TECH REIMAGINED
AN ENDAVA PODCAST

The data dilemma: security vs. safety

00:00:01
Speaker 1: Tech Reimagined, redefining the relationship between people and technology, brought to you by Endava. This is Tech Reimagined.

00:00:11
Bradley Howard: Welcome back to Tech Reimagined. I'm Bradley Howard and I'm glad to invite you to the latest episode of our show. Running now into our third season, this podcast explores how technology is influencing the fabric of our society. That's how we live, the way we work, and how we do business. And our guest today is CISO, that's Chief Information Security Officer, and security expert, Greg van der Gaast. For today, we thought about discussing the complicated relationship between having an ever- growing digital footprint using data ethically and keeping it secure. Welcome, Greg.

00:00:45
Greg van der Gaast: Thanks for having me, Bradley.

00:00:46
Bradley Howard: It's wonderful to have you on the show. So can you tell us a bit about yourself and what you've been up to lately?

00:00:51
Greg van der Gaast: As you mentioned, I'm a Chief Information Security Officer for a company called Scoutbee GmbH, probably not terribly well known outside of Germany, but we help a lot of global companies, extremely large multinationals, primarily kind of fast-moving consumer goods, manufacturing, automotive, aerospace, find and manage their supply chains. So if a certain car company needs to manufacture something and they're looking for parts, we will scour the internet, a lot of machine learning, data science, AI. And what normally takes six months to find one supplier who can forge some rare metal with some special process, we'll do in maybe six weeks and find them seven or eight or 10 companies to make supply chains, both resilient, but also quality options, price options, that sort of thing. And we deal with a lot of data.

00:01:47
Bradley Howard: I'm sure you do. And I'm sure you've been very busy during the pandemic with supply chains going all completely skew- whiff.

00:01:52
Greg van der Gaast: Yes, it's definitely been... It's one of those opportunities in disguise for us.

00:01:58
Bradley Howard: So let's get started on data specifically. So the amount of personal data that's being stored is incomprehensible to the average person. Most of us give some of it willingly in exchange for customized experiences and improved services. And a small percentage of people are aware of the full extent of their digital footprint and how their data's used. So what's your opinion on how individuals and companies are creating the ethics for our data?

00:02:25

Greg van der Gaast: How they're guiding the creation of it, of the ethics themselves is a really good question because it's quite murky. I think the ethics are probably being stretched quite thin in a lot of places. Funny enough, I think some people are becoming a little bit aware of that. There's some pushback on Facebook, for example. Although I'm more connected with security and IT people, so I'm probably seeing a lot more than that than the average Joe is. And in terms of consumers, I think people are actually really, really unaware, incredibly unaware. And I actually recently saw a video about, it was an American, well, I guess it was a grocery store, a food shop store, but they sell everything as they do in America. And they had worked out based on shopping patterns when someone was going to be having a baby just based on what they were buying.

But quite often they would predict this before the people buying those products were even aware that they were pregnant themselves just because they'd figured, oh, well, people start getting urges for this or that. Or they don't realize they're pregnant, but they're feeling a bit, like some kind of physiological response. So they buy a bit more of this, maybe a bit more of that. And it was incredibly accurate. And they actually got into, they had customers, like parents of very young women, who their parents didn't know they were pregnant, outraged at them receiving these targeted ads about pregnancy things. And then having to come back and apologize like, oh, you guys knew she was pregnant six months before we did. And this is 20 years ago. This is before Amazon. This is before any of that stuff.

So you could only imagine how sophisticated the data science is and how much information about our lives can be extricated from a little bit of information, let alone what they have now. And especially, you look at Google, you look at Facebook or now Meta, they have so many data points. People who think that they're being quite private, revealing very little, relatively very little information about themselves online, would be shocked to know how much these companies have actually figured out about them. So the ethics, I don't really think they're there. That's a terrible answer, but that's my answer.

00:05:04
Bradley Howard: Who do you think will create the ethics? Do you think it'll be consumers? Do you think it'll be the companies themselves? And I'm talking about the giants themselves, the Googles, the Facebooks, et cetera. Do you think it's governments?

00:05:16
Greg van der Gaast: I think Apple is an interesting case right now, because I've seen Apple adverts dedicated entirely about to protecting your privacy. So they know they're spending marketing money, showing this to consumers because they know that it will win their favor. They are starting to see that consumers are aware enough. They don't understand how any of it works, but they're aware enough that if we send them a message that we care about this stuff, and we've got features to help you with this stuff that they're going to like that and they're going to buy our products, which in a way is actually using the data that they have about people to shape their shopping habits. So you question the ethics of that one even.

But then there are other cases, which I won't mention specifically where they have had data breaches, not data breaches in conventional security, but where they have been called out for using data in ways which we're questionable. So the question is, are companies... I think companies will drive it, but they'll drive it in such a way that it's a marketing activity and will land them business. So in many ways they're driving the ethics as an excuse or not as an excuse, but as a sales ploy, more than actual ethics, because in the background, they're still quite being unethical. And I think consumers will shape the demand, but the demand is being met with a response of, ah, we can sell you more stuff because you care about this without actually doing it in the background. And the consumer will never know what the actual internal processes are because, I mean, fair enough, they're commercial secrets. You're not allowed to know them. And there's legal commercial reasons why the end consumer isn't allowed to know what is happening with their data. Even with GDPR, it's very tricky.

00:07:17
Bradley Howard: Playing devil's advocate on the Apple story, it's all very well Apple saying, no more third- party cookies, et cetera. That's fine when you manufacture the handset and have such a massive footprint of your Safari browser on your own handsets as well. So you know everything about the user anyway. You're the guardian, basically. You're just saying to everyone else, you can't track my customer now. I just wanted to play devil's advocate on that.

00:07:45
Greg van der Gaast: Yeah. Which is fair enough. You can't track my customer unless you give me this extra money, or we'll use it as a competitive advantage because we have such a monopoly on this data. I mean, our interaction point with the world is primarily our phones for most people. So they have a tremendous platform for gathering that data. And don't get me wrong, I have all Apple products, but I'm not under any illusion that my data is perfectly safe with them and that it's not being used to map me out in some way.

00:08:19
Bradley Howard: So from an end user perspective, that's the vast majority of people, how do you think they balance between security and freedom or functionality? Do you think most people care about security, by the way?

00:08:31
Greg van der Gaast: Well, the interesting thing is, I think people care, but I don't think people are aware. And it's funny how we talk about balancing security and functionality because you know all the times where a website asks you whether you accept or deny the cookies or just the functional cookies or all the cookies or none of the cookies, it doesn't seem to make any difference what I press, I still get the same experience. I mean, I can't recall a time where I've denied all the cookies and the website experience wasn't fine. So why would I ever accept these? So, that's an interesting... Do you know what I mean? Like it's never...

I'm not an expert on any of these things, by the way, but there are certain things where you need to give your data. If I'm going to do some skydiving and they need some next of kin, yeah. If I'm buying something, yeah, they need my payment information. I think it's important to... I think it's everyone's almost civic duty to insist that people collect as little data as possible and be adamant of like, well, you don't need this data. You don't need to know my date of birth. You don't need to know this. You don't need to know that.

00:09:52
Bradley Howard: It's interesting you saying that actually, because although I have a good idea of what goes on behind the scenes on a lot of these products, I like to remain signed in on Google Maps and some other apps, because I find functionality. Like you search for a business and then a year later you're around a particular area and it says

you once visited this place. I find that quite interesting because I can't remember why it looks a bit familiar. So I find that useful, but I know lots of people who think that is the creepiest thing in the world and shouldn't be allowed, which is why I think the whole data ethics has a big question over it about, is it useful? Is it not useful? What's the compromise there?

00:10:33
Greg van der Gaast: Well, I think ultimately, and I think you make a great point though, it's like, shouldn't it just be about choice? Some people don't trust the government for absolutely anything and they want to live in a shack by a lake in the mountains with a bunch of guns if anyone comes within half a mile. And other people are like, yes, yes, implant me with this chip so I can pay by swiping my hand. Different horses for different courses, right? I think ultimately the ethics come down to choice and choice can't be made without awareness. By the way, we've not rehearsed any of this and I am not an expert in this topic. So this is just a discussion, but I think the conclusion I'm reaching for myself is, it's down to choice.

00:11:17
Bradley Howard: Yeah. Can you talk a little bit about the difference between data protection and data security?

00:11:22
Greg van der Gaast: Yeah. And I was actually just about to say the caveat there is the choice has to be enforced. The choice has to be protected by the other party. We were talking about this off air before. So funny enough, data protection and information security say pretty much the same thing, it's data and information, protection and security. However, the way we use it, information security tends to be what we call cyber systems, data, that sort of thing. Whereas if you go to data protection, it's much more the legal process, the principles of collecting data privacy and so on.

And the story I was recanting before was I was once invited to speak at a data protection conference and I was like, well, great, but I'm information security. So I don't really know anything about this. So I decided to present on, because I'm quite critical of the security industry, my presentation was how information security hurts data protection. And I was explaining to this audience, which was all DPOs, lawyers, intellectual property lawyers, privacy lawyers, and how they're focused on you go to a website, you get the cookie notification, you sign up for this. Your name is stored there. It's stored securely. There's a mechanism for you to request information about what we have stored about you. You are allowed to request that your information be purged. We have a mechanism by which that happens, blah, blah, blah, blah. And they do this tremendous job of thinking all these processes out to make sure that you have all these abilities and possibilities as a consumer to protect your information, recall your information, have someone delete your information, all this and that.

What none of these people realize is that most of the time, this will be on a database that hasn't been updated or patched in six years where the password is admin, admin, and it's sitting on the internet and some 13- year- old kid is going to... They're very worried about protecting each individual data record, but some kid somewhere is just going to like log into it and steal four million records in one shot. No one gets upset because two or three records were lost because someone mishandled a piece of paper on a desk, they get upset when your entire customer database of X million people is lost. And I think that's the point where privacy, what we call data protection and information security meets. There's a bit of a vast chasm there. I think privacy in many ways as ambiguous as it is, it's kind of more mature from a legal and process standpoint. Whereas information security is often very questionable, nebulous and run by a bunch of geeks, like 15- year- old me who can't hold a conversation. So we're completely unaccountable for our actions, because no one wants to talk to us anyway.

00:14:21
Bradley Howard: And thinking of you as a consumer, do you trust that most companies keep your data secure? I think I know what the answer's going to be.

00:14:29
Greg van der Gaast: No. It's just a flat no. It's just no. Some large companies, significant legal departments, a lot of process, a lot of governance do a better job, but stuff gets outsourced. We've seen stories where someone... I'm sorry to keep picking on Apple. Okay. I'm a lifelong Apple product person, but there was a story where someone in, I think a support center in India had access to someone's private pictures on their phone or their iCloud account. And they came out, right? So the supply... Especially these very large companies have a better chance of being more resilient because they have the resources, but they also have a lot of people and there's a lot of human factors and a lot of suppliers and dependencies and they probably have third- party risk management. Apple might be an exception. For all I know, Apple has most of its stuff in house, but a lot of companies out there use tons of third- party services. They might be using a data lake for this or hosting for that, a data processing company for something else. And you're dealing with one company that you're aware of, but to provide the service, your data's going through 15 other companies and they have agreements with those companies, but you're not aware of them. They're in the contracts and there's internal audits and stuff, but as an end consumer, you're not necessarily allowed to see them, nor do you have a right to audit for those third parties. So if you request some information about your personal data from the company you actually did business with, and then they ask one of their suppliers in the supply chain like, can you validate this? And then they lie to them, then you don't know, they're just going to feed you back to the answer.

So yeah, it becomes... The bigger the chain gets, whether it's one company with just a sheer scale of factors and people and locations or smaller companies that are reliant on other companies where you get a chain of dependencies, the bigger it gets, the more difficult it is to actually protect data, especially when people are constantly pushing to drive value out of data. Data science is an incredible thing and we use it to drive business. We try to find ways of making money out of data. And every day we use Google, we do searches. We watch videos. We don't have to pay for any of this stuff, and yet people are making a killing off of it. It's like we're getting free stuff and yet someone's earning money off giving it to us. It's only when you do that, the expression that if you're not paying for it, you are the product. And you have to be aware of that. You are the product. You're selling a part of yourself to get this service, to get this convenience. And that's just the equation. There's no way around it. And that's it.

00:17:36
Bradley Howard: So as a Chief Information Security Officer, how do you behave with your technology? Do you take a photo and then make sure that it's not uploaded to any cloud and you come home and you save it to a floppy disc?

00:17:51
Greg van der Gaast: No. I do think a lot of people in security, especially, really are like that. Even some of my own employees, you go to their house or you see their setup in the background that it's like, they've got a bunch of Linux machines and separate storage drives and everything's triple encrypted. And I'm like, yeah, whatever. If someone really wanted to embarrass me, it would probably be pretty bad. I mean, you also have to live your life at some point, because it'd be impossible to compartmentalize everything. I think the easiest thing is simply to give out as little data as possible. I mean, I'm very active on LinkedIn, but I don't put a lot of personal data there. And that's it. I live, maybe it's my old age, but slightly, I mean, compared to your average 25, 30 year old nowadays, I'm basically off the grid. Even though searching my name gives you 20 pages on Google, I'm relatively off grid. I don't have a huge public Instagram or TikToks or any of that stuff.

00:19:04
Bradley Howard: Right. Do you have any security advice for people that don't work in the technology industry?

00:19:10
Greg van der Gaast: So my very, very simple advice, use strong passwords. I know it sounds incredibly cheesy, but use those password managers you can, and the randomly generated password things, and obviously use different passwords for different sites. I know it sounds really simple, but it's actually the most that you can do. And one feature, we're going to say something positive about Apple, when you go into your Safari and passwords, the Apple, I think it's Safari, there's actually a screen on your phone where it will tell you which of your passwords it knows to have been compromised on which sites. And the interesting thing is I have about 100 right now and I use those completely random passwords on all of them. And they're all different passwords and none of those companies, and some of them are big names, have ever notified anyone of a breach. But if my completely random password is out on the darknet somewhere, clearly it came from somewhere and it's only been used in that company. That makes you realize the scale of how many compromises there are in a lot of big companies that we trust that are never actually notified, but you do have a feature where you can actually change it. So, I think that's a big one.

And just give out as little information as possible. If you're filling in a profile, don't reuse passwords, don't share passwords, use complex passwords. If you're signing up to some online form or something, just put a fake name, date of birth, whatever. There's no need for you to put your real address, real phone number, any of the real information in there. And quite often, it's very basic websites that someone sets up. It's just some guy in his basement for his car club or his knitting club or her knitting club or whatever. Saying terribly sexist things. Apologize. They get compromised, but people that signed into that use the same password as they use for their Amazon and their eBay. And that's how they get compromised. So it's important to realize that a site with maybe a lower level of technical maturity is quite likely to get hacked and have your credentials taken. And they'll never know that they've been hacked and they'll never tell you. So yeah, that's my consumer tip.

00:21:33
Bradley Howard: That's really interesting. And do you have any tips for how we can educate the next generation on security?

00:21:40
Greg van der Gaast: It's tricky, isn't it? Because I generally think the best way of mitigating it is to put as little information about yourself out there in the first place.

00:21:48
Bradley Howard: Yeah. But that doesn't really apply to the next generation at the moment. Not from my experience (inaudible) .

00:21:52
Greg van der Gaast: Yeah, exactly. That's kind of my point. They're really quite keen to put it out there, which I guess you shouldn't be too surprised if it does eventually get compromised. Well, they say companies learn very quickly from breaches, so maybe our kids will too. No, other than that, I don't really... I mean, I do think companies, for example, go on Apple, this feature where you can generate your own random passwords, that's very helpful. iPhone now has a feature where every time you have to fill in a password field, it will actually come up with " hide my email" and it will generate a random email address that they own, that if you get an email to, they will forward on to you. These third- party companies won't actually know your real email address. I don't use it and annoyingly it won't actually just put in my real email address. I always have to type it out.

We are building more and more things to help people. And I do think this is a little bit counterproductive in some way, because we're helping people do stuff without their understanding of why it needs to be done. And then they take it for granted. And then when that help isn't there, they're not aware of it. Just like nowadays you have people who crash their cars into the hedge and their answers to why is, " Oh, I didn't realize I had to steer," because we've built so many safety systems into the car that people have lost the ability to think about the problem or what they should be doing. So, it's a bit of a double- edged sword. Younger people nowadays are more comfortable with technology and use more technology than ever before, but they have less and less understanding about how it actually works underneath. And I think that's a little bit worrisome, because there's this disconnect with being able to justify or understand why certain things work certain ways or why you should, or shouldn't do certain things, certain ways.

00:23:52
Bradley Howard: I would extend that even further into not appreciating the business value of that data as well. So in the old days, when we kind of fill in a paper form without details, you were pretty comfortable that went back to the company. That was it. Now, when I was talking to my kids about this recently, every Google search you do, every time you're using any of the Google products, it's just collecting more and more data about your usage, things that you don't even realize, about the time of the day, about some of the weather scenarios, et cetera. And it's creating that entire digital image of your behaviors, and then selling that to millions of other companies that can then start advertising towards you.

Now, I don't have a problem with that, because I think getting a free search engine that's as good as Google is phenomenal. The fact that we don't pay for it, I just can't believe it's going to carry on free for a while. But to understand that their business is to take that data and then resell it on, my kids had no idea about that and I still to this day, don't think they really understood it either.

00:24:57

Greg van der Gaast: Yeah. I think it's important to explain the commercial models behind this. Back to what we said before, it's like, if you're not paying for it, you are the product. And you have to understand that you are giving away a little piece of yourself every time you give some information and they will use it to manipulate you even. And that's, I think the really insidious part, it's not just products. Even governments will try to manipulate your thinking. Corporations will try to manipulate your thinking. So it's quite insidious and we have to be aware of it.

00:25:28
Bradley Howard: Great. Well, thank you very much, Greg. That was really interesting. Well, thank you so much, Greg, for your time and your experience telling us about data security. It's really interesting the stories that you sprinkled in there as well. To all of our listeners, hope you enjoyed this edition of Tech Reimagined. Thanks for joining us today and looking forward to doing so next week as well. Please hit the subscribe button and hit the like button if it's on your app.