Your Phone Really is Listening to You: The Evolution of Data Privacy, GDPR, and Why/How to Ensure Compliance

written by Cat Coode | June 30, 2020

My first long term job was in architecture and software development for a device, Blackberry, that put security first, so everything we were doing was privacy and security focused, including the way we developed the operating system. I was there for over 10 years and at the end of my time there, I was running the architecture team for the handheld software. This privacy-first notion was foundational to me to move into privacy and security, and help other people understand why that was so critical.

Our Limited Understanding of Data Privacy

The concept of data privacy has been developed over the last decade or so. Most people are not as tech savvy about what they're putting online as they think they are. Even most people in the technical fields, including developers, haven't read the terms and conditions on any of the software platforms that they're using on a daily basis.

I've read these terms and conditions for several apps – they're boring and long – and people generally don't realize what they're agreeing to give away. For example, APIs, which are the way that coders get access to information inside the systems aren't just sharing one particular piece of information, they're also sharing all of this other data about you.

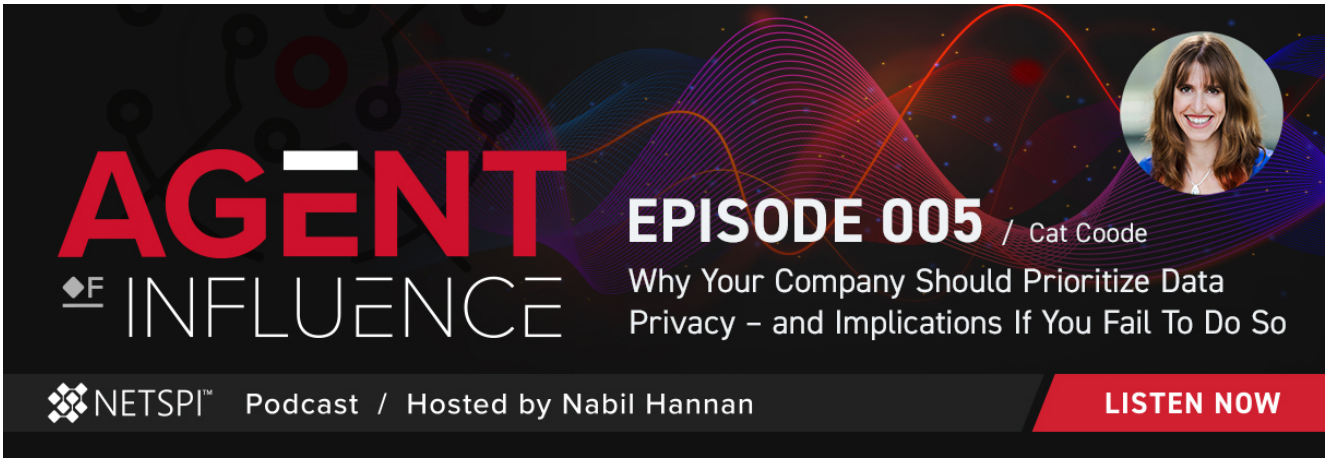
Data privacy is similar to how we have faith in the safety of a microwave, but very few people actually know how it works. You just know it heats your food.

It's the same thing I find with things like Facebook and Google. Google is going to search your results, but you don't stop to think about how much data Google is collecting on you when you're doing that to get you the results you need or what Facebook might be doing in order to set you up with the right people online so you can share photos. We don't question the technology that comes into our lives. And because regulations and laws didn't exist when they were built, they were able to take all sorts of liberties with data that they should never have been able to take.

Google search results are very tailored to you because of the amount of data that they're gathering about you to be able to serve you content in a way that's most relevant to you. For example, if two people search the same keywords on Google or another search engine, the results and order of those results tend to vary significantly based on web browsing habits, email

content, things they've clicked on in the past in Google, etc.

While we are accustomed to this customization, we also need to recognize that it's based on so much information. It's not necessarily a bad thing, but it is a trade-off to be aware of.



What GDPR Means for Data Privacy

GDPR stands for the General Data Protection Regulation and is from the European Union. It's essentially a set of rules that should have been in place a long time ago. As I mentioned earlier, software products have in a way, advanced without regulations and rules. While Europe has always had privacy laws, they finally put their foot down and said to companies, "You can't use and abuse individual's data without their knowledge and consent of what you're doing.

GDPR puts the individual first.

Pieces of GDPR include:

- Companies have to have consent to collect data from people.
- Users have to have a clear understanding of what the company is doing with their data, it cannot be all legalese.
- Companies have to have a retention period, so if you're collecting personal data about someone and it's only valid for a certain number of days, you need to get rid

of that data at that point. If you don't have a legal or business reason to keep the data, you should be deleting it.
- Users also have individual rights, so they're able to go back to a company and ask to see all the data the company has about them. Users can also ask to be removed from the company's system, which is called the right to erasure.

While this is a European-based regulation, it affects any customers who are European and any business that's based out of Europe, so it ends up being fairly global. For example, if your company is out of North America or India or Africa and you serve European customers, you have to comply with GDPR.

In addition, other countries are looking at similar regulations. Brazil is supposed to be launching their LGPD, which is GDPR under their law, and eventually Canada will adopt GDPR-like regulation. In addition, CCPA, which is the California Consumer Privacy Act, is more targeted at not having your data resold, which is more about the fact that the Facebook's and Google's of the world have been taking individual's data and reselling it without their knowledge. It's only a matter of time before other countries and states get on board with having more of these regulations to protect individuals.

Consequences of an Organization Failing to Achieve GDPR Compliance

GDPR has significant fines and they are already imposing these fines. There are several websites that are tracking the fines that are being applied. One example I've seen is a company in Ireland where a user asked to see their information and the company said no. They asked again several times and the company still said no. That individual then contacted the data protection authority and the company was fined $200,000 for

not answering the individual.

The fines are based on due diligence. Every company is going to be breached at some point. The question is, as a company, have you done the best job you can to protect an individual and their personal information? Have you limited what you're collecting? Are you storing it safely?

If an individual asks to see the data you have about them, you have to let them see it. If you do that, then if you were ever breached, you would have small to no fine, but if you haven't done that, you haven't even tried, and then that's where these large fines are coming from.

How Can Companies Make Sure They Are GDPR Compliant?

The regulations themselves are a legal framework, and online you can find checklists from a legal perspective asking if you've taken certain action – Do you have a privacy policy that covers the following things? Do you have an incident response plan?

What I find the checklist misses though is the proper technical implementation of a lot of the requirements, which is something I'm helping companies put into place. For example, privacy by design is seven principals of how to best set up individual-first privacy over innovation, which has been adopted globally. Creating a foundation of privacy, ensuring that you've evaluated the data you're collecting, whether you need it, how you're storing it, etc. But then companies need to optimize on some of these things. If the checkbox on GDPR is: Can a user access their data? From a foundational and technical level, how are you authenticating to ensure that the user is who they say they are? How are you optimizing it so that if 100 people request their data on the same day, you can handle that in your company? Setting up the support at the bottom will help everything else fall into

place at the top.

Why Your Company Should Prioritize Data Privacy

Many companies, especially startups say they don't have the budget for data privacy because they want to focus that money on development. But data privacy is like an insurance policy. For example, an incident response plan, just the plan itself, will save you $500,000 when you have a breach – just by having the plan. If you don't have a plan, then when you're breached, you are scrambling to find your stakeholders, to get on a phone bridge, to figure out who you need to contact to do your forensics, etc.

Creating a plan should take your company less than a week, and you could either do it on your own or hire a consultant to do it. It should cost less than $10,000 from start to finish, and it saves you $500,000.

By putting privacy in place, it reduces your risk of the breach. If you take these steps now to set your company up right, you won't have these large fines and reputation costs down the line.

How Individuals Can Protect Their Data

The number one thing people can do is set their privacy settings. Go into your privacy settings and go through each individual setting, and turn off your microphone, your camera, and your location. If you haven't explicitly turned off microphone use, it is listening to you at all times. This is why people say, for example, "I was talking about going to New York, and now I'm getting all these ads for New York." You want these apps to only use microphone, camera or location-tracking when that app is in use.