Chapter 104
The "Right to be Forgotten" in the Era of Social Media and Cloud Computing

Maria Giannakaki
Karageorgiou and Associates, Greece

ABSTRACT

The globalization and ubiquitous character of information in the era of social media and cloud computing has led to a loss of control over individuals' own data, who face significant difficulties to understand and measure the consequences of the disclosure of their personal information on the Internet, as well as the means and the context in which they are or will be processed. Under the reviewing process of the EU Data Protection Directive, the "right to be forgotten" appears to be the means by which individuals will be able to regain control over their data. However, implementing the new right in the ICT environment and striking the proper balance between conflicting rights, such as the freedom of expression, will not be easy. The purpose of the chapter is to identify the challenges that Web 2.0, Web 3.0, and cloud computing technologies raise, focusing on how these challenges are addressed under the new "right to be forgotten" and providing an insight of the alternative "quasi legal" measures that emerge.

INTRODUCTION

Even before the digital revolution, the ability of individuals to maintain control over their data against improper discovery dissemination or misuse was threatened by governments (wiretap telephone lines, censorship), companies (misuse of customer data), and individuals (identity theft). However, the recent emerging technological and social phenomena, such as social media and cloud computing pose crucial challenges for data protection.

Control is an important data protection concept. In the Web 2.0 and Web 3.0 era privacy relates to the knowledge of what data is collected and for what purpose they will be used, having choices about how they are used, being confident that they are secure and that the data controller and data processor will be held accountable for their collection and use. Another aspect of control is also the right to know and control where such data are transferred (the country, to which data are transferred, if the country's level of data protection is adequate), as well as the third party or

external application (games, quizzes etc), which gains access to such data.

Personal data has become an increasingly valuable currency. However, while the collection and monetization of user data has become a main source for funding "free" services like search engines, online social networks, news sites and blogs, neither privacy-enhancing technologies nor its regulations have kept up with users' needs and privacy preferences. This paper will set out the characteristics of a changing technological environment and socio-economic context and identify the challenges the new ICT technologies pose to individuals' privacy.

The right to informational self-determination includes the notion of control over ones data and the principle of data portability. In addition to that, the widely applauded principles of necessity, proportionality, data minimization, and transparency grant to data subjects with the right ask for a limited period of data retention, rectification/deletion, to ask for information when data are published/transferred to third parties as well as information about the location of their data in the cloud. However, it is questionable whether the existing principles can be applied effectively against the new privacy invasive technologies. Under the reviewing process of the EU Data Protection Directive, the "right to be forgotten" appears to be an effective means by which individuals will be able to regain control over their data.

It is acknowledged that the codification and implementation of the new right will face the difficult task of striking the balance between the right of privacy and other individual's or society's existing rights, such as the freedom of expression and the freedom of society to record history.

However, although binding legal requirements, such as the "right to be forgotten" is likely to be rather difficult to be implemented and enforced, "quasi-legal" measures such as self-regulation, privacy by default, data minimization and data portability appear to be able to secure the data subjects control over their data in the new ICT environment.

THE NEW ICT ENVIRONMENT

Web 2.0 and Web 3.0

Nowadays there is a significant evolution in the way the Web is used to such an extent that many computer, business, information, and legal experts argue that new versions of the World Wide Web are created: Web 2.0 and 3.0. Internet is no longer just a huge repository of digital information enabling users to access read-only content and static HTML websites and to navigate through link directories and portals. New programs, services, and uses are transforming Web into an intelligent and intuitive tool where personalization and contextualization of information is the primary product and goal.

Web 2.0 presents a second generation of web-based communities, applications and hosted services that facilitate participatory information sharing, interaction and collaboration on the World Wide Web (O'Reilly, 2005). Users are not only consuming, but they are also contributing information through Social Networking Sites "SNS" (like Facebook, Myspace, Twitter, LinkedIn), blogs, video sharing sites (like Flickr, YouTube, Digg), hosted services, web applications and mash-ups. Unlike traditional media, which offer a one-way communication (in which media broadcast information for public consumption), social media offer a two-way interactive experience, where users can interact instantly and directly with either the originators or the authors of the preferred information. Social media has enabled individuals and groups to voice opinions and become commenters, editors, content creators, producers, and distributors.

Web 2.0 allows users to use "Web as a Platform" in order to create and distribute their own User Generated Content (UGC) and promote creativity, collaboration and sharing through mass social networking channels. Furthermore, it facilitates users to express themselves, engage in social and political debates, access and participate in economic, cultural and administrative activities, contribute

Related Content

A Framework for Government 2.0 Development and Implementation: The Case of U.S. Federal Government
Yu-Che Chen (2014). *Cyber Behavior: Concepts, Methodologies, Tools, and Applications (pp. 452-470).*
www.irma-international.org/chapter/a-framework-for-government-20-development-and-implementation/107742

Who Are You Online?: A Study of Gender, Race, and Gaming Experience and Context on Avatar Self-Representation
Robert Andrew Dunnand Rosanna Guadagno (2019). *International Journal of Cyber Behavior, Psychology and Learning (pp. 15-31).*
www.irma-international.org/article/who-are-you-online/236158

Fear of Missing Out, Social Media Use, and Psychological Wellbeing Among University Students
Bhavana Arya, Shirin Sharmaand Harshita Kumar (2021). *International Journal of Cyber Behavior, Psychology and Learning (pp. 1-9).*
www.irma-international.org/article/fear-of-missing-out-social-media-use-and-psychological-wellbeing-among-university-students/288496

An Ongoing Journey to Foster Urban Students' Online "Public Voices"
Nick Lawrenceand Joe O'Brien (2016). *International Journal of Cyber Ethics in Education (pp. 32-45).*
www.irma-international.org/article/an-ongoing-journey-to-foster-urban-students-online-public-voices/164408

Applied or Denied?: The eLearning Experience of an Autistic, Mature-Aged University Student
Jillian Downing (2014). *International Journal of Cyber Ethics in Education (pp. 1-15).*
www.irma-international.org/article/applied-or-denied/123979