Privacy in tech: burden or opportunity?

13 July 2021, 02:00

Tatiana Galibus
Annanda Rath

Privacy. Often not a popular concept in tech companies. Privacy is a synonym for the burden of data protection compliance. Privacy hinders system functionality, even conflicts with security requirements. Why care about privacy anyway? Privacy is dead, right? Wrong. Wrong. Wrong!

Privacy matters

Before explaining why privacy does matter, let's find out what privacy actually means. Privacy is about having control over how your personal information is collected, processed, and shared.

Why is it that we approach privacy differently in our digital lives than in our real lives?
No one will question the need for privacy in the offline world. For instance, when someone asks about your day, your answer will vary: a polite 'fine' when you don't know the person well, some highlights of your day to an acquaintance, and maybe a full report with lots of juicy details to close friends. The answer will depend on the context.

You also expect everyone to treat the information you share in confidence. Imagine there is a billboard in your street that informs the neighborhood about your daily activities. Or imagine meeting a stranger who knows all about your personal life through word-of-mouth. Unsettling thought. Fortunately, just fiction.

The same concepts should apply in our digital lives. The fact that collection, processing, and sharing of digital personal data is done by computer systems makes it less tangible, but no less problematic. On the contrary, given the growing number of connected devices combined with the big data hype, there are exabytes of personal information available about each of us.

Remember that billboard and well-informed stranger? They have become realities in our digital lives.

People care about privacy. Tech companies should care too.

The reasoning that if you've done nothing wrong, you've got nothing to hide does not hold. We all want to keep certain things to ourselves and share only bits of information with others. And it's our right to do so.

Technology companies, however, tend to handle personal data more loosely.
"Collect first, think about what to do with it later" was apparently the trend over the past years. Not

a good idea really. For starters, it's illegal. The purpose should always be specified before collecting personal data, there should be a legal ground to do so, and the data can evidently only be used for the specified purpose.

Secondly, the more personal data a company collects, the more responsibility it has to manage the data properly: secure the data, enforce purpose limitation, delete data when no longer strictly required, etc. This is less straightforward than it might sound. Are you for instance sure that all data instances are deleted, including those in backups and log files?

Fortunately, we see a growing interest in privacy. Data breaches and privacy violations have a major impact on a company's reputation. Consumers show they do care about privacy. (Think of the overnight switch from WhatsApp to Signal due to updated privacy policies.)

Privacy tech is booming. Big companies, such as Apple, see the value of privacy and use it as a competitive advantage in their marketing campaigns.

Privacy will not 'break' your system

It's a common misconception that privacy conflicts with the system's functional or quality requirements. However, ignoring privacy until your product is ready to launch, comes down to poor judgment. If you consider privacy only as an afterthought at the end of the system development stage, it will likely conflict with existing requirements. The key is to embed privacy features into the design process at an early stage.

Compare it to building a house. Imagine all the structural work is done: walls, roof, windows, and flooring; everything is ready. Only at that point, you start thinking about the plumbing. That will clearly cause problems. Some construction work will likely have to be redone. You will need to make trade-offs and shortcuts that sacrifice your plumbing requirements, as they are no longer feasible given the building's construction (bathrooms and kitchen sinks are overrated, right…?). Or you will need to tear down part of your building and implement foundational changes to your building's construction. Or, even more likely, you will need to sacrifice both sets of requirements. What a waste of money, time, and opportunities!

Fortunately, that is not how houses are built. During the design phase, you take into account all utility requirements, stability, aesthetics, and so on. You combine and align them to create your dream house.

The same approach should be taken for system design. You should consider all qualities upfront, together with the functional requirements. Combining and aligning them at that early stage will result in a system that will not require big sacrifices.

In a nutshell: Use privacy as a competitive advantage. Apply privacy by design. Integrate privacy early and in a systematic way.

Contribution by Kim Wuyts, Ph.D. (https://distrinet.cs.kuleuven.be/people/KimWuyts)

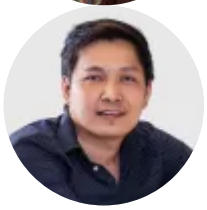


#industriepartnerschap #sterkondernemen

Authors



Tatiana Galibus



Annanda Rath