Dr. Andrea Little Limbago, Chief Social Scientist, Virtru

The Human Element at the Overlap of Privacy and Security

Andrea stresses the importance of quality over quantity when collecting data and says companies need to be able to explain what data is going into their AI models and why. She says it's time the security industry look at how humans interact with technology and tailor their products accordingly. Andrea firmly believes the best way to increase gender diversity in this male-dominated field is to emphasize women and their achievements.

00:47 Andrea's unique role and responsibilities where social science meets cybersecurity
03:45 Hacks are not just security issues but privacy issues too.
06:04 The big data revolution came so quickly that people threw everything in to achieve results. Now we are seeing the repercussions of biases.
08:20 GDPR the disruptor is still evolving.
11:14 Move away from the focus on the user as the weakest link and actually making the technology work better for the user.
14:32 Passwords are not something that works well with the way that the human mind works.
16:57 The security community is a really creative group of people.
20:01 Displaying the diverse aspects of a career in cybersecurity will help increase diversity among the practitioners.
20:54 Security is bigger than your current sphere: This is an area where we can help protect our democracy and democracy around the globe.

21:22 The lack of diversity in cyber cannot be ignored, but the best way to combat is to highlight and elevate and amplify the voices of women as it pertains to their expertise.
24:21 Increasing diversity is not just the responsibility of the underrepresented, it is everyone’s responsibility.

Ashwin Krishnan: [00:00:01] So with me today on the UberKnowledge podcast, I have a very illustrious guest by the name of Dr. Andrea Little Limbago. I will not even attempt to read through her LinkedIn description. It's quite impressive. Instead I'll have her just talk about what she does. Andrea, the thing that I found really interesting is your title of Chief Social Scientist. I'm really interested in that and can you explain where you came from and where you are right now. Just for introducing yourself to our audience.

Dr. Andrea Little Limbago: [00:00:31] Ok, thanks very much for having me. I think I may be one of the only Chief Social Scientists in our industry. And partly because I made up the title a little while ago. This is self-anointed.

[00:00:44] Basically what I do is, I have a background in social science, and my academic training is in political science with quantitative studies focusing on international relations. So, I came into cybersecurity through the national security path through academia and then the Department of Defense to where I am now, which is the Chief Social Scientist at Virtru. There I do a lot of research on the various global trends focusing on data privacy regulation and, really, the overlap between security and privacy. Before they'd been their own circles, but now there's more of a Venn diagram where they're overlapping. So, I do a lot on the human element of what's going on at the overlap of privacy and security, and that's where a lot of the social science comes in. Then I also do a fair amount of work as the bridge builder translating a lot of our more technical work, so that it's more consumable for a broader audience. And then there's also the aspect of culture, so working on culture within my own company and then within the community as well, especially in the areas of inclusion and diversity.

Ashwin Krishnan: [00:01:46] So that is a lot of ground to cover, and all those are just super interesting topics. Let's start with the one that you mentioned earlier, security and privacy. One of my past guests made a really interesting comment, which just stuck in my head. I don't have an answer for it, and I just want to throw it by you. Until GDPR happened, there wasn't a target number that the attackers could go after. But now, with fines of four percent or 20 million euros, one of the things he was saying was he's starting to see ransomware as a service. Where I, Ashwin, would come to you grandly and say, "You know what? I have 50 percent of your customer's information with me. Pay me a fraction of what you would otherwise pay the regulators and I will go away." I mean, it seems a little far-fetched, but it's not really because now you look at it from a risk-mitigation standpoint and a cyber-risk protection standpoint. Would it be less of a hassle to pay me off versus asking me to show what I've got and then get into all the unnecessary publicity? What do you see when we tackle security and privacy? Is this as far-fetched as it seems or is it getting more real?

Dr. Andrea Little Limbago: [00:03:02] I don't think it's as far-fetched as it seems. I don't think that necessarily is the norm, but, at the end of the day, everything comes back to incentives. As the regulations come into play, they're going to impact both attackers and defenders in different ways. Assuming that it is only relevant for one and not the other, I think is actually part of the challenge that we've had for so long. We've really always focused on one and not the other, as opposed to looking at what the various incentives are for each of them and seeing what drives attackers to behave in certain ways and then looking at what incentives we can offer to help promote better security and better defenses. I don't think that's far-fetched.

[00:03:45] Then looking at the intersection of security and privacy, what's been interesting has been with the Marriott breach. It has somewhat been almost a turning point in some of the discussions where China has now been pointed to — if it turns out that they are the ones attributed to the Marriott hack — just looking at how much data they compiled, possibly as far back as 2014, and the privacy implications of it. And for so long it has been framed as a security issue, which it is 100 percent, but then taking the steps now looking at all the travel data, the Anthem data, the OPM data, and so forth, it's actually a huge privacy concern as well. And so that's where you're starting to see a lot of these attacks have really been framed, for the last, I'd say at least five years, when a lot of discussion really started coming mainstream. I kind of point to the Sony hack as to when a lot of discussion went mainstream and certainly happened before then. But as far as awareness of the broader population, that's where a lot of discussion really started to take off. And even now, one shows a fair amount of the emails being posted online. It was a privacy concern but really it dominated more so as a security component with North Korea. And so actually looking at it as a security challenge, we still need to maintain doing that. We also have to understand that there are privacy implications as well. But the good news is that ideally approaching it as both privacy and security concerns can also help guide a strategy to defend against this.

Ashwin Krishnan: [00:05:18] Absolutely, yes. One of the things, as you were speaking, that came to mind is this whole march towards AI and automation and data sets and machine learning. From a competitive standpoint, isn't there a dueling force over here? One is to say, "OK, reduce the amount of data that you collect for privacy reasons," but on the other hand it's, "Hey, collect as much as you can because I need it to train my models." I mean is there also tension or collisions within organizations where people are trying to be competitive versus the privacy czars and the ethics czars who are saying, "Hey, you've got to do the right thing."

Dr. Andrea Little Limbago: [00:05:57] I would almost take a middle ground on that, from my quant background there is also the garbage in, garbage out.

Ashwin Krishnan: [00:06:04] Correct.

Dr. Andrea Little Limbago: [00:06:04] You can have all the data in the world, but if you're training it on data that's not that great your AI, or more so machine learning right now, really won't be that helpful anyway. And so, if you are throwing in everything, including the kitchen sink, it will not be as valuable to you as it would be if you're actually training it on useful data. So that's where I push back. Because the big data revolution came so quickly, everyone wanted to throw everything in as fast as possible and see what they could come up with. But now we're starting to see the repercussions of that with some of the biases. And some of that output may not be as useful as you would think, even some of the ethical components too, and that's sort of the discussion that's really starting to emerge, which I'm excited to see. I think that will help address the privacy and security concerns. It will highlight that we don't need to have all that data for whatever it is, for whatever objective you're trying to get on the security side, which then also helps on the privacy side.

[00:07:07] And then even on the privacy side, talking about the training data set, you still can anonymize it. Although, I think it was the New York Times that published a really great report showing how even anonymizing it, you can still figure out who it is with the geo location. That was a really interesting article if people have not seen that. But there still are additional steps that companies should take to anonymize what data they have. Steps that get at reducing what you're taking and then making sure it actually is relevant for your purpose and that's where some of the GDPR comes into play. Again, it actually is fairly broad reaching. I think when we look at it, often we focus on consent, but there are aspects on machine learning and requiring automated decisions for companies to identify what's driving those automated decisions.

Ashwin Krishnan: [00:08:04] Correct.

Dr. Andrea Little Limbago: [00:08:05] And so that's an interesting area that hasn't gotten, at least in my opinion, hasn't gotten as much of a high profile in discussions yet. But I think that is an interesting area to find out what is driving those and requiring t

[00:08:30] It is just a first step, and that's the other thing with GDPR because it has been so disruptive and it's been such a big regulatory shift. One of the biggest ones we've seen really in decades. But I'd argue, we're going to continue to see it evolve. It's at a starting point right now; it's not by any stretch the end point.

Ashwin Krishnan: [00:08:49] Absolutely. I actually want to pivot towards one of your panel discussions that I believe was at the Atlantic Council. Where you were talking about how to make security more human-centric. Can you explain? I mean, are vendors really failing today? Or is it that they're so caught up with technology, they're throwing everything at the hapless consumer even though they may not be tech-heads? So, what is human-centric security, in your opinion?

Dr. Andrea Little Limbago: [00:09:17] Yeah, we had, I think, an hour-long discussion on that, so I won't go into all the details. From my perspective, it's a couple of different things. One thing is sort of at the tactical level. It is that human-computer interaction. It really is looking at how do humans interact with the software, the applications, the whatnot and making it something that that's much easier for them to use. Whereas the tech industry has really focused on usability and simplifying and making sure that their consumers, across a broad range of demographics, can use their products. Security hasn't, for a while, had that focus. It's really been focusing more on the behind-the-scenes tech to stop the really bad things from happening without the complementary innovations on the user experience side.

[00:10:08] I think that's shifting as security is becoming more and more a core component of businesses. This is where the business model and the business demand are forcing. It has been a forcing function for the security industry. And the consumers and the users are demanding more intuitive interfaces to actually help a broader range of their workforce, or the individual, to be able to actually use the tool. You shouldn't have to have 30 years as a hacker or a PHD in Computer Science to be able to use these tools. For a lot of them, we need to make it more accessible for junior entry-level folks to come in and be able to elevate their game right away and still ensure that's meaningful and providing a lot of utility for the end of the broader workforce. So, I think there's a lot of exciting advancements that can be done in that area. And even thinking about going forward, you're just really thinking about different ways to move away from the focus on the user as the weakest link and actually making the technology work better for the user. I think that's sort of that paradigm shift I would love to start see happen. I have seen that. I was in California a few weeks ago at the Enigma conference and there were a lot more discussions on making the security checklist go away. Let's really raise the game and technology, so we don't have to force the users to go through 20 different checklists every time to make sure that they're secure.

Ashwin Krishnan: [00:11:41] So that begs another question: based on your view of the market and organizations over the past several decades, have you also seen security becoming much more embedded in the business function? Where it's not just me selling to a CISO or an IT person, I'm also selling to HR, Legal, Finance, etc.

[00:12:03] So, I know you've been having this make-a-checklist, where you go through and do some kind of stupid training and you come out of it not knowing why you wasted the last hour on it.

Dr. Andrea Little Limbago: [00:12:14] Right!

Ashwin Krishnan: [00:12:14] But have you ever seen people actually realize the fact that a phishing attack could actually cause a business to go down? We could have human impact, we could have layoffs, bad things could happen.

Dr. Andrea Little Limbago: [00:12:26] Yes.

Ashwin Krishnan: [00:12:27] And is that awareness growing or do we still have that thing where security is somebody else's problem?

Dr. Andrea Little Limbago: [00:12:32] No, no, I definitely think it's growing a lot. And one of the things that I think is most interesting is that over the last year and a half with some of the third-party data misuse, you know, high profile incidents that happened last year have basically triggered a greater awareness of what data people have and what needs to be protected. And so even though that may not be tangentially related to people who are exactly working in the legal field or in health care and so forth. It's caused some greater self-reflection, as far as how to protect their data. Also, who has access to the data, how could it be misused? It has really sparked that broader discussion. I do think that really there has been a significant shift over the last year to two years and a broader discussion and awareness of the need to protect the data, as well as the business repercussions that could happen. And that's why you start seeing more of these checklists becoming more and more prominent. And then because awareness has grown, that's where you're also starting to see some pushback. As far as, "I know this is a problem, but I don't want to have to go through these 20 different steps just to send an email to someone." Or "I don't want to have to call five different people to make sure that they really sent that pdf to me. I want other ways to know that it's already been validated, so I can go about and do my business." And so that growing awareness, in my opinion, is what triggered and help continue a greater push for more usability and more on the tech side to help promote the user behavior that ... You know, at the end of the day, there are some aspects of human behavior that are very difficult to change. And so instead of just saying you're forcing folks to act in a way that they're probably not going to act — at least not for a while, they're too embedded in their own processes. Let's make the technology work better within the current business processes in the current workflow for them. Which gets it all back to the human-computer interaction.

[00:14:32] So I'm excited to see what innovations come along in the future. Just thinking about passwords, passwords are not something that work well with the way that the human mind works. Is that really the best that we can do? And it probably is not, right? We need to be rethinking some of the old paradigms that have been around for a while and perhaps got us up to a point, but we need some rethinking and some more innovation in those areas as we move into the future because it is only going to become more interconnected and more complex.

Ashwin Krishnan: [00:15:06] So, I was reading an article that you'd written. I think it's titled, "Debunking conventional wisdom to get out of the security and privacy rut." I wonder if that was one myth you just alluded to right now, which is we must trade off between security and convenience. You talked about passwords and now two-factor authentication or multi-factor authentication is all the rage. I cannot believe the number of times that I have non-tech friends who complain about that, actually even tech friends too because they have cognitive dissonance, which is what I call it when you come home and become the dumb consumer. Just using a Google app or SMS for a second-factor authentication people just gripe.

[00:15:46] Are you starting to see innovative vendors truly walk the user experience and say either we go down the security side knowing that we're going to cause a pretty poor customer experience or we truly understand what the customer is doing and try to embed security within it? I mean it seems like you're saying, we still have passwords, we still have 2FAs, we still have other kinds of USB sticks with one-time codes. I mean that is not user friendly, in my opinion. So, what do you see happening?

Dr. Andrea Little Limbago: [00:16:23] Yeah, I agree. I think that we're at the point right now where we've acknowledged the problem and so we're really at the very beginning of brainstorming what the alternatives could be. Again, this could be one of those things that should be a competitive advantage. I work closely within our team on the user experience and design and that's where a lot of it can come into play. We have to make sure that it fits within. At the end of the day, one security tool's not going to be the one that can do all the various aspects of what everyone needs. You need to make sure that you focus on the audience, who the target audience is, who the target users are, and make sure it works within that workflow. But I think we really have just started acknowledging that the problem exists and for so long we just blamed the user and expected the user to adjust to the technology. Because we're switching that around now, I'm hopeful that we'll start seeing some more interesting discussions along the lines of making it more user friendly while still really secure. We shouldn't accept that that can't happen. I think that's just too narrow minded in our thinking and the security community is a really creative group of people, so I'd love to see that discussion evolve and see what they come up with.

Ashwin Krishnan: [00:17:44] And talking about the things that vendors come up with, and again I'm not a spokesperson for CUJO AI and I don't get paid for this, but I just talk about the CUJO AI firewall as something that I really, really feel they made a tremendous difference with and try to address that need that you mention. A non-tech consumer with an easy app which just constantly gives you an indication of which devices are talking to whom. And that's just a SOC-like view for the average consumer. So, absolutely I agree with you that it can be done, and there is evidence of companies that are starting to do that.

[00:18:20] So, switching a little bit into women in cybersecurity, and clearly this is probably going to be a big theme at RSA this year as well. Given your journey, I know you have a pretty diverse background not just in tech but also political science and other areas. Where does somebody start? Number one: how does somebody in high school or graduate school think about being in this highly male-dominated field? Number two: what are some of the learnings that you can share from what you have had to go through to inspire and empower the next generation of women leaders? To truly embrace this huge problem, as you mentioned, we need to have diverse sets of individuals with diverse backgrounds to be able to get a handle on this or at least get better at solving the security crisis that there is.

Dr. Andrea Little Limbago: [00:19:19] That's another very multilevel answer. I'll tackle the first one. You know, when I speak to high school students, college students, and so forth across both men and women, the broader mission is one of first things that I start with because it is much more of a mainstream conversation now than it was a few years ago. There’s a lot more thirst to find out how to get involved. And I think one of the interesting things to focus on is moving away from the hooded hacker. Honestly, I think that stereotype is one of the really detrimental ones, especially for getting women into the industry. And we still see it! I mean, I've written articles where they pop in that stock photo, and it just makes me cringe. But it is there. So, if we can open the aperture and make sure that students from computer science to economics to psychology to design know that there's so many different disciplines that are relevant within security. Just growing the awareness in that area really will help attract a lot more because there's so many different ways to be creative in this industry and it all goes back to really supporting both security and privacy. And then you take that even higher, you're supporting our national and economic security.

[00:20:39] A lot of my work focuses as well on that global trend of digital authoritarianism where a lot of censorship and surveillance and the astroturfing and all these different areas are coming together and coalescing. This is an area where we can help protect our democracy and democracy around the globe. So for people across a whole wide range, whether they want to get really detailed and focused on the malware or vulnerabilities and get tactical needs in that area, all the way up to the need for people with a tech background helping shape policies. There is a lot of opportunity. And so that's how I try to encourage and help spark the interest. It's really highlighting how many different ways individuals could have an impact. I think that's a really strong motivating factor.

[00:21:32] Then so far as it being male dominated, obviously we see the statistics a lot, I think the best ways are, one — focus on youth opportunities; two — highlight the really phenomenal men that are out there helping support, and there are a lot of them. I've been very fortunate that I've had these great male colleagues, male mentors, and we should focus on those relationships, but then also when we do, highlight women, especially at conferences, really have them highlight their expertise. I think it's just so critical. If young girls only hear women in the field talking about their worst days on the job and never hear them talk about their best days on the job, that's just an enormous detractor from having them actually join the industry. Women are doing so much interesting work across so many different areas of cybersecurity but that's what we need. We can't have a conference where the only women on the entire agenda are talking about what it's like to be a woman in tech or a woman in cyber.

[00:22:28] So on one hand, I understand we can't ignore that there's a problem, but they really just need to highlight the expertise a bit more because I think it's Girls Who Code to If They Can't See It They Won't Be It. We really need to highlight and elevate and amplify the voices of women as it pertains to their expertise. And I'd argue that be another area for journalists, ensuring that they're sourcing women as much as they are men because that doesn't happen. Same with articles that are published. It's across the board and there's so many different areas that we can work on to really amplify the voices of women and all that will help draw a greater and more diverse population into the field.

Ashwin Krishnan: [00:23:06] You're so right because - I don't know if it's the day or age - but the negative amplification certainly gets a lot of attention versus success or male counterparts or colleagues who've actually helped and mentored you, and you doing the same with other men and women in your organization. So that brings a much more inclusive and positive discussion rather than just focusing on the challenges. Certainly, like you're saying, we can't be overly fixated on that because that could be the turn off for lots of women.

Dr. Andrea Little Limbago: [00:23:41] Yep. In RSA this year we've seen a difference. You know after the last few years and some of the publicity that went there. We'll be doing a half-day workshop on providing women the skills to submit to conferences and having the confidence to speak at conferences, which gets back into something that we can do. If we have more women submitting to these conferences, there's a greater chance they'll be actually the speakers. There are a lot of different efforts out there that are hopefully having an impact, and we're starting to see the change going in the right direction and so we have to all help be that force of change together. All of us in the community. And that's I guess my one last comment on that: too often the diversification falls on the women or the underrepresented groups and it really needs to be everyone involved. It's not just my added responsibility, it should be everyone's responsibility to help progress the community as a whole and bring in a wider group of perspectives. If it's not everyone, it's not going to have the buy-in and it's not going to have the support of the entire community or your organization.

Ashwin Krishnan: [00:24:50] Correct. You mentioned earlier the cultural shift, and this is part of the cultural shift. It has to be embraced by a larger populace for it to actually have effect.

Dr. Andrea Little Limbago: [00:24:59] Yeah.

Ashwin Krishnan: [00:25:01] Very good. Again thanks for your time, Dr. Andrea. This has been an amazing conversation. Hopefully our listeners are getting some value out of it, so they can go and implement some of the things that you've talked about. Looking forward to engaging with you in the future and looking forward to seeing you at RSA as well.

Dr. Andrea Little Limbago: [00:25:19] Yeah. Thank you very much. It was a fun conversation.

Ashwin Krishnan: [00:25:20] Thank you.