Telecommunications Policy 38 (2014) 800–811

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevier.com/locate/telpol

Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception

Meg Leta Ambrose

Communication, Culture & Technology, Georgetown University, 3520 Prospect St. NW, Suite 311, Washington, DC 20057, USA

ARTICLE INFO

Available online 11 July 2014

Keywords:
International privacy law
Data protection
Right to be forgotten
Expression

ABSTRACT

The right to be forgotten is contentious partly because it highlights the difference between U.S. and E.U. prioritization of information privacy and freedom of expression. Recently, a moderate amount of research has been undertaken to explore the conceptual issues underlying the right to be forgotten and how the right conflicts with the U.S. first amendment, but little has been written about its impending implementation and interoperability issues. While this is an E.U. Data Protection Regulation proposing to grant rights only to E.U. citizens, the world has a stake in this right for a number of reasons. This article will analyze the options for non-E.U. countries and data controllers, namely the U.S., to react to the establishment of such a right, now called "The Right to Erasure". These options are the following: (1) adopt the same right to erasure for themselves, (2) ignore right to erasure claims, (3) comply with erasure take down requests, or (4) seek to establish a modified version of the right to erasure. In assessing these options, the article will first address the reality of a right to erasure under U.S. law. Second, it will discuss compliance and jurisdictional issues if the right is ignored. Third, the article will look at the impact of full acceptance of the take-down regime, focusing on the potential chilling effects and abuse. Finally, it will propose that non-E.U. countries encourage a right to erasure that is less disruptive: a right to erasure that allows data subjects to directly request removal of data held privately by data controllers and a right to oblivion for publicly available information that is enforced similarly to defamation claims, requiring a court order.

1. Introduction

In 2010, the E.U. announced it would begin work to create "a new general legal framework for the protection of personal data in the European Union covering data processing operations in all sectors and policies in the European Union," and specifically noted its intent to "introduce" the right to be forgotten (European Commission, Press Release, 2010). Action taken by the data protection agency of Spain ("AEPD") against Google to force the removal of links from its index that directs users to information the agency had deemed 'forgettable' (Daley, 2011) and the language of the right to be forgotten proposed by the European Commission in its January 2012 draft of the new Data Protection Regulation ("DP Regulation, 2012") have caused a great deal of confusion and skepticism about the right to be forgotten and erasure. On October 21, 2013, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") adopted several amendments to the European Commission's proposal for the DP Regulation, including a title change that removes "to be forgotten" from Article 17 leaving "The Right to Erasure."

http://dx.doi.org/10.1016/j.telpol.2014.05.002
0308-5961/

While the DP Regulation is an E.U. proposal granting rights only to E.U. citizens, the world has a stake in the right to be forgotten for a number of reasons. First, content on the Internet is generally accessible around the world and the removal of content affects all users. Additionally, services that derive from big data analytics have the potential to benefit all users. Second, a great number of data controllers that will be obligated to 'erase' personal information will be outside the E.U. (Labovitz, Iekel-Johnson, McPherson, Oberheide, & Jahanian, 2010).[1] Third, designing systems to comply with one country's laws may result in 'privacy creep,' meaning systems and platforms are designed to provide deletion for users in one region, the opportunity for deletion will extend beyond that region to anywhere the platform or system is utilized.[2] Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship leading the changes to the E.U. Data Protection Directive ("DP Directive, 1995"), has made it clear that "[a]ll companies that operate in the European Union must abide by our high standards of data protection and privacy," (European Commission, Press Release, 2010). Reinforcing this point in 2011, Reding stated, "Privacy standards for European citizens should apply independently of the area of the world in which their data is being processed… Any company operating in the E.U. market or any online product that is targeted at E.U. consumers must comply with E.U. rules," (European Commission, Press Release, 2011).

Of course, the eventual language of the right to erasure cannot be precisely predicted, but the article focuses on the aspects of the right that have remained consistent over the last several years as the Regulation has gone through the rule-making process. The article makes recommendations for adjustments to the right to erasure in draft form to support final language that is internationally interoperable. Compliance and enforcement expectations for those outside the E.U. are not clear (Bennett, 2012; Kohl, 2007). The article will consider ways in which non-E.U. countries, companies, and other data controllers may respond to the E.U. DP Regulation's right to be erasure as it stands in the amended version. Options for countries outside the E.U. are to (1) adopt the E.U. right to be erasure, (2) ignore the right to erasure, (3) comply with right to be forgotten take-down requests, or (4) work to establish a compromised version of the right to be forgotten that is acceptable to a number of different stakeholders. As each of the options is analyzed, the last offers the potential for the greatest interoperability, efficient cross-border functionality and preservation of national information policy values. The article concludes by proposing further medication of the right to erasure to create a version that divides its two conceptual forms (the right to delete and the right to oblivion) (Ambrose & Ausloos, 2013) and requires different procedural treatment for removal. The right to delete should only apply to passively created data trails held privately by data controllers and third parties and maintain the current E.U. DP Regulation's proposed removal notice structure of enforcement (Para.1 of Art. 17, DP Regulation, 2012). The right to oblivion should apply to information made publicly available (Para. 2 of Art. 17, DP Regulation, 2012) and require a court order, ensuring that diversity in prioritization between speech and privacy is maintained but in a manner much less disruptive to Internet communication.

2. Related work

The problematic implications of technological advancements for forgetting, forgiving, and reinvention have recently become a policy conversation but have been of concern for privacy scholars since the 1970s when Alan Westin and Michael Baker explained in Databanks in a Free Society, that:

> Many citizens assume, out a variety of religious, humanistic, and psychiatric orientations, that it is socially beneficial to encourage individuals to reform their lives, a process that is impeded when individuals know (or feel) that they will automatically be barred by their past 'mistakes' at each of the later 'gate-keeping' points of social and economic life. Because the computer is assumed not to lose records, to forward them efficiently to new places and organizations, and to create an appetite in organizations for historically complete records, the computer is seen as threatening this forgiveness principle (Westin & Baker, 1972).

In 2002, Jean-Francois Blanchette and Deborah Johnson began discussing how systems can account for forgiveness principles expressed in the American laws of bankruptcy, juvenile criminal records, and credit reporting by categorizing data that will designates its lifespan (permanent, long-term, medium-term, and flash records) (Blanchette & Johnson, 2002). In 2006, Liam Bannon criticized design attributes of computer memory in relation to human memory arguing that forgetfulness is a virtue of memory, not a bug, and should be built into computer memory systems (Bannon, 2006). Martin Dodge and Rob Kitchin (2007) agree, claiming that forgetting should be an integral part of any system and that "the goal is to make the system humane and yet still useful." The authors suggest adding features that mimic absent-mindedness, misattribution, and sporadic blocking (Dodge & Kitchin, 2007). Anita Allen analyzed the legal implications for 'lifelogging,' a total recall movement inspired by Gorden Bell's My Life Bits project, concluding that memory glitches being built into lifelogs protect against its use and misuse by others (Allen, 2008).

[1] Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, and Farnam Jahanian, *Internet Inter-domain Traffic*, In ACM SIGCOMM (2010) (finding 50 percent of Internet traffic is contributed by 150 networks, large companies such as Limelight, Facebook, Google, Microsoft and YouTube generated and consumed 30 percent of all Internet traffic).

[2] While responses to legal requests for information may vary (efforts like Europe v. Facebook, http://europe-v-facebook.org/EN/en.html and #NOLOGs, https://www.privacyinternational.org/blog/what-does-twitter-know-about-its-users-nologs may extend user access to those requests deriving from non-E.U. users, they are not required to), it is expensive and time consuming to design country or region specific systems.