you know I do think that the proposals I'm making actually would be pretty familiar and comfortable to government security agencies.

Stewart Baker: [00:48:42] So one place where they might not be: there's litigation in the Second Circuit now over whether a warrant is required when you gather information under the 702 program that we're all familiar with. It's based on suspicion that a foreigner is a terrorist. But you're collecting communications that may come from the United States. You collect them. You collected them lawfully. The question then is can the FBI just run searches through that database just like any other looking for

Americans they're trying to vet? And it's the Left that has brought this lawsuit says, "No, you need a warrant to do that." I take it you would feel comfortable with the idea that there ought to be some limitations, some showing that the FBI has to go through before it does a search for the name of an American in that database?

Michael Chertoff: [00:49:33] I mean you know again if the database is communication with a known terrorist, I probably have a fairly low threshold for that simply because determining whether there's a contact is kind of metadata. It's a minimal issue. Then depending on whether if you've recorded content – and you know we deal with this all the time, even in the criminal law with minimization – you can generally, if you have a warrant for the actual original interception, look at the material, but then you minimize if it turns out to be irrelevant. So these are tweaks that we're pretty comfortable with.

Stewart Baker: [00:50:09] So let me switch gears a little. At DHS you really turned DHS into a player in cybersecurity in a way that it was not, except theoretically, before that. And the Obama Administration has built on that. Kirstjen Nielsen has built on that. And it's been a while since I've heard somebody just mock the department for its role in cybersecurity. But you talk a lot about cybersecurity. One thing I didn't see – and maybe I missed it – is I didn't see you commenting on the role that essentially the Justice Department plays now in indicting foreign government actors who have engaged in the hacking. What's your sense about the effectiveness of that tactic?

Michael Chertoff: [00:51:05] I recognize we're unlikely to get the indicted people in a courtroom, although occasionally we have cases – I know of a couple – where someone took a trip and they didn't realize they were going to wind up in a courtroom. I think there are two values to it. One is the issuance of a detailed indictment that actually explains what happens often allows us to have a conversation about what's going on that we can't when all we get from the Intelligence Community are vague allusions to things in very general terms.

Stewart Baker: [00:51:34] Right. "Medium confidence."

Michael Chertoff: [00:51:34] Correct. Secondly in some areas it actually has more value. I mean I think in the area of, for example, theft of intellectual property. When PLA members were indicted it kind of sent a signal to companies that might be using the product of their hacking, you know you guys could be next. And that would be an issue because you could wind up, if a company wants to do business in the US or the West, they could be exposed. So do I think it's not a compelling deterrent? It has some value, as does the issue of sanctions have some value, although you can overuse those. But it's part of a menu of tools.

Stewart Baker: [00:52:18] One of the other tools that I was surprised to find – we may agree on more than I usually do with people who've been at the Criminal Division – is active defense. You clearly don't believe in hacking back and just kind of randomly attacking whoever attacks you. But at the end of the day, your position on what companies ought to be able to do or what the private sector ought to be able to do is more nuanced than the Computer Fraud & Abuse Act as it stands today.

Michael Chertoff: [00:52:52] Well, you know I think you have to look at a spectrum of responses. There's everything from honeypots where you lure somebody in, it's all on your own network. And generally things done in your own network in a general sense strike me as within the authority of what you should be able to do. At the other extreme, I don't believe the private sector, unless it's acting at the direction or control of a government agency, ought to be able to move into someone else's network and actually do damage and disrupt: (A) because, putting aside legal restrictions, it's possible to have collateral damage; (B) because you may find that the private party escalates a situation. You know probably the hardest case to deal with is where you kind of dangle something out there that someone steals and when they steal it winds up becoming a poison pill in their own network, and that you could probably debate.

Stewart Baker: [00:53:48] I'm not even sure I would say that's a good idea because you never know what network it's going to end up in.

Michael Chertoff: [00:53:53] Exactly.

Stewart Baker: [00:53:53] On the other hand, you talk about the idea of letting people leave their network to investigate crimes, to see where their stuff has gone, as long as they do it under government supervision with clear [direction] and without causing any harm. And that strikes me as an appropriate place to draw the line but not a place that people have been able to get the government to draw.

Michael Chertoff: [00:54:19] Correct. That's an authorities issue, and I think as long as you're using government authority and direction, I'm okay with that. Now you get into an issue of capability, and it may be that the government is not at this point confident in the capability. Well, I can tell you from work I do with the private sector.

Stewart Baker: [00:54:37] They're pretty good.

Michael Chertoff: [00:54:38] There's a lot of contractors sitting in government offices. So at some level...

Stewart Baker: [00:54:42] And a lot of the private sector contractors who used to be sitting in government offices.

Michael Chertoff: [00:54:46] Right. So there's a little bit of maybe a not-invented-here attitude. And if you want to scale – again, to use that term – your ability to respond, you might want to deputize.

Stewart Baker: [00:54:57] Yeah.

Michael Chertoff: [00:54:57] Actually someone asked me this question: the distinction between deputizing and delegating. Delegating means: here's the authority; you do what you want with it. I'm not in favor of that. Deputizing: you can do this, but it's under my supervision. And so I'm arguing deputize. Don't delegate.

Stewart Baker: [00:55:14] I have long thought that some state attorney general is going to wake up one morning and realize he can deputize people under the Computer Fraud & Abuse Act and essentially immunize them. And he could announce a policy of deputizing cybersecurity companies that are located in his state and produce a pell-mell rush to locate in his state that we could see that happen. What about no-action letters from the Computer Crime and Intellectual Property Section? Seems to me that's a sort of very small step in the direction of saying, "Okay, we know we've written a very broad law. And we're going to tell you there are certain things you can do and certain things you can't do." And maybe they'll do that with respect to beacons, for example. But my sense is that prosecutors just hate no-action letters.

Michael Chertoff: [00:56:12] Yeah, and I think I'd be reluctant to rely on that because you know how much protection it ultimately gives you is a little bit unclear. I think the government, if they're going to authorize something, ought to come out and authorize it.

Stewart Baker: [00:56:25] So we're coming to the end. I do want to ask you – we talked a lot about privacy, and you've been more comfortable with some of the European approaches than I have been. At the same time, you're clearly committed to better cybersecurity. I'm discovering a lot of conflict between the kinds of things you have to do for cybersecurity, which is intensely monitor your network, everything that goes in and goes out, and the idea of these very broad protections for personal data, including personal data that might be wandering around on your network. How do you see that tension and what resolution do you think we're going to get?

Michael Chertoff: [00:57:04] So I think when you're dealing with data on a particular network – and even if it's personal data – you should have the ability to police that network in order to maintain security. The reason I say it is this: privacy is an empty promise without security. If I say, "Oh, I'm going to protect your data. I'm not going to use it for any purpose other than what you've authorized," and I can't do it because I can't even control my network, that promise is worthless. I think you actually enhance privacy when you take the steps in your network to make sure that there's no one

intruding or corrupting it. And I don't view that as inconsistent with maintaining the privacy of the personal data. I view it as actually enabling that privacy.

Stewart Baker: [00:57:51] Fair enough. Let me just, before we finish up, I should ask: you're doing a book tour and for listeners, the name of the book again is *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*. Do you have any speeches or public appearances coming up that our listeners ought to know about?

Michael Chertoff: [00:58:10] You know I've just done San Francisco and London. I think I'll be doing something up in Boston on November 4th. I'm going to be doing a book event. And I expect I'll be talking about this at various places. I'm sure I'll talk about it at RSA next year out in California in February. So stay tuned.

Stewart Baker: [00:58:29] Okay. No, it's a great compendium of all the issues. Very thoughtful prescriptions for how to address them. It is a single book that will bring you up to speed on the entire debate about privacy, cybersecurity, and where we're going online. So it's been it's been a pleasure to have you.

Michael Chertoff: [00:58:49] Great to be on.

Stewart Baker: [00:58:49] Great to see you. And thanks Paul Rosenzweig, Matthew Heiman, Gus Hurwitz for joining me, along with Michael Chertoff to discuss this book. This has been Episode 231 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. If you want to get a coveted Cyberlaw Podcast mug, just suggest another interviewee as good as Michael Chertoff, and we'll send you the mug. If you want to comment on these stories, you can do that on Twitter or LinkedIn where I'm @stewartbaker. Please do leave us a rating. That's how people find us. So if you go to iTunes or GooglePlay or Stitcher, we'd love to get your reviews. We've got some great interviews coming up: Peter Singer from the New America Foundation, author of a new book called *LikeWar*; Suzanne Schwartz is going to explain to us how the FDA approaches the Internet of Things and cybersecurity, and that'll be a heart stopper – literally; the general counsel of GCHQ is going to be on in October; and Chris Krebs,

who's the Undersecretary for Cybersecurity at DHS, will be talking to us about election security about a week and a half before the election. So this should be lots of fun. I want to thank: Laurie Paul and Christie Jorge, who are our producers; Doug Pickett, our audio engineer; Michael Beaver, the intern who has made all of this possible; and I'm Stewart Baker, your host. So join us again next time as we once again provide insights into the latest events in technology, security, privacy, and government.