uberknowledge

Eve Maler, VP of Innovation & Emerging Technologies, ForgeRock

The Outsized Role of Privacy and Consent

Eve discusses the security implications of the social sign-in and considers if there is an opportunity for enterprises to provide IoT identity management.

00:57 The outsized role of privacy and consent
03:50 Does business' love affair with the social sign-in ignore the security implications?
08:45 Seamless sign-on or Social sign-in: it's the underlying business model that determines the sensitivity and risk
11:10 Identity must have a multicloud stance because enterprises are multicloud.
13:56 The non-traditional data center mindset suggests we should give everyone a God Key
17:51 The trend for applying identity to services as well as people, devices, sensors, etc.
19:47 Is there an opportunity for enterprises to provide IoT identity management?
23:33 A framework for understanding how to measure control elements of consent and privacy
30:01 The complex interaction between market forces and regulatory forces.

Ashwin Krishnan: [00:00:02] Hello everyone, with me today I have Eve Maler, VP of Innovation and Emerging Technologies at ForgeRock. Eve and I met back at RSA this year, so I'm happy to engage with you again.

Eve Maler: [00:00:14] It's my pleasure.

Ashwin Krishnan: [00:00:15] For those of you who are not familiar with Eve, she has a storied history both in the development of web technologies and more recently getting really in the forefront of identity, permissions, and context. So, we'll spend probably the next 15-20 minutes just talking about how the world of AAA, particularly authentication, authorization has evolved. And, as we go headlong into this cloud transformation, what are some of the things that people don't think about, whether it's consumers or whether it's vendors? So, with that let's talk about AAA and where it has come from and where we're headed.

Eve Maler: [00:00:57] Well, for me, privacy and consent take an outsized role in what the customers that I'm talking to have to deal with. And interestingly, you know we do digital identity around these parts, and a lot of people's attention when they're trying to deploy these systems is consumed with strong authentication, identity records, and their soundness. And as I look back on the last 10, 15, even 20 years of digital identity and access management, I see a lot of successes actually. Things like the federated identity pattern, being able to fling identity information across domains securely and having it be respected by a partner, so that you can achieve things like cross-domain single sign-on. And so, then you ask, "Well, what's next?" and what's next is the harder thing. If authentication is getting solved, you look at authorization. And authorization, access control, permission management has very close ties — although I sometimes think we don't see it that way — with the privacy and consent proposition because consent management is about granting permissions to get access to your stuff. And that's what enterprises do all day long when they're trying to achieve access management. Especially in this kind of BeyondCorp world where many, maybe most, of your sensitive assets don't live with you, don't live in your data center. It's like everything has to be managed in a zero-trust fashion, as our friend, John Kindervag, might say.

Ashwin Krishnan: [00:02:44] Yes. So from an evolution perspective, I know you mentioned cross domain, for me as a consumer — putting on a consumer hat

first — I think it was this morning, I was going to some website, actually SpotHero I think, anyway it said, "Do you want to log in with your credentials or do you want to log in with Facebook or Google?" and it's easy to log in with Facebook or Google, right?

Eve Maler: [00:03:11] It is.

Ashwin Krishnan: [00:03:11] But can you talk a little bit about the impact of the consent I'm giving at this point, saying it's okay to use my so-called web portal's identity to log in to some cross domain third-party site? But the implications of doing that in the event my Facebook credentials get compromised, what does that do to the larger ecosystem? Has enough thought been given to that first portion of just authentication? I know it's easy to do, but what's the broader implication?

Eve Maler: [00:03:50] So, there's a number of implications. And that example of a social sign-in is, in fact, a specific example of the broader, federated identity pattern. So, businesses really tend to like that pattern, where they can use it. You know, banks will tend not to — although a few do — but retailers really like it because it dissolves or makes invisible the onboarding of a new user. That's why they might have what identity people will affectionately, or maybe not so affectionately, call the NASCAR login. Meaning your onboarding experience just gives you — it's sort of festooned with logos like a NASCAR driver's car.

Ashwin Krishnan: [00:04:32] You're zooming away!

Eve Maler: [00:04:35] You're given all these logos and it means that it's a button press to log in. So logging in and onboarding or registering for an account look like the same flow. What this really means under the covers is that company, whatever it is, and I've got a few of those logins myself — it means I only have the one password to manage for many logins — the business likes it because they don't have to store that credential, they don't have to store the secret or whatever it is. Facebook likes it because they not only get the visibility on who

you're logging into, but that data on you is being shared, and the business really likes it as well. In fact, they're kind of a consumer of Facebook's business or Google's business or whoever, based on what attributes are available to be shared. You know some of those identity providers, social identity providers, IDPs, only have certain attributes available, and so those are the only ones that are viable for that business to even survive. So, in practice, your sharing of that knowledge from Facebook or wherever is now available to potentially many businesses.

[00:05:47] So, some implications from an authentication standpoint. If your account that you use to log in gets compromised, you'd think, "Well, OK there's nothing to be done. Now they're all compromised." In fact, there are standards that have been developed. There's a standard called RISC developed to enable the original IDP, whichever it is, to out of band of your having logged in, alert all those other relying parties that there's something funny going on with your account. They call it a shared-signals model, which is rather quite clever. So, there's a couple of things going on there to ensure protection, given that there's one credential and multiple users of it; on the consumption of your identity records side. In terms of what you're authorizing to be shared, well, this is a way that we see the challenges with what looked like data breaches in the news, but it's really a discretionary business model choice that businesses are making. Both the IDP side, let's say Facebook or Google, and those third-party apps. That's the flow that's going on — the sharing of data by you having consented. That's what happens when you press authorize versus deny. And it's setting up a pipe to share that data afresh every time that you choose to log into that.

Ashwin Krishnan: [00:07:21] This is very illuminating for me, I'm sure, hopefully, for the audience as well, but part of it is the permission that you're granting, for these third parties to use your Facebook or Google credentials, in a sense also means that the trust level that you have with these hub entities is much larger. So, like you're saying, these smaller entities, which now don't have to store credentials, maybe this is actually a good thing.

Eve Maler: [00:07:52] Well, you know, technology is neither good nor bad; it's how we use it, right?

Ashwin Krishnan: [00:07:54] Yeah.

Eve Maler: [00:07:56] What I tend to think is it's the business model underlying the usage that tells the story. In the case of social sign-in, you've got a dynamic where the identity provider, the IDP, you know these big social guys, would have a lot of people who log into them and use them for what they are, but now they turn around and say, "Hey all you relying parties. Here's what I have on offer. I have my user base on offer. I have information on offer." And that's how they make their decisions to put up that NASCAR login, or whatever you wanna call it. Now in the enterprise context we've actually had federated login for much longer. The SAML standard on which I work starting in the year 2000 — oh well, dating myself very precisely — that was to enable, kind of enterprise to enterprise for a start...

Ashwin Krishnan: [00:08:45] Seamless sign-on.

Eve Maler: [00:08:45] Seamless sign-on. The original use case was something like, you're an employee and you want to get access to your 401k site. You'd start from your employer, you're already logged in and you seamlessly go. But then the other pattern came along, which was you start at the — think of it as the benefits provider — and then you get redirected. So, social sign-in is the latter pattern where it's, "Hey, I have an opportunity for you to login using the ID key, then you'll come back to me with a special packet of information," known as a set of claims, identity claims. So, the business model underlying determines the sensitivity, determines the risk, I think, to the individual, whether they're a consumer, an employee, whether it's governed by a contract or whether by their explicit consent, how informed were they, and on and on and on.

Ashwin Krishnan: [00:09:35] So, if we switch gears a little bit to cloud and look at it through, maybe a similar lense, which is instead of Facebook and Google, now you're talking about AWS, Google Cloud, Azure, whatever. And AWS clearly made a really good model of shared responsibility, so it actually shows what you're responsible for versus them. So in that model, there are a number of things, including probably the hardware, the base OS, maybe some portion of the networking stack that the provider is responsible for. And then you have your apps on top or even your infrastructure. So, it remains that as an enterprise, when you are talking about identity, talking about permissions, you are focused on what you are responsible for. And yet, you have this underlying concern, or you should at least, in terms of, "I don't control the lower half of that stack." So therefore, what safeguards do I have to put in place, if any at all, in the event — I hate to use the word rogue employee — that something goes bad? Do I just say, "OK, this is what it is right now, therefore I need to protect myself on the top" or when people talk about multicloud say, "OK, I need to spread my bets."? So, what's your thought on how identity needs to evolve? How does it need to be strengthened to be able to compensate for this lack of control on the lower half of the structure?

Eve Maler: [00:11:10] Well, a couple of things. First of all, I almost don't know an enterprise sufficiently large that isn't multicloud. They do that for a number of reasons, spread your bets, best of breed, in terms of the applications they're working with, and that requires a fairly sophisticated approach to identity because you want to have a view over the identities that you're managing — whether it's employees or whether it's consumers, you know those end users — you need to have a unified view of them across all the clouds. So, whether it's 100 or 500 or 1,000 or 2,000 applications on the back end, and frequently I work with customers who have that many, you actually do need a unified view across all of them. And if it's consumers you serve, you actually want to give them as much as possible: that single-pane-of-glass view into what it is they need to do, just so that they'll trust you, you know, regardless of regulations and here I have to say, cough, GDPR or California Consumer Privacy Act (CCPA) or whatever it is. So that's one element, identity must have a multicloud stance because

enterprises are multicloud. I mean, it's just the way of the world. That's one. Another thing is whenever you have employees that are working in these environments that hop domains, so to speak, is the basic principle of least privilege. And it's hard to do that. It would be so much easier if we could just dispense with it, but it makes it easier to adhere to the security principle of least privilege which matches nicely with the privacy principle of data minimization. If you have a good infrastructure for access control and for authorization and for issuing entitlements, and if you have a good identity basis on which to manage those entitlements — and there I go right back to if I'm doing privacy in consent and consent management, if I have end users of that stripe — base that infrastructure on good authorization infrastructure as well because you have to solve the same problem ultimately. And so, what makes least privilege hard to do is trying to do it application by application and even cloud stack by cloud stack. There are certain architectural principles that BeyondCorp has articulated nicely that make it easier to do.

Ashwin Krishnan: [00:13:56] So, it's interesting when you said least privilege is hard to do. One of the things that came to mind … I'm still grasping the implications of that, I'm not a DevOps person, I've never done DevOps in my life, but efficiency, cost, agility, and the usual buzzwords around why people go to cloud, DevOps is a key reason why that happens. I still remember this particular event, I think I was at an AWS community day about three months ago. I forget the exact vendor on stage, but one of the bigger properties on AWS. He was literally on stage saying we grant DevOps engineers full admin permissions, but we revoke them every 24 hours and see what they've used. That mindset of saying, "Give everybody keys to the kingdom, instrument that to a T, then pull it back." That's a very non-traditional data center mindset.

Eve Maler: [00:14:52] That's interesting, yes.

Ashwin Krishnan: [00:14:56] I mean, as a tech ethicist, as a tech practitioner, podcaster, I love the concept, but it's just if you are the CIO, if you are the VP of Ops., and you say, "OK, who has permissions? Oh, everybody's super admin for

the next 24 hours and then we're going to revoke permissions and give them exactly what they need." What's your response to that?

Eve Maler: [00:15:16] It's an interesting approach. I can see using the descriptive versus prescriptive approach of observing and then in arrears adjusting. My standards colleague, Justin Richer, has an approach he calls the grey list. Instead of whitelisting or blacklisting, you greylist, and then you're in the grey zone, and you can observe and adjust in a more finely grained fashion as you learn. And that's very friendly, I suppose, to things like AI algorithms, where if you get enough data you can start to really adjust. So, I'm sympathetic to the approach, although giving everyone a God key, maybe you don't have to go that far necessarily. Although as soon as you get close to any medal, I always find that the problem is there is only superuser access to a database and then everybody shares the password to the database, and now you have to use unsatisfying approaches to security at that level. And that's where it's much more fun when you're doing things like API security and using these more sophisticated approaches.

Ashwin Krishnan: [00:16:30] So, one of the other things — again on the same topic of superuser access and console access, etc. — another approach, and probably this is becoming more mainstream as we speak, is the fact that your base or the surface area itself is so small and the rapidity with which your features evolve is also continuous. Therefore, if something goes wrong you can actually come up with another version and spin down what you have and spin up something else that you have really quickly; just based on instrumented logic vs. traditionally having to log in a superuser, run a dev trace and do all kinds of stuff. So, in that world again is everybody a superuser? Just from a philosophical standpoint of saying, "You own this and if it is not up to snuff you instrument it and then you make changes and then you deploy." I mean, in that ecosystem, what role does identity play?

Eve Maler: [00:17:32] Gosh. Well, one thing I was going to comment on before, and it's bringing it up again for me is, identity is key for everyone and everything.

I'm reminded of IoT devices where as long as you have over-the-air updates and use them, I suppose that you can apply that approach. So yay, I hope.

[00:17:51] But you know there's SPIFFE as a standard, which is applying identity in a sort of fully-fledged fashion to services and that's quite promising for being able to continue the pattern of applying identity to everyone and everything. So it's not just devices and sensors and people and so on, it's to services and containers and the rest of it. I really like that trend because if you can't identify it, it's awfully hard to manage it. You want everything to be a first-class object in your system so that you can have an identity record and a lifespan that you can manage with a proper lifecycle.

Ashwin Krishnan: [00:18:33] That opens up another point about identity. You mentioned IoT people have always tied identity with individuals. And now this big shift of devices and on average, what, 40 IP addresses per home in the U.S?

Eve Maler: [00:18:55] Oh, at least! I'm just in a new home now. It's probably much higher than that.

Ashwin Krishnan: [00:19:01] That concept of, like you're saying, its identity is not a person anymore, it's every device, everything that has a heartbeat that's talking to somebody else or some other entity.

Eve Maler: [00:19:10] Yeah, that's right. In the last several years, certainly in the last four or five years that identity has got to be thought of as people and things and mobile devices for the longest time now. And now you have to manage the relationships between them. It's not, it isn't your grandfather's IAM, for sure.

Ashwin Krishnan: [00:19:29] So from a consumer standpoint, I think it's battle lost. You can't expect even a tech-savvy head of household to have any idea how many devices they have, let alone the number of connected devices that are edge computing — where devices are talking to each other.

Eve Maler: [00:19:45] They're not going to be making a list of all the identities that all the things have.

Ashwin Krishnan: [00:19:47] That's not going to happen. Is that an opportunity for companies to step in and, just like you mentioned about SAML in the enterprise world or social credential management, is there an opportunity for an IoT identity management? And in a way something permission based, which is I get an alert in the morning saying, "You know what, unknown device detected." I mean, I use Cujo, I have nothing do with Cujo, but I love the way they built that device. It makes it easy to understand, even for a non-techy, as to really what's going on over here. If I can see that there's more traffic today than there was a week ago, then what's different? Am I consuming more video? So how does somebody grapple with this?

Eve Maler: [00:20:33] That is the opportunity. And it's one of the things that alarms me a little bit about some of the regulatory moves around privacy because it tends to be backwards looking with regulation, it's just the nature, whereas innovation happens around the stuff that wasn't there yet. But there is absolutely an opportunity because well, we got 5G coming, so you know maybe everything that used to be more of a dumb device ...

Ashwin Krishnan: [00:21:00] Everything's connected.

Eve Maler: [00:21:02] Maybe everything is its own hub. What we need more of, I think, are smart devices that are really smart about enabling people. You know, consumers are super users of everything they buy, even if they're not technically owning all the software in it, they're licensing stuff. These companies want to empower people to do the things that make their lives better and easier and more convenient and cleaner and faster and whatever. So, managing the permissions to things is partly how people are actually getting paid. For example, Airbnb is managing who gets to come into your place. Uber is managing who gets to come into your car and pay you for being taken somewhere. So, is that consent? I would argue, actually those are forms of

managing consent. And there's money in them there hills if we can do that better and in a more concentrated way because all of our stuff is becoming smart stuff whether we like it or not. But, you know, I think that if we like it better, we'll do it more.

Ashwin Krishnan: [00:22:10] Correct. Maybe we can talk a little bit about the framework that you've been talking about for a long time and that you've talked about it in conferences. So, just for the benefit of the audience — again keeping just the consumer in mind for now — I think in your framework you talked about devices, applications, connectivity, so at every level there is a tacit or an implicit permission that the vendor tries to grab from you, and then you are talking about actual consent that is permissioned by the end user without overwhelming them with blah. Can you talk a little bit about what that nirvana state looks like, where vendors are no longer just looking at GDPR and running for cover or getting thrown off by the CCPA, but really raising the bar of how do I build trust with the consumer while at the same time not frightening them with a 50-page EULA?

Eve Maler: [00:23:12] Right. It's clear that people don't want to just be messing with privacy settings when there's something in the news that is untoward about privacy. Although there's evidence that people do take unilateral action when there's an option for them to materially improve their lives. You know for a couple of years I've been using DuckDuckGo ...

Ashwin Krishnan: [00:23:32] Same here!

Eve Maler: [00:23:33] Nothing can stop me from doing it. It's awesome; it works. At the same time, setting do not track in your browser, well it does nothing at the margin, so there's not much incentive to do it. So, there's an example of the exact kind of thing that doesn't help, right now anyway. And if you set it and it does something and it has negative effect as well as positive effect or only negative effect. People will know that because they're rational beings to that extent. At least last I checked. So, I introduced a framework for understanding

basically how to measure control elements of consent and privacy last year at RSA. The typical way that people understand consent actually is little opt-in or opt-out switches, sliders, and interfaces. And I was finding that it's a terrible way to describe the universe of what we really need, particularly as it pertains to the Internet of Things. I was using connected cars for some examples, but you know, health care IoT, and just lots of examples. And just looking at Google Docs as a classic example of ways that permissioning access for others to our stuff is in our lives. But no regulation forced them to do that, put that in the interface. I had just developed some broad categories of how to measure how much control are you giving to an end user and looking at how much trust businesses need to build with their users. We've got lots of examples of needing to go beyond the regulations when users can abandon you. Look at what Ancestry.com and 23andMe and an assortment of DNA-testing companies just did on a completely discretionary level ahead of regulations now that we've got the California consumer privacy act, some of them are subject to that.

[00:25:35] One dimension to measure is whether you're just giving reactive consent opportunities versus directive consent opportunities meeting your set opportunities to share proactively, like a Google Docs share button, versus how can somebody longitudinally monitor and manage what consent they've given over time. So that's one sort of category. And then another category, now I've got to remember my framework, she says buffering just a little bit, I can't even remember now!

Ashwin Krishnan: [00:26:19] I think you talked about devices, applications, but I think that the broader piece of the framework that I really liked was the fact that there are different levels. As consumers we tend to think about, at least from our phones' perspective, it's just the apps.

Eve Maler: [00:26:34] Yeah right.

Ashwin Krishnan: [00:26:34] But then there's an underlying infrastructure, so I'd probably be at the far end of the spectrum when it comes to privacy: I have

location turned off by default, including Uber, but for lots of people that's inconvenient. I think the ability to ... so I'll give you this example, it shocked one of my most tech-savvy friends. He was at Target, and he bought a diaper for his newborn. All he did was use his Target REDCard or something, and the next morning he gets a Huggies ad in his inbox. He was saying, "I wasn't even using the Target app, all I did was use a physical card." But that's information that's already gone back and it's come full circle. But at least he was aware and he could make that connection. I think a lot of these times the connection is so ...

Eve Maler: [00:27:26] Tenuous?

Ashwin Krishnan: [00:27:27] In the back end and you don't know how you're being targeted, and yet you are.

Eve Maler: [00:27:32] And you know these are cases where companies ... I think people are quite sensitive now to how the game works. In the same way that we all now have password strategies, password management strategies of one sort or another because we have enough logins, we've started to realize how the game is played. What we don't have is a way to change it, and that's due to the environment that lets businesses have these business models. And this is where regulation does have something to say. We're seeing state by state in the U.S. — there's almost competition now among the states, as it were set up to do I suppose — laboratories. And we're seeing the federal government in the U.S. look at some sort of legislation at that level. We're seeing discussion drafts come out. It's likely something will happen, and the motivation may be to smooth the way for business across all the states in the same way that GDPR was done largely for that digital single market. So, I think there's no question that we're going to see movement, at least by individual states, more and more.

Ashwin Krishnan: [00:28:53] So finally, comments on businesses that you've seen make the right moves. I'll give you two examples that actually stand out in my head. One is Tim Cook, I think this was a month ago, was addressing the EU and talking about privacy and consent. Then, I think as of this morning, I think it was

IBM's Virginia Rometty standing up there and arguably pointing fingers at Facebook and Google. But being the CSO of one of the largest iconic brands and standing up there, does this now, forgive me for using the word permission, but does it give permission to other vendors to say it's OK to start talking about this. Right. It's not a chief privacy officer sitting in this corner office worrying about it.

Eve Maler: [00:29:39] Oh yeah, budgets are rising as we speak; you can almost hear it!

Ashwin Krishnan: [00:29:41] So, final takeaways for enterprises: this regulated framework is coming and we can see that, right? Large organizations' chief executive officers are standing up there and starting to talk about this on mainstage. What are you going to do about it?

Eve Maler: [00:30:01] Yeah, maybe as a final comment. There's no question it's not just a backwater of a chief privacy officer. There's a complex interaction between market forces and regulatory forces. The regulatory forces are listening to what people say. People are sensing when they're starting to get an upper hand on where we see market tipping points happen.

[00:30:24] I commented on this recently in another talk, about how in the 1970s we had all these movies come out of the U.S. where people were read their Miranda rights, and I'd heard subsequently — I don't know if this is true, I tried to establish it, but I'm pretty sure I had heard that this was true — that people in Europe watching American movies started to think they had Miranda rights; you know, wishing they had. And so, in the same way everybody in the US who just had to click OK or something because of all the new privacy policies started wishing they had GDPR rights, You know this is part of the revolution of rising expectations of privacy.

[00:31:06] When we first met and did our video podcast, I talked about my framework of understanding what the new data privacy means, and it's really in

three levels. Data protection is one level, of just securing the personal data. And data transparency is knowing what's going on, even if you can't change it. And then data control is somebody giving you the knobs and the buttons to twiddle and thereby gaining much more of your trust — because it's only fair if that does go above and beyond what the regulation says to do. And business models turn on the top two layers. You gotta do the first one even though there may be requirements. But I suggest that businesses pay attention to the differences among these three layers and even consumers; everybody's a consumer too, right. So, when you see something in the headlines, analyze, go read between the lines about what's really going on because when we heard about the Google Plus third-party sharing thing, we still don't know if that was a data breach or a discretionary thing. Now, obviously Google Plus wasn't a big enough service anymore ...

Ashwin Krishnan: [00:32:17] They shut it down.

Eve Maler: [00:32:18] Yeah, they just cut their losses, but we still don't know what category it was in. I suspect it was the top two.

Ashwin Krishnan: [00:32:27] But I think that's a great takeaway, just from a business perspective, from a product manager engineer's perspective it's like: Are you doing data protection, are you doing data transparency, and are you doing data control? Just having that framework in mind would lead to a much better product or service outcome.

Eve Maler: [00:32:43] Yes, product owners, product managers, throughout the land should really be thinking about what they can do to do better for their customers. Along those three lines.

Ashwin Krishnan: [00:32:50] Very, very cool. Again, always a pleasure to talk to you, Eve.

Eve Maler: [00:32:53] Likewise.

Ashwin Krishnan: [00:32:53] Looking forward to the next one. Thank you.