Episode 247: “If I save Earth, you’re gonna owe me.”

Stewart Baker: [00:00:07] So you actually were trying to solve the problem of what to do with ships, and you said, "Why don't I look for a problem that doesn't have the privacy constraint on it and see whether I can solve that problem?"

Jeff Jonas: [00:00:20] Now and then, asteroids hit each other, but we only see them after the fact. The first time this ever happened is in 2010. Hubble was taking a deep space picture, and in the middle of the picture was a giant "X" because it was two asteroids that pounded into each other.

Stewart Baker: [00:00:30] Wow! And then bounced out?

Jeff Jonas: [00:00:31] Yeah. And so then they're going who knows where? They're not going where you thought they were going. Now where are they going? So I asked the question, I go, "Well, why don't you just check to see if they're going to hit each other?" And then they just said to me, "I don't think you understand. This is something called multi-body orbit math, which means you use a lot of compute. It's an n-squared problem. You'd need 10 million computer hours." And then I went, "Well, but why would you even try to solve it that way? Why wouldn't you just solve it this other way?" So I told them about this other way, and they went, "That could work." And I could see it in my head. I went, "Of course it would work." And we delivered to them a 25-year forward forecast of every asteroid getting close to every asteroid. And now for the first time, astronomers are able to look in space and watch two asteroids glaze each other. Yeah, if I save Earth, you're gonna owe me.

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

Stewart Baker: [00:01:19] [Music] Welcome to Episode 247 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government. Today I'm joined by our guest, Jeff Jonas, who's the founder and CEO of Senzing. This is basically "sensing" with a "z," right, Jeff?

Jeff Jonas: [00:01:41] Indeed.

Stewart Baker: [00:01:42] Okay. Jeff is a longtime friend. We go back 15 years, and he's been doing remarkable things with data that whole time, so this will be a fun interview. I'm glad he's here. For our News Roundup: David Kris, co-founder of Culper Partners, former Assistant Attorney General in charge of the National Security Division at Justice; Gus Hurwitz, Professor of Law at the University of Nebraska; Jamil Jaffer, in studio at last, founder of the National Security Institute, Adjunct Professor at George Mason, and a hundred other things. Jamil, I don't know when you sleep.

Jamil Jaffer: [00:02:22] Well not much, but darn glad to be here. Thanks, Stewart.

Stewart Baker: [00:02:24] It's a pleasure. And I'm Stewart Baker, formerly with NSA and DHS, host of today's program and operating on four hours sleep. Thank you, Burlington Airport. You would think they would be better at dealing with below-zero cold than they are. Let's start, David, Jamil, with something that falls right in your area of expertise, which is – God help us, we're going to have another FISA [Foreign Intelligence Surveillance Act] debate all through 2019 because three sunsets at the end of 2019. Bobby Chesney had a nice write up about what was going away, but this debate's going to be a little different, I think, than the last one. What do you see? I'll ask David to kick it off. David, what do you think the main issues are going to be this year?

David Kris: [00:03:20] I think the main issue by a long shot is going to be the ongoing call detail record collection authority that was grafted into the FISA business records provision by the USA Patriot Act of 2015. Just to start with a wider aperture on it, there are three provisions that are going to sunset at the end of this year. One is the business records provision. Two is the authority for roving wiretaps in traditional FISA electronic surveillance where you can follow a target across multiple phones and even multiple providers. And three is the so-called "lone wolf" amendment that allows the targeting under traditional FISA of individual non-US persons who are engaged in terrorism, even if they're not affiliated with a larger terrorism group. Again, of those three, I think it's really the first one concerning business records that is going to raise the fuss. You know that thanks to Edward Snowden, there was a lot of bulk collection of telephony and Internet metadata being done by the government, first under unilateral executive authority and then under the auspices of the FISA Court. When that was revealed, you know there was a big fuss, and the result was the USA Freedom Act of 2015, which prohibited bulk collection under FISA and some other provisions but created in its place this very complicated system for the ongoing collection of telephony metadata or call detail records two hops out from a seed identifier. So under the old system, the government would suck up all the telephone records, and then it would do contact chaining across those records using its own algorithms in this huge pool of data. Under the new system and the Freedom Act, there was this more complex iterative functioning where it would send out a seed number, and then the phone company would respond, and then there'd be a second level of querying and response, and so forth. The big innovation was that NSA wasn't holding all the data, but the price of that was a very complicated system. And it failed catastrophically last summer, causing NSA to just give up and delete all the data that it had received since the Freedom Act under that new program.

Stewart Baker: [00:05:43] So sensing weakness or maybe a collection program that wasn't valued by the apparent beneficiaries, a lot of people are saying, "Well, why don't we just get rid of it?"

David Kris: [00:05:58] Yeah. And I think that's a real question: whether the executive branch in this environment in particular is going to conclude that it's worth the fight to seek renewal or whether they will just throw up their hands and say, "The juice is not worth the squeeze here. Let's let it go." It's a lesson in how sometimes you know the incredible legal and operational complexity of these programs can become a factor, and the perfect could be the enemy of good.

Stewart Baker: [00:06:31] Jamil?

Jamil Jaffer: [00:06:31] Yeah, and I think David is exactly right that the thing that's going to be most focused on here is the call data records collection. I think the interesting environment that we walk ourselves into is the sort of Donald Trump, "the FBI was surveilling or the NSA was surveilling my campaign." I'm concerned about that. You saw during the [Section] 702 fight, the administration sort of altogether saying, "We want 702 renewed," and then the president at the last minute tweeting, based I think on a Fox News report, that maybe it ought not be renewed. That conversation is likely to take place in the context of a different collection, call data records collection, that wasn't really implicated by the questions around the campaign and the like but is a FISA issue and might get caught up in that. And it wouldn't be surprising if, unlike the prior two administrations, the administration doesn't fight particularly hard to renew. That would be troubling, given all of what the Bush Administration said about this being important early warning program and what the Obama Administration did to keep this program alive, albeit maybe hamstrung by the USA Freedom Act and the pressure on in Congress from both Democrats, who never liked the program, and Republicans, who are increasingly becoming libertarian on these questions à la Ted Cruz and Mike Lee, and then increasing movement in the House too and that shift of the Republican Party. And so for people who think this is an important program, which I would put myself in the camp of, even post-sort-of-hamstringing of it by Congress in the USA Freedom Act, there's a real chance this program goes out the door, and then we'll all be left wondering well what happened. Why did we reduce authorities at a time when the terrorist threat remains high? Not just saying, "We beat ISIS."

Stewart Baker: [00:08:05] Yeah. So I agree with – I don't think that the administration is going to give up on this, though I wouldn't be surprised if at the last minute there were a tweet that came from nowhere that appeared to give up on it. That is a real risk, just as it happened last time. I am hearing from a lot of people on the Hill that they're getting pushback on FISA from completely unexpected directions, people who say, "Oh, yeah, I remember that. That's the thing that Obama used to spy on Trump."

Jamil Jaffer: [00:08:38] That thing. Exactly. And you'll have a lot of folks in the House, some the newly elected folks currently there and some of the folks who were left over the last four or five, eight, six years. And then you've got an increasing movement in the Senate in that direction, too. And so with the president out there sort of hearing it on Fox News, the president himself putting it out there, Devin Nunes as the Ranking Member of the House Intelligence Committee, there may be a perfect storm of a challenge for this program. And as strong as NSA might feel about it, given the operational challenges they've faced, it's going to be an uphill road, and the real problem is there are very few voices out there saying, "Hey, hey, hey. This is a really important program for national security. Warning: danger, Will Robinson."

Stewart Baker: [00:09:14] So my hope for salvaging this is something that happened in the [Section] 215 debate. At the end of the day, there was a lot of grumbling about it, and the issue *de jure* was unmasking. And to get the votes of people, for the "Trumpista" Right, they came up with a set of rules that restricted unmasking and imposed some civil liberties constraints. Now, pretty much the constraints that already have been imposed administratively. But still, I think it was a way of respecting a narrative that obviously was important to the "Trumpist" Right. I think you could do that again, if you fought carefully about it. There are plenty of ways to ask – if we were worried not about oppression of some minority viewpoint but of raw partisan misuse of FISA – and that is the narrative we're dealing with now, that the Obama Administration during the campaign and after was taking a national security concern and using it for partisan advantage – if you ask the question, "Well, that's a new problem. That's not a problem that we addressed in the '70s. We couldn't imagine it. Now we can. What kinds of changes should we make in FISA that will make that harder to pull off?" Eh, I think you could come up with something, but it's incumbent, especially for those of us on the Right, to start thinking about that.

Jamil Jaffer: [00:10:51] Agree 100%.

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

Stewart Baker: [00:10:52] Let's move on to a decision that is making news, although God knows why. Well, I know why, but it's not the quality of the decision. A decision, allegedly by a judge out of the Northern California District, saying that passcode and biometric phone access should be treated the same way for Fourth and Fifth Amendment purposes and refusing to grant a warrant that would have allowed the automatic collection of biometrics to open phones. Jamil, can you give us a little bit more about the decision?

Jamil Jaffer: [00:11:33] Yeah. Well, I mean the decision is interesting because it has all sorts of aspects to it, starting right at the jump, that might be wrong if any sort of regular district judge would look at it or if it were ultimately to make the court of appeals, the district judge ultimately adopted the magistrate judge's recommendation. On a warrant – obviously this denied it, but they can always go to the district judge for the warrant. The challenge here is (1) what does the Fifth Amendment have to do with any of this when you're looking at a warrant?

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

Jamil Jaffer: [00:12:01] Why are we looking at the Fifth Amendment as right to self-incrimination or right against self-incrimination? And the judge says, "Well, look, I mean it might be manifestly unfair of me if I were to grant the warrant and then later the introductory evidence were challenged because it's so hard to win when you challenge the introduction of evidence or you file a suppression motion." Well, of course, that is how, in fact, we do Fourth Amendment law. We don't sort of deal with all that upfront. Is there probable cause? Does it have particularity? All the other requirements of the Fourth Amendment? And then we move on.

Stewart Baker: [00:12:36] Well, and suppression motions are hard to win because you're suppressing actual valuable evidence about the person. What the judge here did was suppress even the collection of that evidence. You don't even know what she suppressed.

Jamil Jaffer: [00:12:49] Exactly. And then she also looks at this question of whether it was probable cause and conflates probable cause with particularity. Right? Do you have a well-enough described application as to who's being searched and what's being searched? Well, if you're not describing that in a particular manner, well, there's no probable cause. Those are typically thought of in most courts as segregable inquiries. She conflates the two. And then there's a range of other problems, ultimately culminating in this question of whether facial recognition or thumbprints are the same as passcodes and passwords. There is a debate, I think, in academia – maybe it's just a debate with me – whether the question whether you can actually get somebody to give their password up is appropriate or not, whether that is a Fifth Amendment problem. Is forcing somebody to give their password up forcing them to testify against themselves? I think the answer to that is no. I recognize that a lot of folks disagree with me, including most judges. But –

Stewart Baker: [00:13:39] Yeah, I'm with you. It is not testimonial, and you could certainly solve it by saying, "Fine. We will not tell the jury –"

Jamil Jaffer: [00:13:48] What your password is, or you gave it to us. Right. But then, even if you assume that those judges are right and you and I are wrong, the question of, well, is a thumbprint the same as a facial recognition on your phone the same as a password? Is it something in your mind? No, it's actually something you *are*. As we know, two-factor authentication is about something you *know* and something you *are*. We typically think of those things are separate. Why we conflate the two for Fifth Amendment or Fourth Amendment purposes, it's not clear you should.

Stewart Baker: [00:14:16] And this opinion does not explain it. Gus, can you salvage this opinion?

Gus Hurwitz: [00:14:23] No. So there's nothing good here. I want to actually start with probably an imprudent rant about this opinion. And as far as the media is concerned, this magistrate judge's opinion / order is the same as a Supreme Court opinion. It's reported in the same airy sort of way without any distinction between the two, which is really frustrating. And I've been thinking a lot about this over especially the last weekend or so. The thing I shouldn't touch on, the Covington Catholic situation and thinking about deep fakes and the role of the media in spreading this sort of information that's hard to sort through for the public. The media has to do a better job with this stuff and its reporting of this stuff. So this magistrate judge's order is a break from the general trend in these cases. I'll say there is some defendability, perhaps on the Fourth Amendment side. I haven't gotten into the details of what was being requested on the part of law enforcement here enough, but the order reads as though law enforcement was requesting permission to collect every device from every person who was at the same event as the actual suspects subject to the order and then require every person there to unlock every device. So that might be overbroad, but as Jamil said, we've got severability. We should have looked at this in finer grain detail. The Fifth Amendment issue is just an absolute mess. And the most interesting thing, I think, about how this mess starts up: first, the general recent trend, I would say, at the circuit courts has been to allow these sort of challenges to survive Fifth Amendment scrutiny and, in fact, as Jamil says, to allow disclosure of passwords as not violating the Fifth Amendment testimonial privilege. But how does this magistrate judge reach the conclusion that she does? Well, *Carpenter*. She says the Supreme Court in *Carpenter* says – she doesn't say for the purposes of Fourth Amendment inquiry – she just says generally, courts should make rules that embrace the – and update the law to address – the technological complexities of the day. That's just reading *Carpenter* as license for judges to make whatever willy-nilly law they want. It's really messy. It's a very dangerous reading of *Carpenter* and demonstrates some of the problems that we likely are going to see in coming years as courts struggle with and try to figure out what *Carpenter* means.

Stewart Baker: [00:17:18] So one of the things that occurs to me – maybe this is the fact that I've been around too long – I remember when magistrate judges were magistrates, and everybody knew that they were totally subordinate to the district court and did what the district court didn't have time to do, and you shouldn't treat their decisions too seriously because any of them could be reviewed and overturned by any district judge who said, "You're not really saving me work. You're creating it." And then Congress in 1991 – I'm sure in response to lots of lobbying from the magistrates – said, "Why don't we call them magistrate judges? Then we won't have to pay them anymore, but they'll feel better about themselves." But this is so stupid, and the coverage of it is so naive that it really raises the question whether we should just take that back and send them back to being magistrates, which they were for, what, 200 years.

Gus Hurwitz: [00:18:20] Yeah. I think that's a very wise idea as an outcome of this case. The magistrate judge shows no recognition of the scope of this opinion. The biometrics being collected here are indistinguishable from other sorts of routine biometric collection (fingerprints and DNA, for instance). And this is the sort of opinion and the sort of reasoning that *Carpenter* cannot mean the court should be engaging in and the conclusions they should be reaching.

Stewart Baker: [00:18:59] Alright. Well, I want to try to move quickly through the stories that remain. The insecurity of EDGAR [Electronic Data Gathering, Analysis, and Retrieval system] is producing a whole host of new forms of front-running insider trading. The people who did the front running and who got early access to people's filings are all gonna go to jail, it looks like, because the SEC is pretty good at catching them when they trade, even if it can't catch them in its system. But really, if EDGAR were run by a private entity, how many fines would it have attracted as a result of its inability to keep this stuff secure? Gus?

Gus Hurwitz: [00:19:46] It depends on who's doing the fining. Clearly the FTC would try and come down hard on the SEC in this case. The silver lining, I think, in this case is in the last couple of years, the SEC has, I think, become better in how it thinks about cybersecurity. It's less focused on "Did something bad happen? We're going to find you." They increasingly recognized that they should be focusing on "Are you guys trying to do security? Do you have a compliance program? Do you have a training program in place? If you do, okay, that's good." And the FTC hasn't quite caught up to there. Hopefully that's the direction that they're going, but, yeah, this demonstrates a whole lot of the government's own cybersecurity failings. It demonstrates, as you say, Stewart, the SEC is good at finding the bad actors here and going after them after the fact. And instead of punishing the firms in the private sector context who are trying to do security well and just can't accomplish that Sisyphean task, we shouldn't punish those firms. We should help them out with going after the bad actors where we can. The other really remarkable thing about this case: these guys had access to advanced filings of a relatively small number of companies actually, and they were able to make about $4 million off of it. That number is just mind-bogglingly small to me.

Stewart Baker: [00:21:22] Yeah. I thought that too. On the other hand, they often had access only 10 minutes before the data went live, so there's only so much trading you can do without realizing that you're giving away your insider information. So maybe that's why they could only make four million bucks out of it. So let's keep moving on. I will say that when I pointed out that the SEC probably would have been fined had it not been the SEC's mistakes here or at least their system, Saad Gul, who is a faithful listener, says in a response to my tweet, "Well, Stewart, it's good to be king." Jamil?

Jamil Jaffer: [00:22:09] No, I mean it's exactly right. I mean it was $4 million over six months, to be clear. And what's interesting about this is you've got hackers in Russia, hackers in Ukraine, and hackers in LA. I mean I don't know what's going on here, but the LA connection's interesting, my hometown. And the other thing I think that's interesting is these were test filings, so why they had sensitive data, why these companies were putting in their sort of pre-filing, test filing, they're actually using the real data. I mean that's the moronic play here. So I mean if you're going to be fining anybody, these companies are not the sharpest knives in the drawer either.

Stewart Baker: [00:22:40] Yes, although I have to say, if you want to know that the thing you want to put up can be put up, that's what you want to test. If you tested with some dummy data, that dummy data would end up being released one time out of 100.

Jamil Jaffer: [00:22:55] Or it might work, and then your actual filing doesn't work, and then you're up a creek.

Stewart Baker: [00:22:58] Exactly.

Jamil Jaffer: [00:23:00] That's a fair point.

Stewart Baker: [00:23:00] So very quickly, David, DOJ's OLC [Office of Legal Counsel] flipped on a pretty recent decision about gambling, whether the Wire Fraud Act or the act making it criminal to engage in gambling, applied only to sports gambling or to all online gambling. That decision limiting it to online sports gambling is only a 2011 decision. And now with the new administration, they've rescinded the decision. How unusual is that? Is this a big deal?

David Kris: [00:23:46] It's pretty unusual. OLC does not often reverse itself so quickly, but it's certainly not unprecedented for OLC to do so. And the technical side of this is exquisitely painful to review. But there are basically two clauses in this law, the first of which applies to wire communications in support of bets or wagers on any sporting event or contest and the second clause of which just refers to bets and wagers without reference to sporting events or contests. And, as you say, in 2010 or '11, OLC read both clauses as being limited to sporting events and contests. Now OLC has changed its mind. The reason that the change of mind really gets any media attention at all is because it is to the benefit of casino gamblers, who are interested in restricting online gambling through the expansion of this criminal law, one of whom is Sheldon Adelson, who has given, I guess, a whole bunch of money to the Republican Party. And so the news angle on this has all been about whether DOJ or OLC or the Criminal Division are sort of in the tank and doing the bidding of these big Republican donors.

Stewart Baker: [00:25:03] This is the phenomenon known as the Bootlegger-Baptist Coalition, where the bootleggers and the Baptists want to ban sales of alcohol and nobody else does, but they make common cause in order to keep their illegal franchise going if they're the bootleggers or in the hopes of improving the morals of the populace if they're Baptists.

David Kris: [00:25:30] Kind of a big tent theory. But I don't – sort of riffing off what Gus said earlier about the media – I mean I think the reporting on this has been somewhat more careful than some other reporting about jumping to conclusions. One can note the correspondence between the interests of large donors and the unusual event of an OLC opinion changing course, but I'm not aware of any direct evidence of any real connection there. And having gone through the 22-ish-page – 23-page – OLC opinion, I would just say that before one would make such an allegation in a serious fashion, there would be an obligation to wade through the statutory analysis. I think that would probably cut down on anybody expressing a view if that standard is applied.

Stewart Baker: [00:26:21] I believe there are currently at least 10 interns at BuzzFeed looking for Vladimir Putin's interests in online gambling opportunities. Okay. Why don't we move on – this was terrific – to our interview with Jeff Jonas, founder and CEO of Senzing and acclaimed Wizard of Big Data. He really was a data scientist before data science was cool. Jeff, why don't you talk briefly about how we got to know each other, what you had been doing before that, and then where we first bumped into each other because I think it'll give people a feel for both your data science credentials and your interest in public policy?

Jeff Jonas: [00:27:12] Well, first, it's really great to see you. It's been a little while. I think the last time we saw each other, I was wearing a corset.

Stewart Baker: [00:27:18] Yes, that's right. That's right. You were in pain.

Jeff Jonas: [00:27:23] Can you un-see that? I believe that we first met at the Markle Foundation on the national security task force.

Stewart Baker: [00:27:31] In the wake of 9/11, and what could we do to find the kinds of people who carried out the 9/11 attacks.

Jeff Jonas: [00:27:40] Yeah. And do it in a way that had a lot of privacy and civil liberty protections. It was my first work in policy, really, and it was a great memory. Those are great, great years. Lots of meetings and lots of reports, and I remember seeing output with a few of my words in presidential orders. So I'm like, "Wow! I've actually done something with my life."

Stewart Baker: [00:28:03] Yeah. You had a big impact on it. You brought to the task your experience in Las Vegas finding card counters. So if you've seen the movie *21*, that was about card counters, and the card counters are usually easy to spot because they make tiny bets until they realize the cards are hot and then they start making very big bets. But if you see that pattern, you throw them out if you're a casino. The way these MIT guys overcame that is they had one person who just kept making small bets no matter what was coming up in the cards. But they would signal another guy, who was acting like a drunk who didn't have any idea what his money was worth wandering from table to table dumping large sums on the table, who would come over and start dumping large sums as soon as the cards got hot. And only if you knew that those two people were in cahoots could you realize that card counting was going on. And in fact, if you watch the movie, they do figure that out. And as a practical matter, they were using your software to do it.

Jeff Jonas: [00:29:15] That's true. We did build that software that's used today probably by half the casinos in the world to help find card counters. But it wasn't just that. It turned out there was some additional data. There's a few things you have to do. If you want to use data to catch bad guys, there's only two ways to do it. And one of those ways is you have to have some data they don't know you have.

Stewart Baker: [00:29:36] Ah. Okay.

Jeff Jonas: [00:29:36] If they know you have cameras on three streets, they'll just take the fourth street.

Stewart Baker: [00:29:40] Right.

Jeff Jonas: [00:29:41] And it was on that principle that I stumbled into while working on this project, I stumbled into – somebody gifted to me – the MIT card count team's business plan. How they're going to raise money. How are they going to train, recruit. How they're gonna make sure they weren't penetrated. How they were going to move money.

Stewart Baker: [00:29:59] So it really was a counter-espionage operation.

Jeff Jonas: [00:30:04] Yes, maybe. I still have a copy of that plan, by the way. And I read this plan slowly, sentence by sentence, thinking if I wrote this plan, I was the prime mover behind it, what would I be thinking. And I got to the point in the plan where it said that they were going to recruit primarily from the MIT engineering department. And so I got the wise idea of why not just get the yearbooks?

Stewart Baker: [00:30:26] Which if anybody was going to digitize their yearbooks in the '90s, it was gonna be MIT.

Jeff Jonas: [00:30:34] Themselves. Well, we had the paper yearbooks and then added, fat-fingered in, the engineering department. Not that they're card counters, but if you have somebody that is acting like a drunk and only playing big bets and they happen to also be in the engineering department, it doesn't even mean they're bad. But if you're trying to narrow your focus, what a great place to start. But by the way, that was not in the movie. The movie was primarily theater. But it was not either in the book, and most of the people in in the MIT card count team don't know that because they think it was the facial recognition that we implemented in '96, which is just a facade.

Stewart Baker: [00:31:10] So obviously if what you're trying to do is to find hidden connections among people who are out to cause you harm, the application of that to terrorists who are vanishingly small as a percentage of the population but who can do overwhelming damage, the ability to spot connections among the 19 terrorists would have been enormously valuable. And so it was obvious that what you had done in Las Vegas had implications for the counterterrorism problem.

Jeff Jonas: [00:31:44] True.

Stewart Baker: [00:31:45] And when you talk about trying to do that, find those connections, without violating privacy, while respecting privacy, what kinds of things did you suggest the government ought to be doing?

Jeff Jonas: [00:32:00] This is one of the tricky things is everybody agrees on both sides, the government and the privacy community, that false positives are bad because you're tapping people on the shoulder unfairly. That's where I think there's the biggest agreement.

Stewart Baker: [00:32:14] Yeah, because from the government's point of view, it's a complete waste of their resources to go out and stop innocent people.

Jeff Jonas: [00:32:20] Yeah. On the other end, it's tough because you can only make sense of the data you have. If you're trying to figure out where to focus your finite resources, say to find a bad guy, you need enough data points so that you cannot have a lot of false positives. It's like you need more puzzle pieces to get a richer picture. If you announce every single puzzle piece you have, clever bad guys – this is one of my two principles –

Stewart Baker: [00:32:45] They do the screen on themselves, and they say, "Okay, you're not going on this operation. We're going to send somebody who doesn't flag under these tests."

Jeff Jonas: [00:32:55] Yeah, exactly. So there's two ways to catch really clever bad people. One is to have data they don't know you have, and that's difficult. How do you do that if you're a government and you need to be transparent in the kind of data you're collecting? And the other one is maybe your adversaries know all the data you have. Maybe because of the Snowden breach, they can really imagine more data about what you have. Maybe they've even exaggerated it in their head, and they imagine you have more data than you really have. Then the only way to catch them is you have to be able to perform compute on the data in a way that they cannot fathom. And an example would be they know you have a video camera in the parking lot, but they never got the memo that there's something called license plate readers. You see?

Stewart Baker: [00:33:36] So they stay in the car, and they never get out of the car. Then nobody can see their face, but that doesn't matter because you're reading their license plate.

Jeff Jonas: [00:33:43] They don't know that that's computable. They know you have a video, but they don't know it's computable that there's a plate. So when you think about catching clever bad people, you have to think about those two vectors. And then how to square that is the tricky part. And that takes thought. Lots to process.

Stewart Baker: [00:34:00] So what Senzing does – what I'm struck by is the continuity in your career because so much of what you've been doing since the Las Vegas days is saying, "We can find connections. We can identify people and say, 'This is this person, and they have all of these attributes,' from piles of fairly random, not very well-organized data." You did that in Las Vegas, did that in the connection with counterterrorism. You're still doing it. You've got a project now on voter registration.

Jeff Jonas: [00:34:42] Very proud of that project. Yeah, but just to be clear, we don't have data. We're not finding the connections. But organizations struggle with this. They've got piles of data, and they don't realize it's the same person. And if you're in healthcare, they think it's two patients, but it's really one patient. That's important to know. I go check into a hotel, and they think I have three loyalty club cards. It's just me. These are all what's called entity resolution problems. Duplicates in your phone. If you look in your phone and see duplicates, that's an entity resolution problem. Marketing lists. When they've got a bunch of duplicates in there, they think I'm three. Some company's marketing to me, and I'm already their customer. That just means they haven't been able to match me. So the purpose of Senzing is to take what's been difficult, which is this entity resolution – and historically the really good stuff is millions of dollars and is really only available to the elite. I'm just democratizing that. I'm letting the whole world have it.

Stewart Baker: [00:35:36] Yeah. You've been releasing this on a kind of freemium basis. That is to say, the code is free for people who want to use it to do entity resolution – I'm going to ask you a question about that in a second – and then obviously if the amount of data gets really large, people will pay for it using the data to use the code to process the data. So let me ask you a question, very personal. I've got all these people in my Outlook database who have moved on to other jobs. I also have a fair amount of it out of LinkedIn, which is usually much more up to date because people want to put their up-to-date contact information in there so that they can be contacted about their next job. Could I just take the code and use it to go through Outlook and whatever I've downloaded from LinkedIn to both entity resolve and get rid of the old data?

Jeff Jonas: [00:36:35] You can download your Outlook. You can export your Outlook to CSV [comma-separated values], just means a comma-delimited file. You can do that with LinkedIn as well. Until about six months ago, LinkedIn would include the email address, which is a really great hint. Now, unless people opt into sharing their email address, it doesn't export. And I just retested mine in LinkedIn, by the way, and no one in my 5,000 friends have gone in there to opt in for "yes, share my email."

Stewart Baker: [00:37:04] Of course not. Well, presumably this is LinkedIn basically trying to start their walled garden effect to say this data is really valuable and we're gonna make it hard by claiming that it's a privacy problem to share the data.

Jeff Jonas: [00:37:19] Maybe. Was it privacy first or hoarding first? Yeah. But you could sell that one either way. But what I do is I download all my Outlook. I download my Salesforce to CSV. Then I go export everybody that asked for my newsletter. And then I have my Halloween party mailing list. I entity resolve that together, and then I can make a single search and find that person across all my channels without having to go to each one. And it's less than 10,000 records, and that's just free for everybody.

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

Stewart Baker: [00:37:56] That's great. So tell me about the – because I think this will give people a feel for how it works – tell me what you're doing in voter registration.

Jeff Jonas: [00:38:03] We're so proud of this project.

Stewart Baker: [00:38:04] I have to say, this strikes me as a landmine-filled path that sooner or later you're going to make Republicans or Democrats angry because you've tripped over one or another of their shibboleths.

Jeff Jonas: [00:38:22] Well, half the country's running on it now, both Blue and Red states. I hate to claim a victory there, but a lot of work was done with this. It was originally primed with Pew Charitable Trust. And so here's the goal of the system is to improve the quality of the election rolls, and one of the first problems you have in the election rolls is people move and they forget to un-register.

Stewart Baker: [00:38:47] Because why bother?

Jeff Jonas: [00:38:47] I don't know. Who's going to remind you? So you live in Colorado. You move to Oregon, and you forgot to un-register. So now the rolls in Colorado are bigger than the population maybe.

Stewart Baker: [00:39:00] Or you die and you forget to un-register.

Jeff Jonas: [00:39:02] Yes. Well, shame on them. We need to go after them – and their families. I kid. So what happens in this system – it's run by a nonprofit called ERIC [Electronic Registration Information Center], and states on-board with them, and they take their voter registration data and the DMV data from each state. And if you can see that the voter has turned up in Oregon, yet they're still registered in Colorado, then they send a recommendation to Colorado that says you might want to verify with your voter that they still want to be registered. By the way, they might still need to be or want to be registered because they own property for state elections. So then they reach out and actually contact the voter. This is beautiful because it creates a very loud feedback loop. Like if you're contacting people saying, "Hey, we think you moved. We think maybe you should be off the roll. Do you want to be on or off the roll," and you're wrong, that's a loud event. The second thing is when you show up in Oregon, if you're in the DMV file but you're not in the voter registration file, then it's a chance for the Oregon election officials to reach out to say –

Stewart Baker: [00:40:06] Do you want to register?

Jeff Jonas: [00:40:06] Yeah. So it really works on both sides of the equation, and hence why it's –

Stewart Baker: [00:40:11] Why it might not set off either side too much because you're saying, "We want everybody registered, but only once and only properly in the place that they actually reside."

Jeff Jonas: [00:40:22] Yeah. And anyways, my whole team, everybody's really proud of this. It originally launched in 2012 with four or five states. It's got 24 states now, plus Washington, DC, and it's just working across the country.

Stewart Baker: [00:40:34] So let me ask you the Kris Kobach question. It's been tweeted by the president that large numbers of people who are here who are not citizens may have voted. And there's some evidence, but it's pretty modest. You could answer that question.

Jeff Jonas: [00:40:56] I couldn't.

Stewart Baker: [00:40:57] Sorry. The secretaries of state could answer that question if they just asked DHS for access to the database of people who had visas to be in the United States but weren't citizens.

Jeff Jonas: [00:41:10] You could run entity resolution, and that just means matching identity data. If it was legal and within policy to have both data sets, you could run that and you could see where there was overlap. Yeah. Just like they also load the deceased persons file where you have name and date of birth and ZIP code.

Stewart Baker: [00:41:29] So Kris Kobach's question that he set up this whole process – that is more or less collapsed now – to answer, he probably could answer it today if the USCIS [United States Citizenship and Immigration Services], which keeps the visa records, simply said, "Sure. You can resolve that." Now to exchange this information, to protect the privacy, you've been hashing the data, haven't you?

Jeff Jonas: [00:41:53] Yeah, yeah. And over a decade ago I invented this method to do match identity records but hashing the fields first. So hashing the name and the driver's license and the date of birth. In the voter registration, it turns out you only have to hash the driver's license, social [security number], and date of birth. You don't have to hash the name and address because those are public record. And the goal of it – by the way, there's lots of ways to attack these hashing schemes –

Stewart Baker: [00:42:17] Especially if you can find the social security number for a large number of people and you have their name and address, you can go back and reconstruct the hash key, I assume, and say, "Okay, so now we know how they hashed all these records."

Jeff Jonas: [00:42:33] Well, I would say it's a bit more work than that to try to hack through –

Stewart Baker: [00:42:37] Because you would have to –

Jeff Jonas: [00:42:38] We have these things called secret keys. And then you run a couple of them, and you have to steal two secrets from two places. There's a tax. But the point is, it's better than clear text, meaning text everyone can see, and it just reduces the risk of unintended disclosure, just raises the bar. And you could raise it higher with more complexity, but that system runs that way so if somebody were to just outright steal their database that the ERIC organization runs, it's got names and addresses, public record, and a bunch of stuff that would be really, really hard to turn into real data.

Stewart Baker: [00:43:11] And as I've followed your career, I've been wondering – and you were a fellow at IBM, which is a big deal.

Jeff Jonas: [00:43:21] Very proud of that. Yeah. That's probably one of the most unexpected things about my journey.

Stewart Baker: [00:43:26] Five Nobel Prize winners were your colleagues.

Jeff Jonas: [00:43:30] My peers, yeah. I'm the one that didn't finish high school. I've gotten to nomad status, where I've reduced everything I own to 180 pounds, but I have three framed things that live under a bed on my boat. But one of those framed things is my IBM Fellow certificate. It is probably the single most prized thing that I have.

Stewart Baker: [00:43:45] That's very cool. Very cool.

Jeff Jonas: [00:43:47] You can't will that. You can't pay for it. You can't will it.

Stewart Baker: [00:43:51] Yeah. Yeah. So you started your business selling – I mean your first program was junior high, if I remember right.

Jeff Jonas: [00:43:58] Yeah, I wrote a word processor for a computer no one knows anymore called a PET Commodore, and my teacher went, "Well, that works pretty well." I had smoke'n pot all that damn summer. I quit in '85, for the record. But he sold this thing to the Los Angeles school district, and I got a check. I mean talk about getting yourself out of harm's way because I was just being a bum. I'm like, "Man, you can do something you love and people send money?" So I got serious, cleaned myself up, and then just really got dedicated to writing software. It's so fun. You can have a hobby, and people send money. It's crazy.

Stewart Baker: [00:44:29] Yeah. This is how I felt about law. I said, "You just read, and then you write down what you think? And it's all indoor work?" It was great. So yes, I felt the same way when I went to law school. If you were giving advice to somebody who was technically adept in high school, enthusiastic about this, would you say, "But you still ought to go to college"?

Jeff Jonas: [00:44:54] Yeah. All my kids went to college. I would say go to college, but I would at the same time say find as many practical problems and apply yourself to them. There's just so much to be learned by doing the actual, real things. But I have certain gaps in my head because I didn't go through the normal education process. They're just –

Stewart Baker: [00:45:15] Yeah. So my bet is you think you have gaps. We all have gaps. You just know that you have them.

Jeff Jonas: [00:45:21] Oh, yeah. I am so cautious. (A) it's humbling, and (B) I'm very careful about when somebody presents something to me that's a problem that's interesting. I very instantly can either see my way through it or not. And therefore I just go, "Yeah, I actually can't help you with that. I don't have the raw material to do that."

Stewart Baker: [00:45:38] So this is what's interesting and what I only realized recently about what you do is it's not just that you're really good at figuring out ways to resolve identity. It's that you find ways to simplify the problems so that computers can address it in a way that matches intuition rather than just brute-forcing the solution.

Jeff Jonas: [00:46:04] Maybe I would say computationally efficient because you can brute-force things with computers – and a lot of people do – but that just doesn't scale.

Stewart Baker: [00:46:12] This was the problem with finding a few terrorists in 30 million visitors. You're never going to find everything about everybody. You have to start using heuristics to figure out who are we looking for, at what point do we start diving deeper on a smaller number of people.

Jeff Jonas: [00:46:35] Yeah. The more quickly you can get to a very small number of things to spend a lot of energy on, the better.

Stewart Baker: [00:46:40] Right. I mean this really is what like CBP, which has 30 seconds to evaluate people in the ordinary course, does. They collect enough data to say who's coming, what do we know a little bit about them, their travel patterns, their names, phone numbers, and if there's a hit, even a kind of modest hit, that says there was a problem with this person they say, "Well, okay. Let's put them on a list of people. Prioritize the list. And whoever comes up at the top of the list, we're for sure going to talk to, and in the middle of the list, the likelihood that they're going to get talked to depends in part on how they do in that 30 seconds with the guy at the border." And that's basically saying we're going to have some rules of thumb that allow us to decide when we're going to dive deeper, and when they dive deeper, they're going to spend two hours with you asking you questions and looking at your stuff – all 180 pounds of it.

Jeff Jonas: [00:47:40] It makes me remember I was on a flight once, and the guy sitting next to me had been at the same apartment as Mohamed Atta. He literally lived in that guy's – not while Mohamed Atta was living there – but he lived in the same apartment.

Stewart Baker: [00:47:52] I bet he got stopped a fair amount.

Jeff Jonas: [00:47:53] And I'm like, "Oh, man, that's going to haunt you for a long time." I didn't really have a remedy for him on that. A lot of these systems don't take enough care when it comes to dates, like the dates that somebody lives there. Just address or address. Address's the same, but people move every five years so –

Stewart Baker: [00:48:10] But you would say, wouldn't you, that that is data.

Jeff Jonas: [00:48:14] Yes!

Stewart Baker: [00:48:14] The fact that he lived there two years later might be significant or might not. Right? Maybe the lease was handed down from terrorist to terrorist?

Jeff Jonas: [00:48:23] The reality is probably not. In fact, it's a funny thing about Big Data. I'll be talking to somebody in Big Data from time to time – I'll say newbies in this case – they'll say, "Yeah, I've got all this Big Data, and I'm going to look in it for anomalies, things that are rare." And I just look at them and go, "Man, in Big Data, things that are rare" –

Stewart Baker: [00:48:41] Are everyday.

Jeff Jonas: [00:48:41] Yeah. Things that are one in a million happen a million times a day.

Stewart Baker: [00:48:49] Right. So you can't look for – or then you'll only be looking for anomalies like this is the first time a redheaded person has stood on his head and typed that key.

Jeff Jonas: [00:49:00] Right. The tail is so long of these rare events. So it really takes collections of things, and those collections of things rarely occur on one transaction, meaning one puzzle piece.

Stewart Baker: [00:49:10] Yeah. So the thing that I liked that I learned this time around is about how your mind works.

Jeff Jonas: [00:49:20] What? Tell me!

Stewart Baker: [00:49:21] Was the asteroid problem, where it was not an entity resolution problem exactly, but it was taking a computationally infeasible problem and kind of quickly resolving it. Plus, if we don't get hit by an asteroid because NASA saves us, we'll all be sending checks to you.

Jeff Jonas: [00:49:46] Yeah, if I save Earth, you're gonna owe me. That problem was I was meeting with astronomers – first I'll say I was working with the Singaporeans around maritime and figuring out which vessels are the most interesting in the Malacca Straits – half the world's oil supply, a third of the world's commodities. And in that project –

Stewart Baker: [00:50:02] And probably 20% of the world's pirates, if I remember right.

Jeff Jonas: [00:50:04] Those are actually off the tip of Africa. But one of the data points that they have is where vessels are and how they move around. And I crafted something I call the space-time box so you could figure out how long something was hanging out in the same space – and big spaces like 20km or tiny spaces like 610m. Well, the Singaporeans said, "Hey, we love this. Can you add Z?" I'm like, "That's crazy!" – Z, elevation – "That's crazy! Ships don't float!" I mean if they're in the bottom of the sea –

Stewart Baker: [00:50:32] They don't hover!

Jeff Jonas: [00:50:33] They don't hover. They don't fly. And if they're on the bottom of the sea, who cares? And you know they said, "Airplanes." So I worked with my team and crafted Z. And I wanted to test it, but I didn't want to test it on anything that had to do with people, and it turns out asteroids have no privacy. They all are potentially evil bastards, and no one is gonna go say we're invading their privacy. So I went and met with astronomers, and they told me I had a problem.

Stewart Baker: [00:50:59] So you actually were trying to solve the problem of what to do with ships, and you said, "Why don't I look for a problem that doesn't have the privacy constraint on it and see whether I can solve that problem?"

Jeff Jonas: [00:51:11] Yeah. So I went and hung out at the Institute of Astronomy in Hawaii at the University of Honolulu, and they taught me about astronomy. And I asked a bunch of dumb questions, but along the journey, they said, "Now and then asteroids hit each other, but we only see them after the fact. The first time this ever happened was in 2010. Hubble was taking a deep space picture, and in the middle of the picture was a giant ‘X’ because it was two asteroids that pounded into each other."

Stewart Baker: [00:51:37] Wow! And then bounced out?

Jeff Jonas: [00:51:38] Yeah. And then they're going who knows where. They're not going where you thought they were going. Now where are they going? So I asked the question, I go, "Well, you know these 6-700,000 asteroids, and you know they don't hit Earth. You know their orbits. Why don't you just check to see if they're going to hit each other?" And then they just said to me, "I don't think you understand. This is something called multi-body orbit math, which means you use a lot of compute. It's an n-squared problem. You'd need 10 million computer hours." And then I went, "Well, but why would you even try to solve it that way?" This is one of those examples where it just popped into my head. I go, "Why wouldn't you just solve it this other way?" So I told them about this other way in about a minute, and they went, "That could work," and I could see it in my head and went, "Of course it would work." And we delivered to them a 25-year forward forecast of every asteroid getting close to every asteroid.

Stewart Baker: [00:52:19] And the way you did that, if I can oversimplify this – correct me – is you said, "Alright, we know where they all are in the sky. And" –

Jeff Jonas: [00:52:30] We know their orbits.

Stewart Baker: [00:52:31] "And we know their orbits. So we know when two of them are within a parsec or two of each other. And so instead of looking at every orbit and every asteroid, why don't we just look at the ones that are reasonably close and start calculating whether they're going to bump into each other?"

Jeff Jonas: [00:52:52] Yeah. And the way that we did that, though, was we went to the first asteroid and we said, "Where are you gonna be tomorrow at noon?" And this old ancient Fortran code that they still use – we're all going to die – their ancient code comes back and goes, "It's gonna be right here tomorrow at noon, like exactly right here." And what we do is go, "Yeah, yeah, yeah. Who cares? What ZIP code is that?" Pretty big space-time box. And then we say, "Where's that asteroid gonna be the day after tomorrow at noon?" And it comes back, "Oh, right here." We're like, "Yeah, yeah, yeah. What ZIP code is that?" So we just went to all of these between 600,000 and 700,000 asteroids, and we said, "Where are you gonna be every day at noon?" And then we just fuzzed it up into ZIP codes, and it turns out on any given day, there's only 2,000 asteroids in the same ZIP. So then we went back to those asteroids and say, "Where are you gonna be every hour? Where are you gonna be at 1 AM, 2 AM, 3 AM?" But it's a smaller number. And it turns out then, the total number of asteroids that are going to be in the same – call it a street because that's a smaller space-time box – that are gonna be on the same street on the same hour. Then you go run their heavy Fortran program. Well, when you do that, it goes from a 10 million hour computer problem to a couple thousand hour computer problem. We gave them a 25-year forecast, and now for the first time, astronomers are able to look in space and watch two asteroids glaze each other on purpose. Yeah. It was really a fun project.

Stewart Baker: [00:54:11] And what's beautiful about it is that it's kind of counter-intuitive because you're basically saying fuzzier data is better data.

Jeff Jonas: [00:54:21] Fuzzier... If you fuzz things up first, it allows you to operate on the abstract, and then only when you need to, spend the heavy compute. And all too often I see people in my field using heavy compute for everything because they can.

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

Stewart Baker: [00:54:32] Right. And you could do the same thing with trying to disambiguate people. You say, "I don't care whether your address is exactly the same because sometimes it will have a suite. Sometimes it won't. Sometimes it'll put northwest on it if it's in DC, and sometimes it won't." So you're not looking for exact matches. You're looking for – and people misspell Connecticut –

Jeff Jonas: [00:54:53] To find candidates. To find candidates. And by the way, it's the same way when you put a puzzle together at home. Let's say the puzzle is 75% done. You get the next puzzle piece out of the box. It's got some red and white on it. You don't go try it on every piece. You don't go start in the top left corner and try it everywhere. You look at the puzzle and say, "Hey, are there any other red and white pieces?" And then you just test it on those. That process – I'll tell you, too often in computer science, they go, "Well, you just start in the top left. You just scan it on every single one," and instead of saying which ones are even potential, that have even red or white. That's kind of fuzzy. It's not perfect red and white. It's not the exact shape of red and white. It's just anything with red and white.

Stewart Baker: [00:55:29] This is great. And I like to think that this is you saying, "I can only think about this so long because I've got another Ironman tomorrow. And there's only so much I can think about while I'm running, swimming, biking. So I have to simplify these problems down to something that I can process."

Jeff Jonas: [00:55:50] There's some truth to that, man.

Stewart Baker: [00:55:53] So you hold a record – or held a record – for having run every Ironman in the world?

Jeff Jonas: [00:55:59] Well, there's five of us that have done every Ironman. Like, if you go to the Ironman website, it's just got like four or five –

Stewart Baker: [00:56:04] And do you fall off that list when somebody invents a new Ironman?

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

Jeff Jonas: [00:56:08] No, then we all – this whole club, the five of us – have to go and do it.

Stewart Baker: [00:56:11] Oh, so it guarantees if I started an Ironman, I would have guaranteed five!

Jeff Jonas: [00:56:16] You'd have a minimum of five. The five of us show up. But I'm the only American. There's two Canadians, a Mexican, a German who's the newest one in the club, and then I'm representing America. I've got two this year.

Stewart Baker: [00:56:26] That's very cool. That's very cool. So last question, maybe two parts. We usually ask people what events they have coming up that listeners might want to participate in or documents, reports they're issuing. But before you do that, I want to ask you a harder question. You may not answer it. We've talked about things you *have* done. What challenges are you looking at now that you haven't talked about that you're comfortable discussing publicly?

Jeff Jonas: [00:57:02] You know if I could, when I graduate from this current entity resolution work, there's a way to apply the technology that we have to some interesting problems in life science and biology.

Stewart Baker: [00:57:15] Okay. Which is full of kind of compromises and good-enough solutions.

Jeff Jonas: [00:57:23] Maybe.

Stewart Baker: [00:57:25] Ultimately not good enough.

Jeff Jonas: [00:57:27] I'll just give you a quick example. Let's say that there's a group that's working on studying a mold that kills 30% of the world's crops. And let's say there's some other scientists working on a protein that they think is related to

Alzheimer's. They really can't find each other. One's maybe studying a molecule. One may be studying a protein. But maybe they're compatible in shape and charge. And I can see a line of sight to do something around that to improve the quality of collaboration between very dissimilar groups.

Stewart Baker: [00:58:04] So basically processing massive amounts of published studies to say are there things in here that are in common that you wouldn't otherwise see.

Jeff Jonas: [00:58:17] So that you can connect people so that they can come together. A lot of innovation comes when you take two very diverse things and jam them together. I'll give you one example. I learned this from a talk Burt Rutan did. There's a kind of termite mound in Africa, and the shape of it allows it to be roughly the same – it gives you climate control despite the huge swings in climate of day and night in Africa. When you take those people that study those, and you put them in the same room with somebody that's studying how to make buildings and high-rises green and more energy efficient, sparks fly.

Stewart Baker: [00:58:53] So you're automating insight, innovation?

Jeff Jonas: [00:58:56] Serendipity, man! It's engineering serendipity. I want to work on that maybe five or 10 years from now when I feel like I've saved the world from its ails with regards to entity resolution. Then I'm going to try to go –

Stewart Baker: [00:59:13] And the sweet meteor of death too.

Jeff Jonas: [00:59:13] Asteroids.

Stewart Baker: [00:59:13] Okay. So for people who are intrigued by this and want to know more, what should they do?

Jeff Jonas: [00:59:19] Senzing. Or email me at jeff@senzing.com. I answer every email I get from everybody on Earth.

Stewart Baker: [00:59:25] That's amazing.

Jeff Jonas: [00:59:27] It does take a little while, but it creates a lot of goodwill, and I meet a lot of really amazing people.

Stewart Baker: [00:59:33] Alright. So we usually give our guests a mug – highly coveted Cyberlaw Podcast mug. I know you're not going to keep it, but I'm going to provide it to you. And I hope you'll give it as a gift to the person least likely to get one from me.

Jeff Jonas: [00:59:52] That person is going to have it in approximately seven minutes. They don't know it's coming.

Stewart Baker: [00:59:57] Terrific. Alright. Jeff Jonas, it's been a pleasure. It's so much fun to see you again.

Jeff Jonas: [01:00:03] I'll have a new corset this year, when you see me later this year on Halloween.

Stewart Baker: [01:00:06] Yeah, exactly. Very cool. Okay. This has been Episode 247 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Don't forget: if you've got an interviewee to suggest, send the suggestion to CyberlawPodcast@Steptoe.com, and I will send you a Cyberlaw Podcast mug if they come on the program. Occasionally I will tweet out the stories that I'm looking at, so watch @StewartBaker on Twitter if you're interested in getting a preview or commenting on it and telling me stuff that you're particularly interested in hearing our guests talk about. Go on iTunes and Stitcher and Spotify and Pocketcasts to give us ratings. We really appreciate it. Write scathing, entertaining, abusive reviews. As long as you give us the five stars, we're happy to take the abuse, and I'll even read it on the air. Coming up we're going to have John Carlin, the author of *Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*. I've resolved to ask him only questions he hasn't been asked in the many podcast interviews that he has done, so tune in to see if I get that right. Show credits: Laurie Paul and Christie Jorge are our producers; Geoff Kesler is our audio engineer; Michael Beaver is our intern; I'm Stewart Baker, your host. Please join us again in Episode 248 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.