uberknowledge

Joseph Stuntz, Director of Federal, Virtru

Federal policy, data protection, and identity fraud

Joseph talks about data protection and breaches, points out the opportunity regulation offers vendors, and welcomes the possibility of federal government sharing identity attributes to help fight synthetic identity fraud.

03:03 The different silos of data are meaningless to the end user. They just want their data to be where it should be and protected.

06:27 Data breaches will happen; it’s how a company handles them that matters. Clear and transparent communication will win customer trust.

12:04 The way we've historically treated data sharing, collaborative and risky versus closed and secure, isn't good enough anymore.

14:50 You can’t buy your way into compliance. The vendor community needs to take the regulations and work out how to make it easy for companies to be compliant.

20:19 Encryption is not a cure all, but it is a really important piece of the puzzle.

24:55 Could opening federal identity attributes for private sector identity providers and identity solution providers help fight synthetic identity fraud?

Ashwin Krishnan: [00:00:46] So we are with UberKnowledge today, and on the podcast I have a really interesting guest and his name is Joseph Stuntz. Is that how you pronounce your last name, or did I get it wrong?

Joseph Stuntz: [00:01:02] That's just fine.

Ashwin Krishnan: [00:01:04] OK, great. Joseph is with a company called Virtru. So Joseph before we get started, why don't you give a quick introduction about yourself and your company, and then we will dive right in?

Joseph Stuntz: [00:01:16] Sure, absolutely. Thank you for having me today. So I am with Virtru. We are a data protection firm, sort of secure information sharing, really focusing on security and privacy but at the data object level versus network or application level; I have just been here for a few months. Previous to that I was in consulting for a little while, and before that was at the White House Office of Management and Budget with the Office of the Federal Chief Information Officer working with the federal CISO on improving government-wide programs around security and identity management. So, I have focused in government for about the last 10 years, but really excited to be in industry now and try and develop solutions that can help across the board, both government where I'm focused but also on the commercial side.

Ashwin Krishnan: [00:02:09] Excellent. And that's a brilliant segue way into talking about your history. Let's start with an article you authored about a year ago titled, "The New DHS [the Department of Homeland Security] Breach Illustrates What's Wrong With Today's Cybersecurity Practices." But I'm going to start with the closing sentence, and this is how it reads, "Organizations should focus less on how a breach occurred (hacking, insider, fraud, etc.) and focus more on building up and preserving customer trust in their products and services." The labeling of this as a privacy incident versus a security, insider, fraud, misinformation is something you elaborated on. Can you shed some light on why this labeling is done by organizations in the first place, regardless of whether it's federal or commercial, and why talking about the impact on the customer in understandable terms is often neglected or ignored?

Joseph Stuntz: [00:03:03] Sure. This is something I'm very passionate about. I don't know if it comes from me being not smart enough to understand the different nuances between them, but I definitely have been frustrated about some of, seemingly, the silos between security, privacy, data protection, fraud, even insider threat. You know at the end of the day, from a customer perspective, my data is not where it's supposed to be. It was accessed by someone it was not supposed to be accessed by. Whether that person was an insider, whether that person was a hacktivist trying to make a political statement, whether that person was an organized criminal trying to make money, or a nation state doing espionage activity, it actually doesn't matter. The customer's data is not where it's supposed to be and it was seen by people it was not supposed to be seen by. So that has always just been, you know, there are details in terms of operationally how those different motivations and actors are different. But from the end user perspective, it truly doesn't matter.

[00:04:08] And so I've been sort of frustrated, but also slightly more optimistic recently around the initiative zero trust — which is a buzz word and something that's getting a lot of love from vendors, such as myself — but I think the actual framework behind it is really important. It doesn't matter where the person's coming from, it doesn't matter the device they're using, trust-but-verify doesn't work anymore. It's really a continuous process and that's where I want people to focus. So back to the point of that article is calling it these different things is helpful in some regulated contexts. There are rules around privacy, breaches, and notification, and that's good. Those are good things; it sort of enforces discipline in certain circumstances, but for the customer it's really irrelevant. And I applaud a lot of companies that I've worked with in consulting, and in other just talking-to situations, that are moving more of a trust and safety model and how that interacts with security, fraud, insider threat etc. It's really focusing on the data and where the data is and who's accessing the data, regardless of what you'd like to call it.

Ashwin Krishnan: [00:05:25] Yes, it's an interesting point that you make. But if you look at some of the largest breaches that have occurred on the commercial side, whether it's the Equifax breach, before that it was Target, or more recently it's Quest Diagnostics, financial and healthcare seem to be at the top of the radar, understandably so. But in an industry that's so highly regulated, and the point that you make about preserving customer trust in their products and services, I mean, you mentioned that you're more optimistic now than you were before. What sorts of behaviors have you seen in organizations that come out and build customer trust in the wake of something bad that has happened, especially in regulated industries? Because I am sure in the unregulated industries, probably there is more room for, let's say, innovation in terms of how do you approach it. But in regulated industries how does how does a vendor go about doing the right thing, even if they want to?

Joseph Stuntz: [00:06:27] Yeah. So, I will say there's both been progress because people have to make progress, and progress just being more transparent. I think as a customer, going back to some of the privacy legislation, one of the problems is the terms of service are hundreds of pages and written in words I certainly don't understand. And instead of that continuing to be OK for things like breach notification, I think there have been some really good examples of where something happened and people or an organization, excuse me, did a really good job of communicating clearly and as upfront as possible. I think in general, people, end users are sadly used to these types of events happening. And so, the more that an organization can be upfront and as transparent as possible, even in a regulated space — whether you're supposed to do so in 72 hours, whatever the regulation says that

"Terms of service are hundreds of pages and written in words I certainly don't understand."

an organization falls under — upfront is really going to win that customer trust. Things happen. Customers are sadly in 2019 aware that issues occur. And so being upfront and transparent is a way to bring them into the process: here's what happened, here's what happened with your data — this is this customer's data; the organization is just the custodian of it — and here's what we're doing about it, and we will keep you informed along the way.

[00:07:54] I think where people get really frustrated, and I will include myself in this, is when we find out about something after the fact, even if there was no action that we could have taken. Just being uninformed, feeling like something was hidden from us, I think, makes a customer feel much worse. And so being upfront, this happened, we're addressing it in the following ways, we will communicate in the following ways going forward. I mean, Equifax has had plenty of people pile on, for lack of a better term, and we don't need to go do that again. But the fact that they had a website that they linked people to that was actually a phishing site that people got an email about or just the fact that it happened is what it is. It's really how you address it. We've seen, unfortunately, that example highlights that when you point people to a website that seems to make things even worse, that is one of the fastest ways to lose customer trust. And I think we saw a pretty unique thing happen where Moody's actually downgraded them as a response to mainly the costs that they had to incur because of this. But hopefully that starts to take into account other things like customer trust and reputation, so a company can really do the right thing and be rewarded for it versus be downgraded for it.

"This is the customer's data; the organization is just the custodian of it."

Ashwin Krishnan: [00:09:21] Yeah. And that's a great point. So when I was researching you prior to the podcast, I stumbled upon something else that you had written. And it was very positively reinforced just looking at what the OMB this week published regarding the memorandum on U.S. federal data strategy and you were quoted there. But just for the purpose of the listeners, it outlines 10 principles and the categories were really interesting comprising ethical governance, conscious design, and learning culture.

[00:09:53] But the thing that I want to call your attention to — and this is a big one, it is something that affects everybody, and I know you're passionate about it, so I want to probe a little bit deeper — how does the connection between generating value while maintaining privacy and the protection of data work? And this is huge, right? In the context of the federal agencies sharing of data results in higher efficiency and higher value for the end user, but it needs to be done transparently, and it needs to be done with data protection in mind. Given what your experience is with the federal agencies and the need to share data, and on the commercial side, what we saw with Facebook-Cambridge Analytica as just one example, how do organizations really come to terms with the need to provide personalization, the need to provide value, yet at the same time ethical governance and transparency and data protection are critical? Are these really seemingly at odds with each other or is there common ground?

Joseph Stuntz: [00:10:58] That is a great question and something I am more positive on than I have been. Working at an encryption- and attribute-based access-control-focused company, like I do now, it's probably part of that optimism because I get to see some of the stuff that we're doing, and that others are doing as well, to really focus on the data again versus the network. But back to your question. For a long time, those two things have seemed to be in opposition to each other, in conflict with each other. Either it's you swing the pendulum, we're going to close everything down, so in theory we're more secure, but we're not going to actually generate value with the data that we have. Or we're going to be open and collaborative and share, but we run the risk that the wrong person will come in and be collaborative with us, and then we run the risk of breaches, etc. So that has always seemed to be a back and forth, and you try and find the right balance. I really like this data strategy because it does not accept that.

[00:12:04] I'm certainly not going to say that there are perfect ways to do this today and that if everyone just bought the magic box that this would this would be solved. But I think that it's important, a policy document like this to set the set the stage and set the priority that we are not going to accept this opposition. They have to be together, and that is a way to really emphasize that the way we've done business for a long time of open and sharing versus closed and secure that isn't good enough anymore. Again it's easier to write than it is to execute, but I think getting it down on paper and getting it into a federal policy now gives both the agencies that are implementing this, but also folks like myself and the vendor community, we have to meet this. We can't say you can be super secure or you can be open and collaborative, we have to enable agencies to do both.

[00:13:01] And so whether that's through an encryption solution, whether that's through again the zero-trust framework that ACT-IAC and Forrester and Gartner and others have talked a lot about Palo Alto. You know, it is getting to the data, and then how do you protect that in a way that gives you confidence when you're sharing? You can generate value from data while being confident that it is not going in the wrong place. We're not there yet, certainly federally or across the board, but we're seeing a lot of good momentum in that direction. And so again, this policy does not flip a light switch that says we can now do both of these at the same time, but it's a direction that people need to go and I was happy that it's in the document.

Ashwin Krishnan: [00:13:44] Yes, so leading from that answer and into talking about the evolution of regulations, just for a minute, switching gears, let's talk about GDPR which has effectively been in force for over a year now. Interestingly, a few of my past podcast guests have emphasized the fact that they are starting to now use GDPR as the baseline framework for all their customers going forward and using innovation on top of it. And exactly like you mentioned on the federal data strategy as well, the codification of what that means allows companies like yours and others to now build on top of it. Am I reading too much into it, or are you starting to see a mind shift happening in the vendor community as well? Looking at regulations not just as a checkbox in order to get past regulatory authority but rather use them as a must have and then build on top of it.

Joseph Stuntz: [00:14:50] Yeah, I think it's more of the latter and whether it's GDPR or in the US a lot of the state-level related that are very much either framed or learning from GDPR. So CCPA in California is probably the most well-known and ready to be implemented or ready to be enforced starting in January of next year. For a long time those have either been a checkbox, as you mentioned, or buy our magic box and you are automatically compliant. That is not being super honest in most cases. I'm sure there are some products out there that can do that, but in general, because there's people, processes, and technology you know you can't buy your way into compliance with a lot of this because there also are internal organizational processes, and there are also things people have to do.

[00:15:47] But from the vendor community, when a policy direction is made, whether that's through the data strategy or whether that's through a data protection regulation, hopefully it means that we're all moving in sort of the same direction. We think that we are protecting people's data through our technology, and other vendors would say the same that are in this space, and that's not because we think it's the only way to be successful. We think we are a really important piece to an organization, sort of security, again, organizational trust. We think that protecting data is a pretty important piece to that. You know, there have been a lot of rules on data breaches, there have been a lot of frameworks on cybersecurity and things like that, but to see GDPR and now getting these … I don't want to call them operational privacy but translating privacy from legal down to how does this impact business operations, how does this impact day-to-day work, and so I think these regulations are really important to do that.

> "The best way to go about this is to see the policy direction, and then say how do we make this easy."

[00:16:50] A lot of the privacy community focus on some of the statute and regulations in that group and that's very critical to move those forward. And so in the vendor community, how do we take the direction that we're seeing from regulators and a bunch of different areas in the United States and the E.U. and others and turn that into things that are easy to use? If we can say that we can help you be compliant with something, but it makes your business processes much longer and is much harder for users, then we certainly have not done our job. And so I think that in the vendor community, the best way to go about this is to see the policy direction, and then say how do we make this easy. If we're doing that then I think we're contributing to the better environment that we want to operate in.

Ashwin Krishnan: [00:17:37] Correct. That's a great point, just in terms of how the vendor mindshift needs to change. Talking about data protection and privacy, one of my past podcast guests who is, I believe, a connection of yours as well, Dr.

Andrea Little Limbago had authored this article entitled, "Stop Demonizing Encryption," after the discovery of the WhatsApp encryption vulnerability. It's a great article, just talking about this is not the time to pile on, on why encryption is broken etc. So two questions: the first is, given your role, both in the past as well as with Virtru today, what is your take on where encryption as a technology stands? I know there have been all kinds of doomsday scenarios of whether it's quantum computing or in the case of WhatsApp, it's end-to-end encryption, except now this is a vulnerability. So, is it expected that the world continues to have blind faith in encryption, or completely disavowing encryption when something like the WhatsApp thing happens or is there, just like you mentioned zero trust before, is there a way to assess encryption and its trustworthiness?

Joseph Stuntz: [00:18:54] Yeah, so Dr. Limbago is much smarter than I am, so if I can get through this half as well as her article does, I'll be happy.

Ashwin Krishnan: [00:19:01] [Laughs]

Joseph Stuntz: [00:19:02] With that said, we — her and I — completely agree on this topic. The fact that a vulnerability was discovered in one particular instance of an encryption implementation, by no means should we all ignore the value that encryption brings. In a lot of ways, there are a whole bunch of other technologies that when implemented incorrectly or configured, misconfigured if you will, we don't throw all those out. Every time someone finds an unencrypted S3 bucket, we all don't immediately say we should stop using the cloud. I certainly understand that when there's a public vulnerability that there is backlash to that, and that is appropriate in a lot of cases. But in this one, you know, encryption has been around for a long time because it works. Now it has not been the easiest to use, and going back to my previous answer, we in the community have to do a really good job of making this stuff easy to use or else people will get around it to do their jobs and to get what they need to get done, which really negates the security impacts.

> "Encryption has been around for a long time because it works."

[00:20:19] But on encryption specifically, it is a really important piece of the puzzle. It is not a security program. It is not a one size fits all. It is not a light switch that you turn on encryption and everything's good. But it is really important. Even just TLS, that's an encrypted connection that there are advantages to that. There are also disadvantages, in terms of not knowing where the content is going at the end, sort of that last mile. We at Virtru focus on true end-to-end encryption in our in our email solution. It's done on the browser of the individual that's receiving the message. So we never see the content and the content provider, whether it's Google or Microsoft or whoever it is, never has the encryption key. So the only people that can see the decrypted message are the person who sent it and the person who receives it. And that's just sort of an operational example of a zero-trust-type framework. We never see the content. We don't really want to see the content. And Microsoft and Google don't get the encryption key, so they never can decrypt the content. So that provides a lot of value.

[00:21:33] And again, as a technology, encryption is very valuable. There are certainly implementations of it and vulnerabilities, you know you get into someone's device and then you can see the content when it's decrypted because you're already in the device. That is certainly a risk, but that isn't necessarily because the encryption is bad, that's because the security on the device was not enough for the use case.

[00:22:00] So I think, in general encryption, is a very helpful tool, and I believe it, and that's why I currently work where I work. But I also think that it has to be seen as a tool in the toolbox and certainly not as, "well this is encrypted so it's definitely secure." It has to be put in the right context of the device you're using and other things to think about. That's a long answer, but this is something we are certainly very passionate about here because we've seen some of the use cases that we've been able to help people with. Whether that's internationally working with folks that may want to get information out of a country, out of a government securely, and you know, encryption is a really helpful tool for that.

> "Whenever I hear, 'We should stop doing X,' my first question is, "And replace it with what?""

Ashwin Krishnan: [00:22:49] Got it. That's a great answer. Don't trust it blindly, but at the same time don't wait for the first opportunity to start calling it unworthy of trust.

Joseph Stuntz: [00:23:02] You know, whenever I hear, "We should stop doing X," my first question is, "And replace it with what?"

Ashwin Krishnan: [00:23:13] Right.

Joseph Stuntz: [00:23:14] It's very easy to criticize, and I've certainly done it. Again, I've misconfigured cloud buckets that just leak hundreds of millions of records; that strikes me as not great. And you know sometimes I've criticized those events before, but the cloud provides so many benefits in terms of efficiency and scalability and speed and all that. Do you want everyone to go back to on-premise? Well, probably not. So we just we have to be realistic with the tools we have today, and how to actually make them as useful as we can, while not just throwing everything out the second something happens.

Ashwin Krishnan: [00:23:58] Absolutely. So Joseph, one last question and this is again something you mentioned earlier as part of your tenure at the OMB is the consolidated identity management policy. The first question is, on the face of it, I can see why a common identity across agencies would be a good thing. On the flip side, again the commercial equivalent is maybe a Facebook login or a Google API login across third-party websites and applications as well, does a common identity actually make things easier for the hacker because instead of going after ten different LDAP databases, they can just go after one and be able to crack that open and have at it? Or do you see the benefits far outweighing the risks?

Joseph Stuntz: [00:24:55] Yeah, this was something we talked about when I was in government and even before when I was working with a number of agencies in a more consulting capacity. There are trade-offs, you know, not dissimilar to the openness versus closed discussion that we had earlier. But we have, as the policy lays out, a number of different items. I think there's centralization but with the centralization piece there is additional risk that you just highlighted but that can be ... you know, there are already today a number of identity systems in government and it is certainly easier to manage one versus many. There are risks factors, and so how do you manage that from a segmentation and some more technical controls and things like that. But where I'm really excited about that policy in particular that came out a few weeks ago is, they talk about opening federal identity attributes for private sector identity providers and identity solution providers to leverage those federal attributes. And this is something that, again there are experts in this field who have been working on this topic for a long time, but could you be able to go to the Social Security Administration to verify Social Security numbers and a couple other attributes to fight synthetic identity fraud? I know there's a movement on that on The Hill recently as well. And this seems like something that SSA is going to be doing and that is incredibly exciting. Synthetic identity fraud is a huge problem: the combination of real attributes from different people to create someone who doesn't exist but has real attributes when taken on their own each individual attribute. There are only a few places that are well equipped to do that.

"Synthetic identity fraud is a huge problem."

[00:26:48] And federal government as the holder of a lot of these attributes, either the originator of them for something like your Social Security number or the holder of them in terms of tax information etc., is uniquely positioned to verify attributes and combinations. The federal government has to do that in a preserving, privacy-enhancing way, ideally. And that is also set in the policy. But it's really again going back to that getting the value out of the data. The federal government has this information; it could help solve really, really expensive problems and synthetic identity fraud, and they should do that. And again, that doesn't mean when you write it in policy that it happens tomorrow. But it's really exciting that the government is moving towards opening up more while continuing to state that privacy and security have to be built in. So now the smart people, not necessarily including myself in that, but the smart people can go say, "All right, given that we need to protect privacy and security, how can we open up these identity attributes to protect people online?" And I think that's a really exciting mission. And I was excited to see it in the OMB policy.

Ashwin Krishnan: [00:28:02] Yeah I think the light that you shed on synthetic identities is a great one because I think lots of times the average person, myself included, doesn't think much about those kinds of issues, unless it happens to you, in which case all hell breaks loose.

Joseph Stultz [00:28:20] Yeah, and it seems like, I don't want to say it's victimless, but there isn't a real person that's going to get a credit report, but there is a social security number attached to it that comes from a real person and an address that comes from someone else, and it just costs institutions so much and that makes them worse off in terms of their financial performance. You know, synthetic identity fraud is complex, but if government can help address it, they should be.

Ashwin Krishnan: [00:28:49] Great. This has been a really interesting conversation. Joseph, I thank you for your time and looking forward to seeing more success for you and Virtru going forward.

Joseph Stuntz: [00:29:02] Thank you for having me. I appreciate your questions because some of my articles and papers go a little all over the place, so I appreciate you taking the time to read them. All right. Thank you.

Ashwin Krishnan: [00:29:16] Absolutely. Thanks, Joseph.