Chapter 9
Cloud Based Social Network Sites: Under Whose Control?

Jean-Philippe Moiny
University of Namur, Belgium

ABSTRACT

In studying Social Network Sites (SNSes), this chapter starts from the identification of a loss of users' control over personal information. It briefly defines what SNSes are and links them to "cloud computing." Its purpose is to identify how American and European (or as the case may be, Belgian) laws empower users to recover some control where they lack technical means to control information related to them. It will be shown that user's consent is central to numerous legal dispositions. To this end, four legal themes are studied: privacy, data protection (consent and right of access), confidentiality of electronic communications, and the prohibition of unauthorized access to computers (hacking). Through these reflections, the American and European perspectives are compared, and the differences between these inevitably lead to a final title underlying the importance of rules governing prescriptive and adjudicative jurisdictions concerns. These rules are finally sketched, before the conclusion finally summarizes the whole purpose.

As the author of this chapter is a European jurist, European law constitutes the point of departure of the reflections, and can be sometimes (titles I and IV) the sole legal framework of the discussion. The information in this chapter is current up to January 28, 2010, save as otherwise stipulated. It should be noted that the information that is studied in context is constantly changing.

DOI: 10.4018/978-1-61350-132-0.ch009

INTRODUCTION

Two quotations illustrate a claim for control coming from the users of Social Network Sites (SNSes). From the US civil liberties association, before the American Federal Trade Commission [FTC], "EPIC urges the Commission to […] require Facebook to give users meaningful control over personal information" (EPIC v. Facebook 1, 2009, no. 3)[1], "[c]ompel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers" (EPIC v. Facebook 1, 2009, no. 118)[2]. Actually, "users desire control over the collection and use of information about them" (UC Berkeley, School of Information [UCBSI], 2009, p. 5). More recently, a modification of Facebook's privacy settings lead to a new complaint of EPIC noticing that users are now forced to make public data they could formerly keep restricted (EPIC v. Facebook 3, 2010). It has notably been claimed that Facebook "Converted Facebook Users' Private Information into "Publicly Available" Information" (EPIC v. Facebook 3, 2010, nos. 35 and ff.) and "Discloses the Personal Information of Facebook Users without Consent" (EPIC v. Facebook 3, 2010, nos. 65 and ff.). As regards the European Union and the group known as the Berlin Working Party, SNSes providers were already advised to "[i]mprove user control over use of profile data" (International Working Party on Data Protection [IWGDPT], 2008, pp. 6-7).

In the context of SNSes (I), Internet surfers seem to partially lose the legitimate[3] *ownership* of data relating to them. They suffer a *loss of control*[4] (II). To some extent, law – at least, the fields studied here – faces this concern. But how is and should it be done (III)? American and European regulatory systems both need to be referred to, and their differences brought into focus. While individuals are not generally bothered by these differences, these SNSes often have a foot in Europe and the other in the United States – frequently California (Facebook, LinkedIn, and Second Life). But which law and which judges are in control (IV)?

This chapter defines what SNSes are, legally and technically. It also suggests some consideration related to the SNSes market. For the needs of the whole purpose, Facebook is taken as a recurrent example. SNSes generally constitute information society services pertaining to cloud computing technology. Therefore, some ideas can be extended to cloud computing in general. The technology used and the functioning of SNSes lead to identifying a certain loss of control over their personal data by users. Some legal issues related to this loss are therefore addressed. Moreover, privacy and data protection are studied in this chapter. A legal conception of privacy which empowers users is chosen as regards American and European perspectives. In this respect, the horizontal effect of the fundamental right to privacy is discussed. The focus then moves to specific concerns related to data protection. The quality of consent of the data subject, apparently omnipresent in the context of SNSes, is discussed. The data subject has to be informed by SNS providers. His consent should be separated from his consent to the general terms and conditions of the SNS. And finally, such consent has to be freely given. This last point requires to be linked with the considerations related to the SNS market. The relevance of the data subject's right of access in the context of SNSes is then examined, before the confidentiality of electronic communications is brought into focus. The use of cookies by the SNS provider is specifically discussed in this framework. And some reflections relate to the qualifying an SNS as an electronic communications service. Mainly, this chapter identifies which communications are protected. The interest then moves to the protection of the user's terminal. The prohibition of hacking is discussed in the context of SNSes. It is questioned if a breach of the terms of use of an SNS by a user