

Trondheim revisited: from Directory Services to big data

Type

Presentation

Authors/presenters:

Erik Huizer (CTO, SURFnet)

Evelijn Jeunink (Corporate Privacy Officer SURF, legal counsel SURFnet)

Author Affiliations

SURFnet
PO Box 19035
3501 DA Utrecht
The Netherlands

Keywords

Privacy principles, data protection, big data, Directory Service, Data Protection regulation

Abstract

"A Directory Service contains information about organizations, services and, most important for this article, people. When a Directory contains personal data, the processing of this data, can conflict with a person's right to informational privacy.

There are two EC directives concerning data protection, named SYN287 and SYN288. The SYN287 defines amongst others the circumstances under which processing of personal data is allowed.

This article focusses on the matters of interest relevant when applying the rules to Directory Services. It describes why a balance has to be found between providing personal data in order to facilitate easy communication and withholding data because it concerns the privacy of the data subject."

The paragraphs above are part of the abstract that was submitted by us, exactly 25 years ago for the TNC predecessor JENC 1993 in Trondheim.

Over the last 25 years, technology has transformed our services, our work and our lives in ways we could not have imagined in 1993. From local to the cloud. From limited data sets to (meta)data collected by services and social media we use every day. From a relative innocent phenomenon as Directory Services to big data and advanced data analysis.

During this 25 years the concept of privacy was subject to debate. The unrestrained sharing of personal data on social media led to the statement that privacy is dead (and we better get used to it). Others approached privacy as a monetary transactional concept, or as primarily a contextual concept. In the past 25 years there were times with little or no interest in privacy, there were moments of glory (the Max Schrems court ruling) up to a lively privacy discussion today.

Data protection law also evolved during the years. In an attempt to ensure our privacy the EU adopted the General Data Protection Regulation (GDPR) in 2016. From a EU legislative point of view one of the greatest achievements in recent years. With thanks to the Snowden revelations in 2013, that gave at a critical moment a push in the right – privacy protecting - direction.

The Regulation replaces the Data Protection Directive we discussed in 1993 (adopted in 1995) which already aimed at a high standard of data protection but lacked the accountability and enforcement principles of the Regulation. In an attempt to keep up with the technical and social developments the GDPR requires transparency in automated decision-making systems, implementation of privacy by design principles and risks assessments.

What we need to protect is no longer the relative static personal data stored in a database but our behavioural data, gathered from websites and applications. We need protection against incomprehensible and not transparent algorithms resulting in decisions that have an impact on our lives. We have to deal with the challenges related to mass-surveillance, big data, online behavioural advertising and cybersecurity.

Within our community of Education and Research we see the impact of these developments. Of course we still have to deal with our online (Directory) Services with care, but the privacy challenges of the moment are completely different from those of 1993. Think of the data gathered for learning analytics, automatic decision making based on study application procedures or the combining of large datasets for research which takes away the anonymity of data and goes beyond initial defined purposes.

Data protection principles and regulation alone are not sufficient to protect our privacy. Those principles were relatively easy to apply 25 years ago on Directory Services. Today's practice makes this a lot more challenging. If data minimisation is a principle, how to deal with the European Open Science Cloud and the resulting big data? If purpose limitation is a restriction how to deal with open data access and research combining sets of data without knowing beforehand which correlations or hypotheses can be found?

The presentation discusses the development of the concept of privacy, the applicable rules and today's practice. If we take the protection of privacy seriously we should not treat it solely as a compliance issue. To answer the above questions, we need the discussion with and participation of the inventive and creative minds within the NREN community.

Erik Huizer is CTO at SURFnet, the Dutch national academic and research network. He is currently working as interim CEO for GÉANT, Europe's leading collaboration on e-infrastructure and services for research and education. For over 30 years he has been involved in education and research networking, Internet standardization and Internet governance. For his contributions to the Internet he has been inducted into the Internet Hall of Fame in 2014. In 2015 he was honored with the title of Dutch ICT personality of the year.

Until 2015 he served as part-time professor Internet Applications at University of Utrecht. He remains a research associate at this university.

He has been teaching at various developing countries workshops on Internet policy and technology. He is a TEDx speaker.

Evelijn Jeunink studied Law and Business Administration at the Rotterdam School of Management both at Erasmus University. Evelijn specializes in privacy and data protection. She is Corporate Privacy Officer for SURF and legal counsel for SURFnet. See also <http://www.linkedin.com/in/evelijnjeunink>