uberknowledge

Jon Callas, Sr Technology Fellow, ACLU

Title

Encryption, Business's Moral Dilemma, and Diversity

Rubric: Jon Callas talks about his long and illustrious career, offers unusual advice on how to address the diversity and the skills gap, discusses the advantages of encryption, and is positive about the protection of privacy, believing the future lies in proper policy, regulation, legislation, and consumer activism.

01:09	Jon's long and illustrious career in four minutes.
06:44	Privacy isn't doomed. The future lies in proper policy, regulation, legislation, and consumer activism.
09:44	We are seeing consumers take action to safeguard their data, and Apple made a good start on that with transparency, consent, and control in iOS.
11:14	We need tools we can set in our devices to monitor our usage and therefore gauge our dependency
13:35	We are moving to a world where SSL and encryption will be the default but this poses moral questions for business.
15:10	Encryption makes it easy to dispose of digital waste. Encryption enables recycling
19:05	Companies need to set their own moral compass or outside influences will do it for them.
23:28	Tech was an incredibly diverse field, it can be again, if companies stop looking for staff in the obvious places.

ADD 37 Ashwin Krishnan: [00:00:38] So with me, I have Jon Callas. I need to quote what Wikipedia says about you, "One of the most respected and well-known names in the mobile security industry." And I just educated Jon because he hasn't gone to Wikipedia in a while. So Jon Callas, who, all kidding aside, has done more for the security industry than most other people have, I want you to just walk the listeners through your journey and specifically where you are today.

Jon Callas: [00:01:10] All right. So today I am senior technology fellow at the ACLU. I work on the Speech, Privacy and Technology project. And a lot of what I do is helping lawyers with cases that they are working on. In some cases, it is being a research librarian, some cases it is being someone to come up with positions and analyze what we are doing and also to be an advocate for positions that we are taking on technology and policy.

Ashwin Krishnan: [00:01:43] And your illustrious background, which is obviously good, starting with everything and through PGP as well?

Jon Callas: [00:01:48] Ok. Well, I started off many years ago at Digital Equipment Corporation, and I worked on the VMS operating system for about 10 years. I worked deep in the kernel. I also did user experience. So I started off doing user experience fonts, other things. I got tired of putting bits on screens, so I went into memory management and schedulers and other things like that.

[00:02:18] I got into doing collaboration tools after that happened with DEC and created an online meeting system that we called meeting space and that startup got rave reviews and we sold tens and tens of copies of it ...

Ashwin Krishnan: [00:02:38] [Laughs]

Jon Callas: [00:02:41] The world was not ready for it. But Apple saw it and hired me and moved me from New England to California to work in their research group at the time. I got into cryptography because of doing collaboration tools that people said, "Oh, I don't want to collaborate on the internet, unless people have something, they can do with it, anybody could sniff my traffic." Well, there was no SSL in those days. So I went to the second RSA conference ever with an eye towards, I need to start encrypting traffic on the internet, how do I do that? And as time went on, I found these security things more and more interesting and stayed with that rather than the collaboration tools.

[00:03:38] Then PGP formed, and I came in as a server architect. I wrote a lot of part of the first key server that they had. I became chief scientist, and when PGP was sold to what is now McAfee, what was Network Associates then, I stayed there for a while. I went to go work for Bruce Schneier at Counterpane, worked for Taher Elgamal at his Securify company, worked for Wave Systems on their secure microprocessor. And then in 2002, a team of us, including Phil Dunkleberger, started up PGP again. We bought the assets and started up the company and went for what we were calling then zero-click encryption, that was our name for it.

Ashwin Krishnan: [00:04:36] Zero-click encryption, wow.

Jon Callas: [00:04:38] It was ... the correct way to do the user experience is essentially don't have any. No decisions, no nothing, we are just going to protect things. And

that was pretty much the way that we did things. It was a philosophy that carried into our doing full disk encryption and other tools where the idea was that you shouldn't have to think about it. It should be managed by policy. You might sit down and say, "What should my policy be?" but once you save, it just works. You don't have to think about it again. And similarly, in an enterprise the security people can decide what the policy is for the company and it just happens. I used to say my robot servants handle all my crypto for me.

[00:05:28] So after PGP was sold to Symantec, I ended up at Apple. I worked on firewall too there. I became CTO at Endtrust, formed Silent Circle and Blackphone. After that went out, I went back to Apple, and now I'm here at the ACLU.

Ashwin Krishnan: [00:05:47] OK. I should say that this is the longest ever intro out of any podcast.

Jon Callas: [00:05:52] [Laughing] You're going to cut it or you could you could have me rerecord it.

Ashwin Krishnan: [00:05:55] No, no, this is important because I think part of the conversation is also about the fact you have seen so much of the evolution of the security industry. The part I want to get to next is how has your, Jon's, views of privacy and encryption evolved over so many projects, so many companies, and where do you stand today? I had the privilege of listening to you talk at the CSA summit earlier today. For the listeners who weren't there, you talked about privacy in a manner that I have not seen being talked about before. So just talk about how awareness is rising both in consumers as well as surveillance states, and what kind of world are we getting ourselves into?

"I believe that we need to make changes based upon policy, regulations, law, custom."

Jon Callas: [00:06:44] Well, the talk that Jim Reavis gave me for the title was, privacy: is it pretty good or is it futile? And I said, it's neither. It's really easy to look at anything that is in the news and say, "Oh, my God, privacy is doomed, da de da de da."

[00:07:02] But there are a lot of things that are bright spots. There is progress that is being made. And it also ties into what I have been doing with my own career, which is that I believe that we need to make changes based upon policy, regulations, law, custom. Because, you know, policy doesn't have to have the force of law behind it. If we all kind of agree, this is the way a company will work, and we will not buy their stuff if they don't act a certain way. Things have gotten bad enough that we definitely want to change things. And you can see this in GDPR. You can see it in the California privacy laws. You can see it in things like the Illinois biometric privacy laws, where people are sufficiently concerned about the misuse of these really cool technologies that they're putting restrictions in place for things. And I think that is what's going to happen. We aren't going to be able to do what we could 20 years ago, which would say, "I have a really good idea for a thing I can build, and I'm just going to go build it."

Ashwin Krishnan: [00:08:15] So one of the things you mentioned is that awareness is rising, which is good. But at the same time, I'm hazarding — I might be off — but I'm

just guessing, an average person has somewhere between 35-40 apps on their smartphone.

Jon Callas: [00:08:31] Wouldn't surprise me.

Ashwin Krishnan: [00:08:32] So, let's go with that number. To truly understand which one has biometrics turned on, which one has location services turned on, which one is actually connecting back to Facebook SDKs is impossible. So when we talk about awareness, I mean, how do you see consumers as well as vendors take the fact that they have a highly distracted consumer, who is spending less and less attention to … Simple example, I actually go through all my apps every month and things that I have not used over the past month, I just delete them. It seems simple, but it's, "Man, I've got to spend five minutes going through my apps," Never mind, my wife's, my daughter's. It does take an act of absolutely needing to fortify myself to go through that. But it seems like a simple thing.

Jon Callas: [00:09:29] Yes.

Ashwin Krishnan: [00:09:29] So in your mind, yes, awareness is rising; yes, as you look at the Marriott breach or you look at the latest Facebook snafu, people are getting wiser, but is that translating into action?

Jon Callas: [00:09:44] It is translating into action, because you see people saying, "I don't want to do this stuff anymore." You can see things that are going on the devices themselves. At Apple, the phrases that we used, we talked about transparency, consent, and control. And you can see that in iOS, on your iPhone or your iPad, that everything that is there is always pulled up front. Here's what it is that you want to do. You can always go see who has it, and you can always change your mind later. And that is an incredibly good start for how you manage these things.

"We talked about transparency, consent, and control."

[00:10:30] There's also, I think so far inadequately done, automated versions of what you are talking about. There is a way that you can have apps essentially offload themselves. There's a little cloud icon that appears on them. So they don't actually go away, but it would be really cool if things got extended to, you know, archive it, put it away, let me look at it somewhere else, automatically. And I could say something like, if I haven't used this thing in six months, just get rid of it. I know that there are, in fact, games I have not played literally in years, and yet I cannot bear to delete them.

Ashwin Krishnan: [00:11:13] But that's a choice you make.

Jon Callas: [00:11:14] Yes. And I think that extending the idea of transparency, consent and control, doing things like what was done for screen time, where you can see what you are doing, what you're tracking, because if you can be aware of what you're doing, you can manage it better. I think that screen addiction and other things is just a moral panic. You know, there were times when we had similar sorts of things about people reading books, and people playing video games, and people listening to music, and this, that, the other thing. This is our generation's version of, "Oh my God, what are we doing with ourselves?" And, you know, the tools to do it can either let

you know that you're doing something that you didn't want to or you could say, "OK, I can live with this." I think that sort of transparency, that sort of informing people of what's going on is exactly what is needed because this way we can have a rational discussion about it. If I don't know how often I do these things, then I can't talk about it.

Ashwin Krishnan: [00:12:32] Yeah. You make a really good point, in fact. GDPR is probably going to be used, I don't know, a million times in these four days at RSA, which is actually a good thing because it's raised awareness.

[00:12:43] But I want to come back to encryption because it seems that it's become the de facto go-to place for everybody right now. Figure out where your data is, and make sure it's encrypted, and make sure you understand who owns the keys. Is there more burden being put on encryption than there ever has been in its history, especially data at rest? With data in transit, we've talked about SSL, we've talked about other sorts of VPNs.

Jon Callas: [00:13:15] So **the good thing is that we are pushing as a world that SSL will be the default**. And you can see that the browsers are starting to move towards rather than saying, here's a gold star for going to an SSL site, they're putting a big red X off, if you're not. The idea that they are actively working to say, **normal is encrypted, not encrypted is abnormal** is part of our changing view of the world.

> "Normal is encrypted, not encrypted is abnormal is part of our changing view of the world."

Ashwin Krishnan: [00:13:46] So let's assume that in transit, everything is going to be encrypted or everything will be at some point in future, how does this now play into the surveillance state? You kind of get into this notion of moral decisions that companies have to make. I'm thinking Google and Project Maven or Microsoft with the DoD. So, what's Jon's opinion about a vendor both wanting encryption tools for consumers and businesses as well as providing snooping tools, like in the case of Apple and San Bernardino, then taking a stance? Are we also getting into this stage where companies need to have a moral stand, which is going to be tested? And if so, we don't have any blueprint for that. I mean, Apple did not turn into this this highly upright moral corporate citizen overnight.

Jon Callas: [00:14:44] That's correct.

Ashwin Krishnan: [00:14:44] We've seen opposite of that with Facebook and Mark Zuckerberg; where everything coming out of his mouth, people are second guessing because it gets disproven the next day. So, I mean, how do you see this evolve? What's your opinion on how companies get tested? We don't want them to get tested with your data and my data.

Jon Callas: [00:15:01] Right.

Ashwin Krishnan: [00:15:02] So is there a playing ground, so you can actually test where they stand and then, ultimately, what's right and what's wrong?

Jon Callas: [00:15:10] Ok, unpacking that really quickly. For data at rest, one of the major advantages that encrypting has is data then becomes easy to get rid of. That, for example, with your laptop right there, I'm presuming that you have encrypted the disk because it's on by default now. And if you wanted to sell that, all you really need to do is the equivalent of reformat your disk. And now all of the data is gone in the sense that they would have to have the right keys to do it. And the next person who gets that laptop has a disk that they can't read and they just put their stuff on it. And this is really, really useful for us to be able to get rid of, essentially, the digital waste that we would put around, which would impede our ability to recycle and reuse things. So that, ironically, is the most important thing to do with encryption. And this is also why disks that are in data centers are encrypted by hardware or software, because if the disk is encrypted, you can just throw it away. Yet you don't you don't have to say, "Oh, my God, what was on this thing? What do I do?" You delete the keys and the stuff's gone.

[00:16:31] So going forward then, remind me of the next part of the question.

Ashwin Krishnan: [00:16:37] The next part of the question was as a vendor, like let's say I'm creating the software that allows zero-click encryption, but I could also be creating tools for data and transit as an example for NSA or the Chinese government, whatever civilian state of choice, to be able to crack it open. Is there a moral stance that a company needs to now have because they're going to be faced with this dilemma? I mean, is Satya doing the right thing by saying Microsoft will continue to sell to DoD, even though some Microsoft employees are waging war against that?

[00:17:21] Or in the case of Google, they caved in saying, we're not going to be supplying Google's technology to Project Maven, I think starting next year or something like that. So, we've already seen two marquee companies being faced with this dilemma of what's right and what's wrong, and how does somebody come to terms with that? How does an organization come to terms with that, and how does an employee then, either for or against?

Jon Callas: [00:18:22] I think it's really good that this is happening, that we are having the discussions, and **I laud the companies for taking their people seriously**. Whatever decision gets made, it's obvious that, for example, neither Microsoft nor Google has basically said we're doing this my way or the highway. Even in analysis and explanations, he's being incredibly respectful to the other point of view, even though that's not what he's going to do. So kudos to everybody for that because this is a discussion that we need to have. Companies need to decide what their business is in and what it is that they are going to do.

"I laud the companies for taking their people seriously."

[00:18:37] A long time ago, when I worked at DEC, for example, there were lines where the company said, we won't do this. For example, they said we will not work on things that actively put someone's life in danger. We won't work on nuclear or anything. And there were some lines that were made over, this is something that we're just going to forego.

[00:19:05] The company deciding who it is, what it is, and what it believes in is really important because if you don't decide it, it will happen. And the worst thing that can happen for an executive is to wake up and discover that your company is not the company that you really want to be in charge of. And then you have to go figure out how to get out of that mess. If you already have a contract, you need to say, I'm going to wind this down and I'm not going to do this anymore.

[00:19:38] When I was at Entrust, I was brought in because I was an outsider and contrarian to say, how do we go forward? I said things like, cross certification of CAs was not a good idea because you want to understand who is responsible for what, and you don't want to blur that. So there was a policy that the company put in place to wind down everything else immediately. They said, we will not make any new of these. And then a little bit later, they said we will not renew any of the existing ones. And a couple of them, they flat out said, we don't believe that this is good for us and went and negotiated breaking the old contract. So that was the company deciding that I don't want to be in the business that I am in. I don't believe that's the correct thing for us to do.

Ashwin Krishnan: [00:20:39] So those are great examples of organizations standing up.

Jon Callas: [00:20:42] Any of these is OK. Merely saying something like, "I'm never gonna make a deal like this again. I'm going to let these go out," and then deciding who you would continue with within an existing relationship is a good place to start. It's a really good thing to do.

Ashwin Krishnan: [00:21:03] So, changing focus, I know you mentioned Bruce Schneier. Obviously, you're here. Phil from Nok Nok Labs is going to be here tomorrow. So there are people like you, who've been in the security industry for a long, long time. And finally this year, RSA is taking diversity as a big focus for inclusivity and diversity. In your mind, and I'm broadening the scope of diversity, not just based on gender, but also based on demographics.

Jon Callas: [00:21:36] Yes.

Ashwin Krishnan: [00:21:37] How does inclusiveness play a part as we move forward? Whether it is women, whether it is kids who have other choices they can make, why and how does security become ... Because we keep hearing about the skills gap, we keep hearing about data bias and algorithmic bias and all that. Now, it's no longer just a question of we need to have women because they need to feel the security industry is welcoming of them. It's also going to be existential. So in your opinion, what more can the industry do to be more welcoming, be more forthcoming, to be more inclusive and empowering of both kids as well as women, as a starting point?

"The most productive thing is to broaden your scope … and to look in new places."

Jon Callas: [00:22:22] When I have worked with groups that have wanted to increase diversity, the thing that we have looked at as the most productive thing is to broaden your scope of where you are looking for new people and to look in new places.

Because if you take the top 10 universities in the world, and you say, oh, I want to hire from these, you are going to end up statistically hiring the people who resemble the student populations of those. So you need to go out, and you need to go find these things. You need to break the catch 22 problem of I'm not sure that the right students are there. Oh, come on, there are good students there. You need to decide that your requirements and the sort of people that you want are not based upon what courses that they took.

[00:23:28] When I started my career, tech was one of the most diverse places that there was in all of industry. And from the mid-80s on, it declined from there. And I think it was because there weren't many certifications. You got to where you were through being interested and, essentially, on-the-job skills. Those of us who were in the business, we're all people who had gotten there because we were out of the ordinary, and we had fallen into where we were. We liked this stuff; we thought it was interesting, but we fell out of the margins to go do it. And many, many people had interesting backgrounds. I mean, you know, my degree is in pure math with philosophy and English literature. And, you know, the answer to what do you do if you have a philosophy degree is, you were taught to think, you should consider high tech.

Ashwin Krishnan: [00:24:34] But that's true!

Jon Callas: [00:24:34] And you know, I believe that the background that I had in performing arts, in music and speech and acting and other things helped me in tech. One of my coworkers, who was a development manager, went off for fun and he took some courses in improv comedy. And he said that it was an absolutely wonderful thing to learn because there were things like how to keep a straight face when someone tells you something that is absolutely absurd. The idea of you take what you're given, and you say take that and run with it and go more. These are all skills that turn into, you have a meeting, you need to find out what is the next year's plan going to be, and the skills that you would learn for that sort of thing are directly the skills, and they're more important than other things.

"The answer to what do you do if you have a philosophy degree is, you were taught to think, you should consider high tech."

[00:25:33] I find it interesting that many of the craft skills that we have are so available for cheap. There are so many places where you can for anywhere from 20 to 200 dollars, get a course that will teach you how to program in Python or Java script or learn C++ and that you are not having to go to a university to learn these sorts of skills. So why not spend your university time becoming a broader person, learning to do these other skills that when you have a job, how you program is the least of it? And on the web, there are plenty of places, LeetCode, etc., where you can go and learn to be a good programmer. You don't have to have that course to be a programmer.

Ashwin Krishnan: [00:26:26] Ok, so that's amazing advice because you're right. I was just thinking about improv comedy and being able to respond to a hostile customer environment, to be able to think on your feet and be able to assess the audience

reaction and be empathetic towards that, are all skills that are grossly understated.

Jon Callas: [00:26:48] And you know, how else are you going to learn them? It's like a lot of the diversity is really going to be going out and looking in the not obvious places and saying, I want to find people who are different than the people that I'm getting, and so I'm going to look in not obvious places.

Ashwin Krishnan: [00:27:09] Very cool. So, one last question before we wrap up. There's been lots of talk about RSA being a vendorfest and nobody worth their salt actually goes there, etc., etc. But it continues to be a place where there are good ideas — I haven't been here half a day and already I've learned so many things. What in your mind is, I mean, having been on the founding team of CSA, which has come ten years, right, how does an organization that … We have just two minutes left; we've talked about people needing to improve and we've talked about how you get your skill set. We've talked about organizations needing to figure out their moral fiber. How do conferences evolve into something that people actually want to go to?

Jon Callas: [00:28:01] This has always been a very good course. I mean, a very good conference, for as I phrased it yesterday, I could not spell CISO, and now I am one. You know, you are a smart person, you've done lots of things, you have been pushed into security, you know how important it is, how do you go and run around and find things that you were not going to find out otherwise? And that sort of training is the sort of thing that RSA conference does very well. There is a need for that sort of thing. There are other conferences that are geared towards the specialists in one field or another. And this is a generalists' conference and it serves that purpose. And then when people become an expert, they will then come here for other reasons, like, you know, this is where I see the people that I took those courses with. This is what I do this with. And also, to help bring your own people, who are learning to be something, and having them come here, perhaps guide them with what ought to be good. So that's a good thing for RSA to be doing, and it's got that niche in the world.

"As I phrased it yesterday, I could not spell CISO, and now I am one."

Ashwin Krishnan: [00:29:20] Got it. So it's a beginner's introduction to cybersecurity as well as a place for you to learn from what others have experienced. Very good! So, again, this has been a fascinating conversation. Thank you for your time and hopefully we can connect again in the future.

Jon Callas: [00:29:36] My pleasure. It was fun.

Ashwin Krishnan: [00:29:37] Thanks.