uberknowledge

Aaron Turner, CEO of Hotshot

GDPR: A New Ally for CISOs

Aaron Turner is an industry veteran and CEO of Hotshot. Here you can hear him talk about:

02:55 How it feels to be a victim of GDPR
07:07 GDPR (when properly interpreted) - means fewest eyeballs
08:13 Zero-trust architecture
12:15 Cloud has seen speed to deployment and efficiency, but not a great focus on security
13:50 How do companies get up to speed on security in the cloud?
16:18 The evolutionary question for vendors
17:47 Controlling your collaboration destiny will give you the flexibility to make decisions
19:55 Don't trust anybody but yourself

Ashwin Krishnan: [00:00:01] So, thanks for joining the UberKnowledge podcast. Today I have Aaron Turner, the CEO of Hotshot, with me. That's an amazing name! So, if I call you the hotshot CEO of the Hotshot company that will not be too far off. So, without further ado, I'll turn it over to Aaron to give a brief introduction of himself, and then we'll get into the topic du jour, GDPR. Aaron, all yours.

Aaron Turner: [00:00:33] Thanks Ashwin, for having me on your podcast. A little bit of background about myself: I've been doing security and technology development for over 20 years now. I cut my teeth on some really tough security problems when I worked at Microsoft in the late 90s and early 2000s helping to improve the Windows systems and Microsoft's enterprise server platforms from a

security perspective. Later the U.S. government invited me to join a research project to look into the computer vulnerabilities that exist in the electrical power grid, cell phone networks, and other critical infrastructure. In 2008, I started a mobile payments company and ran that for two years. That technology was later acquired by some major players in the mobile payments industry. In 2015, I sold a company called Terreo to VeriFone. It was a credit-card-skimmer detection platform, helping merchants avoid the problems of credit card skimmers in unattended terminals like ATMs and gas pumps. And then last year I left VeriFone and started Hotshot, which is my latest security technology venture. It basically is the convergence of the last 20 years of my life, where I am taking security applying it to collaboration, but also overlaying it with some interesting policy capabilities to help businesses solve the toughest security, privacy, and policy challenges. I'm really glad to be here on the podcast with you.

Ashwin Krishnan: [00:01:56] That's a great segue, tougher security policy and compliance leads me to GDPR. It's been three months and counting since probably the most sweeping cybersecurity regulation went into effect, passed by the EU. You've obviously been at the frontlines for this, I know you were at a conference in Europe very recently. Where do you think the maturity level is when it comes to organizations, besides just feeling the pain of "Hey, what's the impact of a 4% global revenue fine or 20 million euros going to be?" There's all this hype about what could go bad, but are you also seeing a heightened sense of awareness of how GDPR can actually help you be more competitive and not just compliant?

Aaron Turner: [00:02:55] So, I have some firsthand experience of how GDPR can negatively impact a company. I was at VeriFone commercializing my credit-card-skimming platform and preparing to release the platform into Europe. The credit-card-skimming detection platform would take unique MAC addresses off of devices in an area and look at them. As we went to go deploy that in Europe, some of our privacy and policy attorneys that were working for us at VeriFone notified me that elements of GDPR would make it very difficult for us to do the monitoring that we needed to for detecting credit card scammers in Europe. It

made me take a step back and say, "Well, wait a second. GDPR supposed to be about privacy, are you telling me that GDPR is protecting criminals' privacy? Criminals who inject credit card scammers into ATMs?" and they said, "Yep, unfortunately any European resident is protected by GDPR; they have a right to privacy." And so, it's been almost two years now since I had that first conversation with some EU-based attorneys about this, and it actually put a big speed bump in my deployment plans for my project at VeriFone. We had to make some significant changes to our strategies and so I was sort of the victim of GDPR. We actually had to shelve some of our technologies because of the privacy constraints.

[00:04:12] Now I've left VeriFone, and I've basically been taking a look at how GDPR can help us. Now that we have a better excuse to invest in higher-grade technologies, how can we do that? In the security world the CISOs are fighting for security principles, but oftentimes they don't have an ally at the senior executive level to help them make good decisions about the relative integrity of technology that they're purchasing and using. So, the nice thing about GDPR is it now gives the CISO an ally. Now the chief privacy officer or the data protection officer has the ability to come in and say, "Look we need to make better technology decisions. Let's improve our infrastructure so that we can comply." So, I think it's a net benefit, but it's going to cause some disruption. And in the interim, what's happening is there are so few people who are properly trained, so few attorneys who know how to interpret the law, so few technology companies that are prepared to respond appropriately, that I think we're kind of in the whirlwind right now of a lot of marketing hype, not very good guidance, and then with the overlay of just analysis paralysis for a lot of people because they just don't know what to do.

Ashwin Krishnan: [00:05:28] That's a really good observation. What you mentioned about marketing hype, any self-respecting or not so self-respecting vendor out there has to have some material in GDPR, right? And clearly the catchy phrase, "The right to be forgotten," is something that most people use without having any real understanding of what it means. But what you

mentioned about the uniformity of applicability of GDPR means that a consumer and a scammer are equivalent. That's a really interesting observation because I didn't realize that the applicability of that law is regardless of the intent or malintent.

Aaron Turner: [00:06:13] Exactly.

Ashwin Krishnan: [00:06:14] That's really interesting. I think the other piece of that is when you talk about analysis paralysis. So, let's break that down into bite-sized chunks. You talk a lot about data encryption. What's the way to help the CIO and CISOs and chief privacy officers? They have to deal with the implication of something going wrong and clearly that puts all kinds of conspiracy theories in their heads. But if you, Aaron as the CEO of Hotshot, were to look at their situation what would be your recommendation? Would you say, "This is the basic stuff that you should be doing, regardless of whether this is GDPR or not, and guess what, by doing that you're actually ten steps ahead towards compliance"?

Aaron Turner: [00:07:07] If you think about it from the implementer's perspective, the easiest way to comply with GDPR is to make sure there are the fewest set of eyeballs possible that can ever see data relating to a European Union resident. If you can constrain that scope, at that point you don't have to implement a ton of controls. Let's take the typical collaboration tool, which is Outlook plus Hosted Exchange or Exchange Online, and the way people are working through the daily course of business, and then a whole bunch of documents that are stored up on Onedrive, Dropbox, Box, or whatever data storage solution they're using. By using those typical enterprise-class collaboration tools, they're subjecting themselves to a very long supply chain of everyone who has the potential to see that data. So, in the standard configuration of Office 365 that means any Office 365 administrator can look at the data. Anyone along that supply chain can look at the data and it creates a very long tail for how you can actually comply and reduce the scope there. And so, the approach that we've taken at Hotshot is to move to a zero-trust architecture, where essentially the only individuals who

have access to the data are the authorized individuals at the end point. There is no back-end data that can be viewed by system administrators, untrustworthy technology companies, or anyone that's sitting along the end-to-end path of that data flowing from one device to another. At Hotshot we believe that controlling the scope and limiting potential eyeballs will help resolve a lot of the headaches. We can say, "Look, we won't have to worry about compliance on those back-end servers because there is no back-end data to look at."

Ashwin Krishnan: [00:08:52] Got it. As you were speaking, I was about to ask you the question on zero trust, but you already brought it up. Clearly that seems to be becoming much more mainstream. John Kindervag, ex-analyst at Forrester and now at Palo Alto Networks, coined the term zero trust, and the assumption of that zero-trust model is obviously much more mainstream among the security companies.

[00:09:18] But let's switch gears a little bit and start talking about cloud and the journey towards cloud. Is that intersection allowing for better protection or, as you mentioned earlier, is there a collision of priorities or philosophical mandate, if you will? You have that ability for people in the DevOps team, for instance, who are all about creating instances and turning it off and turning it down in a jiffy; continuous integration, continuous development, trying out new cloud-made tools that are available, like serverless computing or Lambda, about something like that. On the flip side is zero trust, which is really locking stuff down. In the journey towards the cloud, predominantly people go there for agility, efficiency, and cost reasons but not so much for security. Do you see, maybe a "collision course" is too strong a term, but do you see two different mindsets when it comes to going to the cloud? Where there is a fear mindset of "out of sight, out of mind" and everything you mentioned earlier about visibility, transparency, and reducing the nuclear radius, versus the other mindset of Dev Ops or the lines of businesses who really are going there for efficiency reasons.

Aaron Turner: [00:10:52] I think there is a way to enjoy the efficiencies of rapid deployment and low cost of ownership that cloud represents. We've achieved

that with Hotshot; we're still essentially a zero-IT deployment system. There are no servers to install, there's no need to have operating staff making sure that things are running, all you have to do is install the Hotshot app, and you can enjoy end-to-end encrypted collaboration with very powerful policy enforcement tools. We think that we've achieved the benefits of cloud, but the way that we've achieved it is through assuring that we never have access to the encryption keys. Hotshot never has visibility into the encryption keys that control the data from one end point to another. The benefit that gives our customers is even if I get a legal request asking, "What is this person talking about?" all I can do is shrug my shoulders and say, "I don't know, I have no idea what they're talking about. Would you like me to stop them talking? I'd be more than happy to shut them off, but I don't know what they're talking about." Basically, that's the approach we've taken because any time that you bestow trust on an organization, on a group of administrators, there is the potential that the data that you're sharing back and forth can be abused and accessed without your authority or authorization.

[00:12:15] When you take a look at traditional cloud computing there's stuff like you were mentioning, AWS, the Google Cloud Platform, Azure and that sort of thing. There has been a lot of focus on speed to deployment and efficiency, not a great focus on security, but we believe that you can achieve that. And one of the things that I find ironic about the zero-trust situation is one of the greatest promoters in the ecosystem around zero trust is Google with their BeyondCorp initiative and the documents they published with vendors, like Yubikey and others, and what is ironic about that is Google is the king of the surveillance capitalism ecosystem. Here they are promoting zero trust, but at the same time they're monetizing every bit of data they can get about you. It's just an interesting thing that we're seeing right now, and that discord, that dissonance is going to have to be resolved at some point.

[00:13:09] You take a look at technologies like Slack, they just released an article this morning saying, "Hey, you know what, end-to-end encryption is not important." And I literally had to laugh a little. Well, you're right, Slack, because

you're trying to monetize all of your users' data. So, you're right, it's not important because in the Slack business model you need to have access to that data. It's just one of those things where you take a look at the situation and those organizations that truly care about the integrity of their data are going to have to start migrating towards things like Hotshot to enjoy the benefits of the end-to-end security without the potential for untrustworthy technology company administrators and others to have access to the data.

Ashwin Krishnan: [00:13:50] I have to read that article on Slack because it's making my blood pressure go up! You mentioned Hotshot, as a company, does not have access to customers' keys, so therefore you remain in that zone of not being able to monetize a customer's data. But you have an unfair advantage between your experience, between Srini's experience, and the collection of individuals at the company. I mean you are a top of the pyramid technology company who knows how to use cloud effectively. 99.9% of companies don't have that expertise. So where do they go to even get the basic understanding? How much data am I collecting? Why am I collecting the data? What's the most important one? Where is my PII data stored? How much primary, secondary backup do I have? Is it encrypted? Where are the keys stored? How does a company, which literally can sign up to cloud in a matter of seconds, even come up to speed with what does security really mean?

Aaron Turner: [00:15:00] From Hotshot's perspective, the way we view it is that you start with the day-to-day collaboration. If you can get your arms around the data that's being created by your knowledge workers, by the people that work for you, that they're focused on servicing your customers. We believe that's the first best step. Now it's not the only step, as you mentioned. You've got all of these data stores, large back-end data sets and that sort of thing. At Hotshot we're mainly focused on secure collaboration and making sure that you have that in your policy. But because of our experience, we have had several large global enterprises, name brands that you would recognize, ask us, "Can you help us?". We're in that process of trying to lend our expertise to them so that they can use the power of Hotshot, but also leverage our expertise to solve

some of their bigger problems about the back-end data authorization relative to GDPR, labor law compliance, and that sort of thing. We, at Hotshot, perceive ourselves as something that's offering an immediate solution for near-term pain relative to collaboration information, helping get your arms around that. But long term we want to be a partner with enterprises to help them solve those bigger problems. We're actively looking for pilot customers that we can start trying out some of these new policy enforcement mechanisms for that back-end data.

Ashwin Krishnan: [00:16:18] I guess that leads to a really evolutionary question for vendors. You come in, you're talking about collaboration and solving that first order of business, but then you mention becoming a consultant, becoming a partner in the journey that your customers are going through. How many companies out there have the knowledge, the inclination, and the staying power to be able to really engage with their customers? To be honest, I was on the vendor side for about 20 years and we used the phrase, "Walking in the customer's shoes." But to truly walk in the customer's shoes you have to understand where your customer is, where they've come from, and where they're going. That takes a lot of attention away from building the right product or trying to get to the next valuation round, and so on and so forth. Is it time to rethink what walking in the customer's shoes really means and make it more of an existential thing? Know that you can't have a road map or a strategy discussion with your customer unless you truly understand where they're coming from and where they're headed. And know that maybe you don't have a business opportunity today, but you are able to truly get to that point of dialogue where it's less about selling and more about understanding and seeing where the fit may or may not be.

Aaron Turner: [00:17:47] So you know, we're obviously biased, right? We're a startup, we're trying to get our foot in the door as many places as we can. At the same time though, we're bringing to bear a couple of decades of our own experience on how things have gone wrong. My background working on security teams — not just from security technology development, but also from

time to time with government agencies to actually undo security for the sake of monitoring — means I've seen the security angle from both sides: trying to build it from a technology perspective and trying to break it from a government surveillance perspective. What I'm trying to bring to bear is that experience to say, "Look, get yourself in a situation where you control your own destiny. By controlling your own destiny, now you have the flexibility to make decisions you didn't have before." And that's what we're trying to do with Hotshot, give people control of their collaboration destiny so that they have the ability to make the decision. Make sure they're not backed into a corner, forced to make a decision because someone else has put them in a bad situation. It's about giving people control and letting them take advantage of that. We think that's the best way forward, to make sure that they can take best advantage of our platform.

Ashwin Krishnan: [00:19:05] I completely agree with you. I think education goes hand in hand with control, for them to totally understand what control really means. You've had experience on both sides in building secure communication for enterprise and consumers. At the same time Big Brother is watching and being able to do stuff for the government so they can actually protect nations.

[00:19:28] This is a great conversation. Any final takeaways that you have for people pulling their hair out, whether it's over GDPR or whether it's over cloud? What would be the two to three things that you would consider the first step — and that's universal, regardless of region, regardless of expertise — before they embark upon these journeys?

Aaron Turner: [00:19:55] I think the first step for any company is to take a step back and don't trust anybody but yourself. Take a look at all of the different vendor relationships you have relative to data flows and where data is being stored and how data is being processed. Take a step back and think, "Can I trust those people? Can those people really be held accountable? If I have an incident, and I've got to make a disclosure to the European Union, are they going to be my friends in this?" Our first response is trust yourself. Reduce the

number of dependencies you have on your data lifecycle. Secondly, we believe that in the future, as GDPR enforcement becomes more mature, you're going to see a lot of cross-border data-transfer situations, where you're going to have to put location-based restrictions on where data is accessed from. That's where our geo-location capability and policy enforcement comes in. Then thirdly, from a compliance perspective we're starting to see more and more situations where labor laws are being enforced to say people have the right to disconnect. That means you've got to be cognizant of when people have access to the data. We're trying create that triumvirate of high-security, location-based encryption, time-based encryption so that you are in a super-compliant spot. We're looking to create opportunities for people to extend our capabilities into the greater enterprise to help them solve these hard problems. That's really what we're trying to do. Hotshot is trying to bring this innovative technology to market in a way that solves deeper problems in a way that they haven't seen before. And all at a level of simplicity that they can get set up and running in a matter of hours.

Ashwin Krishnan: [00:21:41] I was about to get to that one. It has to be simple because if it becomes complex, 10 clicks instead of one, people are going to walk away.

Aaron Turner: [00:21:51] Exactly, people don't have the attention span anymore. It's simply, effectively, securely, and within the policy constraints. We're stacking all of these requirements for the poor IT teams, and our approach is, "Hey, let us help you solve that problem in a way where you retain control but can do it simply, effectively, and with simple policy enforcement mechanisms."

Ashwin Krishnan: [00:22:11] Very good. Great conversation. Thanks for being on the podcast, Aaron. I'm looking forward to seeing continued success for you and your team.

Aaron Turner: [00:22:19] Awesome. Thank you, Ashwin.