Laura Noren, Director of Research, Obsidian Security

Tech, Cybersecurity, and Ethics

Coming from years in academia, Laura brings a unique perspective to the security space. She talks about the insular nature of the cybersecurity community; the need for a conversation about ethics and the part VCs have to play there. She exhorts the industry to create their way out of the problem, not just delete and retreat, while pointing to the unique clout of tech employees and their part to play in helping society figure out the appropriate use of technology.

Ashwin Krishnan: [00:00:02] Welcome, Laura, to this podcast. I know we're going to touch upon a topic which is not reported. I was about to use the word under-reported, but that means there is some reporting but there's nothing at all, which is security and tech. But before we go there, just for our listeners, your background is very interesting. You spent a long time in academia and now you've entered the vendor space. What are some of the 'aha' moments or things that startle you coming into this security community.

Laura Noren: [00:00:37] Yes, I just left academia. I was doing a postdoc at NYU and the Center for Data Science, so my entire academic background has really been weaving sociology and tech together. Coming into this community the first things that I'm seeing are just how how sealed and self-contained cybersecurity really is. The vendors all know each other. The CISOs all know each other. They all know the vendors, and the journalists all pretty much cover just this area, they cover cybersecurity. And there isn't really a lot of layering back into the greater tech, which means that the conversation about tech ethics that's surrounding Facebook, surrounding self-driving cars, all those kinds of things, it's not being inserted into cybersecurity. It's just too much of a self-contained unit to layer over that.

Ashwin Krishnan: [00:01:30] So in your opinion, what needs to change, because as you can see with Black Hat, there is already an overload in terms of what vendors are producing. Whether it's effective or not is a different question because there's a lot of noise. The number of vendors on the show floor is evidence of that. Also, the CISOs are getting bombarded with more and more vendor pitches. So, in this world, how is the topic of ethics even getting started in the conversation, be it on the vendor side or the practitioner side?

Laura Noren: [00:02:11] Well really it takes either a company, a vendor, a CISO, or a journalist with some courage to just say, "Hey, we've got to change." We need to change the way this conversation is going; it's gotten too narrow. We're leaving important considerations by the wayside for someone else to deal with, and frankly, there isn't anyone else addressing this. How do we deal with the fact that legally most of the companies out there that cybersecurity vendors are talking to can do a lot of surveillance on employee data. We know that legally they can do that. They're not getting away with it. That just is what's legal. Is there a conversation about ethics that we need to be having so that this field can avoid what happened to Facebook? Facebook had a business model that was okeydokey with everyone for a long time, except a few - frankly my academic peers and I were the critics, shaming, shame fingering, shaking our fingers, you can't do that, you can't do that, and finally history caught up with that moment. What remains to be seen is exactly how Facebook is going to change, but we'd like to be a leader in cybersecurity saying, 'Let's rethink this.' Who comes first, is it the customer, is it the employee? Let's have that conversation and see if we can come up with creative solutions that will give you better cybersecurity and more secure environments and reintroduce the concept of the civil liberties that employees might have. You don't usually think of employees in terms of civil liberties, that's just not a conversation that's happening. Probably a lot of people are allergic to it and are howling right now.

Ashwin Krishnan: [00:03:57] One of the things that I see having come from the tech vendor space, and now kind of outside of it but still watching in, is the incestuous relationships that employees have with their employers in the tech world. And lots of times, essentially you never think work rights as an employee, as potentially you would if you were in a different industry where you had a union. And there's this concept of employer and employee. Here, thanks to Facebook, Google, and others, even non-traditional B2C companies and B2B companies that I've been part of, you are either are in it or you are not. And if you're in it, you give up all your rights. So, even from an employee perspective, even if there's a notion of activism, the culture needs to change to say, 'OK, while you're at work you're on a mission, but you're individual and who you are and that still needs to be at the forefront.' I think sometimes that gets lost, or most of the time it gets lost, because you have to drink the Kool-Aid.

Laura Noren: [00:05:08] Yeah. I would like to point out there are a couple of them. There are a significant number of companies that are trying to be more inclusive, which means that they do try to expand, say, healthcare access to LGBTQIA populations before that was ever a regulation. So there is actually a fairly long history of that in tech, but that kind of inclusivity and recognizing populations that maybe are a numerical minority or have unique needs or both, is a little different than some of the activism that is coming out of Google right now. They're not looking for the typical kinds of things that a union would be looking for, it's not about healthcare access, it's about putting their intellectual and virtuous persona as back up to the products that they're willing to work on. And I think that's really, really interesting and it's good. It's good for us because they're building the world we live in, whether we are aware of that or not.

Ashwin Krishnan: [00:06:13] Let's start with Google for a minute because this whole Project Maven thing has obviously gotten a lot of attention. The reason I think Google is able to do that is partly because of its muscle and because of the kinds of talent it attracts, the diversity of population, and they give the employees a voice, which is important. But the biggest thing about Project

Maven, and I've tested this with a few people and it has raised more questions than answers, is, going back to ethics, where does the discussion about - do you care about how your customer uses your product? And if the customer uses the product in ways that you had not envisioned, do you have an obligation to do what Google did, which was say, 'I'm not going to sell drones to the US government'? Again, I don't see any talk track over here - I don't see anybody talking about those things. So where that awareness needs to come, or be a discussion at, is product inception, product definition. We expect this product will be used in these kinds of environments. If it isn't and if you get a feeling that it's being used for drone-based killing then we got to pull the plug, right?

Laura Noren: [00:07:41] I'm going take a 30,000-ft view on this one. From the sociological perspective of how does a community figure out what is appropriate use of technology, that is actually a very old question. Usually, when you see this functioning in a healthy way, it comes out of the entire ecosystem of all the players. So it's good to have journalists around who are critical, they're not trying to sell, they're not themselves oohed and aahed by all the new features and artificial intelligence. They're asking the hard questions. They can start these conversations. But obviously a journalist has a limited capacity to create a different kind of product. They're not out there building products, they can't create their way out of this problem, and they can't make purchase decisions. Everyone in the ecosystem has some kind of responsibility. Typically, where we see this function the best is where there are industries that make products that can have really negative unintended consequences; you see that they develop a really strong professional ethic. Journalists for instance, journalism is a for-profit entity but many journalists have signed onto a pretty strict code of ethics that prevents them from doing things like, shilling for a particular person, taking kickbacks, citing sources that don't exist, plagiarizing. So those strongholds of professional ethics do matter. Of course, as a sociologist, I'm sort of biased towards the flexible social fabrics that keep us moving in the right direction. But frankly, if there is a better strategy I don't know what it is. I do not think that the better strategy is to try to rigidly build our way out of this, like the technology detects it's being used and then it just shuts. No, that's not, we're never going to get there. It's always humans, we are always going to be in this loop. And that's how it's going to succeed. Humans are the best of what we have to offer on this planet and we're also the worst.

Ashwin Krishnan: [00:09:52] From a security vendor's perspective right now, given that there is no place for having this discussion, either with the customer or inside your own company, where do you think the conversation has to start? We've had this concept of the chief ethics officer, and usually the Band-Aid solution is to bring an outside entity to do this new-fangled job to get the regulators off our back. Or you have the social conscience that you appease. Where do we start? Is it at the board level, is it like the Google cases at the grassroots level? Is there a one size fits all?

Laura Noren: [00:10:32] In the Google case, I think that was pretty powerful. They had thousands of people signing onto this petition. It happens to be in tech where there's not just a surplus of thousands of talented workers, so that was pretty powerful. Obviously the traditional answer would be, it should start with leadership, and I agree with that. For us, one small vendor in a sea of many vendors, we want to flip the script a little bit on what it means to do ethics. For us it doesn't mean we're going to come in and tell you what you shouldn't do. That is the antithesis of technological innovation, finding out what you can't do. Innovation is about finding out what you can do. And so we're flipping it and we're saying, “Look you can add this feature and it will improve your cybersecurity, but it will also help you enable your employees to be active participants. It will cost you nothing and it will give them a lot of privacy protection that they didn't already have. Look at this awesome feature we can add,” because that's the way the language goes. Would I wish that it were some other way, and we were all reading philosophy? I don't even know, but maybe that wouldn't be so good either. But that's how we're trying to flip the script. Let's make ethics about how do you create your way out of this problem, not how do you delete and retreat, which to some degree it is how I feel about the GDPR. It has some really good features, but in essence to me it seems like it's fundamentally a delete and retreat strategy.

Ashwin Krishnan: [00:12:06] The other participant of this whole ecosystem is the venture capitalists, especially when it comes to security given the amount of investment that goes in. Is there a responsibility that they have as well? Because as an entrepreneur, if I'm going to a VC and pitching, maybe there's a code of ethics that says, "What's the ethical principle that you are going to adhere to? Before I even look at your proposal." Is that something that should be?

Laura Noren: [00:12:37] Good question. What is the role of the funders? We have already started to see some of the VCs take a look inward and say, "Why don't we have more women? Where are people of color, including women of color, where are these folks? They're not in our midst." That is a good first step. That sense of reflexivity, the sense of taking stock internally first, that's a good first step. That's about as far as I can speak to the VCs as I'm relatively new to this. What I can say is that in academia one of the most important changes when academics are fighting for science to be more open, for scientific findings to be published so they're not behind a paywall. So the data can be shared, so people can try to reproduce the data, can do new studies with the same data and not have to pay the NIH over and over again for the same study because nobody can get access to the old data. The most important change there - and there was a ton of grassroots behind it so that was probably a big, big factor - where you could really see things change, was when the funders started saying to the private foundations, which actually generate very small amount of funding in the academic system, when they started saying, 'We're not going to give you funding unless you agree to publish in open-access journals. I don't care if you can't get into Nature; you can't get our funding. You have to give up on Nature. You have to give up on some of these very prestigious paywall journals, deal with it." Gates Foundation did it. Moore Foundation, Sloan Foundation, a lot of the foundations are going that route, the Welcome Trust in the UK. We saw that become a huge change. So, I would love it and sing Hallelujah in public if the VCs wanted to say, "Let's run everyone through an ethics test, let's see how that works. Let's see how you respond to some of these kinds of tradeoffs that are applicable to your industry, to your specific product."

Ashwin Krishnan: [00:14:34] I think Reid Hoffman and a few others have started this initiative there. They are at least putting together a fund which funds ethically ingrained startups. I think that's a start.

Laura Noren: [00:14:49] It's a start, but let's just say it should be in every product.

Ashwin Krishnan: [00:14:51] It should be.

Laura Noren: [00:14:53] This is not a sideshow, this is domain.

Ashwin Krishnan: [00:14:55] Putting on my vendor hat, which I wore for 20 years, it's at the product definition phase that security can't be just added it has to be built in. The ethics piece is also something that needs to be built in. It's not like you have an incident response team because an ethical event happened. I think some of that is conferences like these, where you failed to find any discussion notes about this. And, as we talked about earlier, thanks to Facebook and Cambridge Analytica, at least on tech and ethics, and supposedly AI and ethics, there is active discussion happening. So there's an awareness. On the security side, I think fighting the bad guys and looking for ways to preserve your solvency seems to be the number one issue. So in some sense, if ethics needs to take a backseat to protect, again back to your discussion about employee's data, is that the right thing? And at some point you look at it and say, "OK I can't even, with all the threats that are looming and GDPR being more of a question mark right now than actually solving anything." How do you balance where ethics fits in the continuum of security, privacy, cost, services, skills shortage? And it's a hard question. I think part of it is, how do you figure that out?

Laura Noren: [00:16:33] One of the nice things about the cybersecurity community is that everybody here is very well aware that you can't just go in and patch a data breach. Once it's happened there's no patch available for that. So that's the same concept that I use when I'm persuading someone to pay attention to ethics. Once you've harmed someone, you can't take it back. You can't unrun over that lady in Arizona and that's that. You can't do that. And you also can't do that to someone's reputation, you can't take it back. If you've de-identified their data to the extent that you can't easily find it, maybe because you're not trying that hard, but someone else can re-identify it, then you can't. You've just admitted you can't get it back. You've got to think about that before you build the product. You're correct, it really doesn't work as a Band-Aid. And you know we're talking about ethics but we haven't truly defined it. For me it's about fairness. And many cybersecurity companies are really excited to talk about machine learning and artificial intelligence. I will not comment on the degree to which they've fully integrated machine learning and artificial intelligence, so let's just accept that they are trying to do such a thing. You really have a lot of fairness questions about that kind of process. It's all data or human first, and humans are biased and we have a long history of acting in ways that discriminate against particular groups to the advantage of others. Unless we're actively trying to remedy that we will, at minimum, replicate it and probably amplify it because it turns out those features are predictive. When features are predictive they become amplified in your model.

Ashwin Krishnan: [00:18:28] That raises an interesting question in my mind. Is the amplification of the biases the way this gets to be front-page news? So, humans start looking at devices much more carefully. In some sense it's like I'm going to tell you, "Hey you're biased," and you can say, "What does it mean?" But if you have 10,000 Lauras ae showing up and algorithms that are actually showing you what you look like. Maybe there's...

Laura Noren: [00:19:00] We'll see. I mean, the only social mirror that I can think of — that is essentially what you're talking about, a social mirror to reflect all of our biases back to us like a truth serum — for society is the #MeToo movement ,right now. And I think it's very interesting to watch what's happening to Les Moonves, he's not been asked to step down. The line of discussion that's being followed there is, "I didn't do something as bad as Harvey Weinstein, therefore this isn't so bad as that."' I wish it were as simple as having one's biases or society's biases reflected back and then it changes, but it doesn't change that fast. I mean we were talking about this beforehand, but it takes both the courage to see and the courage to look and also the humility to accept that means we all have a lot of hard, hard work to do. And a lot of us aren't willing to. CBS could get rid of Moonves but then they'd be without this extremely charismatic powerful leader. They could do it, but it would be a lot of hard, hard work.

Ashwin Krishnan: [00:20:14] That brings up the question about crisis, right. So a lot of the GDPR naysayers are the people who are dragging their feet. They're saying there's going to be a scapegoat, there's going to be somebody who's going to be fined 4% or 20 million euros or whatever else there is and then people fall in line. So, is there something similar to Facebook/Cambridge Analytica that's going to happen to the security world, where there is an ethical boundary that gets exposed or breached and is that then going to get people to... I mean do we need a crisis for something like this to get momentum?

Laura Noren: [00:20:53] There will be such a thing, I think, because employee data, which is largely the currency of cybersecurity, because that legally is just in a very different state than user data or customer data at the moment. We're behind in terms of this. Can we please see this as an opportunity to get ahead? But at the moment we're not seeing it that way. Well, not all of us are. I am. Before I joined Obsidian, I was doing job interviews. I went around to a lot of companies, and you actually get kind of an open kimono when you do job interviews. They're trying to explain to you exactly what they do. And I spoke to one company that I won't name, but it was being asked by its customers if they could please start to predict things like sexual harassment. Could you please predict when that might happen? And you know, it's not really like a forensic investigation. Did it happen? We have a report. Now follow up on that. Instead it's could you predict when it might happen? And I objected to that use of the technology because you can't really do something like that if you have questionable accuracy. But you also can't really do something like that if you have no particular intervention that is sensible for that. So, you think that Jane might harass Aleesha, what are you going to do about that? If you have no particular intervention that's tied very closely to exactly the kind of data you have and the kind of prediction you're making, you risk stigmatizing someone who has done nothing wrong. And that person may actually be the putative victim in this case. It just doubles down; either way it's not a good situation. So I have a feeling, because I know there are companies out there asking for that and there are companies out there who'll provide that, and that will be our employee-data moment. Like, 'Wait, how much do you know about me?' Because employees generally don't have much...I mean the current research I'm working on is to try to find out how much are employees aware of what their employers know about them. What kind of data do you think your employer has? No one in this industry has any kind of motivation to ask that question. So, surprise, surprise, there isn't a study out there like that, but we're looking into it.

Ashwin Krishnan: [00:23:23] Very, very interesting discussion, like I said, nothing like this throughout my 23 or 24 conversations at Black Hat. Which is again indicative of how important this topic is, yet how underrepresented it is. Any last takeaways for vendors? Any pieces of advice that you want to leave them with?

Laura Noren: [00:23:52] I would just say being ethical about employee data is not a space that you want to miss out on. All of us can do it and we can still differentiate our products in other ways. You don't want to be on the wrong side of history here.

Ashwin Krishnan: [00:24:08] Very very interesting discussion, thanks for your time.

Main topics:
02:11 How to start the ‘ethics in cybersecurity’ conversation
07:41 How can a community figure out what is appropriate use of technology?
08:52 Professional ethics do matter
10:32 Project Maven and the power of ethical objection
12:37 Should product ethics be tied to VC funding?
14:55 Build ethics into products—before the problems happen

19:00 Ethics is hard, hard work

20:14 What will be CyberSecurity's crisis moment?