"Privacy is over" is a familiar statement dating from the first internet wave, but is it still true and applicable for the near and long-term future? This interview outlines the potential developments with respect to data privacy and personal data ownership, also in relation to the attractiveness of data for services, marketing, security and intelligence purposes.

Who Cares About My Privacy and Who Should?

Ronald Koorn

Data Privacy is an ambiguous subject that defies description; there's no global standard and not even a uniform definition in the EU Data Protection Directive (and its 28 national implementations), nor in the upcoming EU General Data Protection Regulation. Individual interpretations of privacy and the sensitivity of personal data abound; in addition, governments, (intelligence) agencies and companies have their own privacy interpretations. Will laws, regulations and all these different interpretations of privacy converge or diverge across the globe?

What's all the recent media attention on privacy about?

A number of concurrent events such as the invalidation of the EU - US Safe Harbour agreement, high-profile privacy breaches (Ashley Madison, Target, JP Morgan, US/UK governments, Sony, etc.) and Snowden's disclosure of massive intelligence activity all result in increasing privacy awareness.

Is there a real issue? After all, everyone gets online services and a social network for free or in exchange for personalized marketing.

There's no free lunch, you just pay for these online services with the value of your personal data. Almost everyone is tracked, both in the physical and the online world; most personal data is hoovered up via "data dragnets" and very detailed profiles of your person have been assembled and sold. By now, the organizations with these profiles may well have a better idea who you are than your friends. Some privacy-sensitive people use multiple IDs (personas/avatars) to circumvent online tracking.

The negative privacy effect is not limited to spam and viruses; ID theft and unfounded criminal accusations are serious consequences of data breaches or erroneous use of your data. If your biometric data is compromised, this may have unpleasant consequences as it might be difficult to obtain another iris or fingerprint.

The EU enacted privacy legislation 20 years ago. Do most organizations comply?

That's still a challenge. Only a few organizations are sufficiently mature and capable to be fully privacy-compliant. Most have a policy/paper-based approach with limited implementation of privacy controls in all their processes, IT systems and third-party contracts, as well as "soft controls" with regard to staff behavior – an aspect not to be sniffed at. The internal privacy stakeholders from Legal, Marketing, HR, IT, Compliance and Marketing hardly ever see eye to eye on privacy, let alone that they understand each other's terminology.

Why do 50+ countries have privacy legislation but no security legislation?

Good question. Initially people's privacy was the primary human

right to protect, and the security of personal data was considered to be included. However, with the advent of cyber security threats, several countries have enacted or are now embarking on (cyber)security legislation, especially with respect to the nation's vital infrastructures. By the way, security alone could and will never solve the entire privacy problem.

After all the terrorist attacks, who would not sacrifice privacy for national security and personal safety? If people have "nothing to hide", why would they object to privacy-invasive measures by governments?

This sounds plausible on the face of it, but everyone has something he would prefer to keep to himself (when did you lie or have an extramarital affair recently?). No one looks forward to having a Stasi-like, over-transparent society, where we voluntarily relinquish control of our own data and personal freedom. Without countervailing powers, this may eventually lead to a surveillance state (*1984*). In case of accidental mistakes in criminal investigations and prosecution, there is no presumed innocence and a reversal of the burden of proof.

What will change after the EU's General Data Protection Regulation has been enacted?

Unlike the current Directive, this regulation will be immediately imposed on all 28 EU Member states after a two-year transition period and will not require any local legislation to be passed by national governments. It additionally requires a formal Privacy Officer, documented controls and procedures, Privacy Impact Assessments, specific protection of data of minors, notification of data breaches (already moved forward to 1 January 2016 in the Dutch Privacy Act), the right to be erased/forgotten, personal approval ("explicit consent") for Data Analytics and profiling, etc. The national Data Protection Authorities can finally build up their staff if they are allowed to collect the high fines, which can run to € 100 million. Although self-/co-regulatory or legislative approaches all have limitations, on a global scale more and more countries will adopt a type of privacy legislation similar to the EU.

Will that be sufficient for the next 20 years?

Probably not, although the positive side is that the upcoming regulation has been formulated in an IT-agnostic manner, which will make it independent of inevitable technological developments. Consequently, practical, context- and risk-based guidance is needed to implement the appropriate privacy controls. Where countries apply different legal privacy requirements, there is a need for further convergence of privacy definitions and regulatory frameworks and requirements, as the internet doesn't recognize borders.

Will there be other game changers or tipping points for privacy?

Unfortunately, a major privacy incident with significant impact on a large part of a nation's population and high-profile organizations may be needed to raise sufficient awareness. Politicians, Boards, media and society at large will then demand or organize better global privacy safeguards. I expect that such an incident will happen within 5 years. The combined ensemble of Big Data profiling, multi-media surveillance, use of biometric, neurological and genetic data and "stealth"-like monitoring via the Internet of Things may cross a creepy line and provoke a public and political backlash. When predictive analytics include discriminatory algorithms or biases, a major public outcry is usually heard. As a result, citizens may demand new privacy arrangements with the private and public sectors alike, facilitated by civil society institutions such as privacy platforms and/or consumer associations. These organizations can negotiate "premium" services – for a small fee – to be offered by commercial entities without their customers giving up their privacy. Otherwise, "data supermarkets" may emerge which will buy and sell personal data sets in a self-service manner.

Can we predict the privacy situation in 30 years' time?

Organizations will increasingly have their information and privacy governance and accountability of the entire information lifecycle under control. Governments will have strengthened their regulatory enforcement and citizens will have the privacy protection of their sensitive data (medical, financial, biometric data) in their own hands. Within the next 10 to 15 years, the reasonable expectations of guaranteed privacy of customers and citizens will be met by most organizations.

By that time we will all be using some type of Personal Data Wallet to be in control of our own data effectively. It can disclose personal data to third parties in private and public sectors, based on granular but user-friendly configurable authorization levels. Moreover, personal data sets will be encapsulated in a standardized "Data Transfer Container" and provided with meta-data indicating its source, ownership, authorization, data transfer and residence restrictions ("geo tagging"), etc.

Most data in rest will be encrypted, anonymized or pseudonymized ([Koor15]) (without governments controlling the master key or backdoors), preventing even intelligence agencies to access it. National security and privacy are no opposites on the same continuum; anti-terror surveillance can co-exist with privacy protection. All organizations are required to not only secure, handle and destroy personal data in a strict manner, but they will also need to be fully transparent about their personal data usage to ensure trust in our information society. Unfortunately, experience has shown that solely relying on an organization's statements of good privacy practices is insufficient; supervision by a data protection authority, preferably per continent, and enforcement through internal and external audits and certifications will definitely be required to back it up.

Reference

[Koor15] R. Koorn et al., *Big Data Analytics & Privacy: How To Resolve This Paradox?*, Compact 2015/4.

Ronald Koorn is a partner of KPMG IT Advisory and the new editor-in-chief of Compact. With a combined Business Information Systems, IT Audit and Business Administration background, he focuses on various IT Governance subjects ranging from digitizing and IT program control to regulatory compliance/privacy and IT costs.