The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1750-6166.htm

Data protection issues pertaining to social networking under EU law

Eleni Kosta
Interdisciplinary Centre for Law and ICT (ICRI) – Katholieke Universiteit Leuven, Leuven, Belgium

Christos Kalloniatis
Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, Mytilene, Greece, and

Lilian Mitrou and Stefanos Gritzalis
Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, Samos, Greece

Received 12 December 2009
Accepted 5 March 2010

Abstract

Purpose – The purpose of this paper is to examine how the introduction of new communication channels facilitates interactive information sharing and collaboration between various actors over social networking services and how social networking fits in the existing European legal framework on data protection. The paper also aims to discuss some specific data protection issues, focusing on the role of the relevant actors, using the example of photo tagging.

Design/methodology/approach – Privacy in social networks is one of the main concerns for providers and users. This paper examines the role of the main actors in social networking, i.e. the providers and the users, scrutinised under the light of the European data protection legislation. Specifically, how social networking service providers deal with users' privacy and how users handle their personal information, if this manipulation is complied with the respective legislation and how "tagging", one of the most familiar services provided by the social networking providers, may cause privacy risks.

Findings – Social networking is one of the most remarkable cultural phenomena that has blossomed in the Web 2.0 era. They enable the connection of users and they facilitate the exchange of information among them. However, the users reveal vast amounts of personal information over social networking services, without realising the privacy and security risks arising from their actions. The European data protection legislation could be used as a means for protecting the users against the unlawful processing of their personal information, although a number of problems arise regarding its applicability.

Originality/value – The paper discusses some privacy concerns involved in social networks and examines how social networking service providers and users deal with personal information with regard to the European data protection legislation.

Keywords Privacy, Social networks, Data security, Law, European Union

Paper type Research paper

1. Introduction

The development of the internet and the emergence of Web 2.0 introduced a new era in the communication of the internet users and the exchange of user-generated content.

Transforming Government: People, Process and Policy
Vol. 4 No. 2, 2010
pp. 193-201

1750-6166
DOI 10.1108/17506161011047406

One of the most remarkable cultural phenomena that blossomed in the Web 2.0 era are the online social networks (or else "social networking sites" or "social networking services"), such as Facebook, MySpace, Friendster, Bebo, Netlog, LinkedIn to name just a few. Social networking services are very popular among adolescents and young people, but they also attract the attention of users of an older age. The latter prefer, however, more profession-related social networking services, such as LinkedIn (Anderson Analytics, 2009).

The introduction of new communication channels facilitates interactive information sharing and collaboration between users over social networking services. At the same time, social networking services serve as platforms for the exchange of vast amounts of personal information to a sometimes potentially public audience, as the profiles of the users are not always restricted to be visible only by their friends. Privacy and security considerations have been raised parallel to the great success of social networking services. The privacy settings of the services can be used as a tool for the users to protect their privacy. Via the privacy settings they can restrict the access to their account and distinct parts of it only to specific contacts or categories of contacts. However, not many users change the default privacy settings, which means that the privacy of the users is to a large extent in the hands of the providers of the social networking services. Recently, Facebook changed the default privacy settings of all user accounts, so that specific information, such as their list of friends, pictures or the pages they are fan of, are visible to everyone (Facebook, 2009). The Electronic Privacy Information Center (EPIC) has filed a complaint with the Federal Trade Commission, urging the FTC to open an investigation into the revised privacy settings of Facebook (http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf).

2. Social networking services

The vast expansion of social networking services reveals a tendency of the users to acquire as many contacts (friends) as possible accompanied by their eagerness to reveal personal information. Indicative is the experiment that was organized by the information security company Sophos in 2007, which wished to increase user awareness on the dangers of social networking in the advent of the phenomenon. Sophos created a Facebook account for "Freddi Staur" (an anagram of "ID Fraudster"). The account was represented by a small green plastic frog who divulged minimal personal information about himself. A total of 200 friend requests were sent out in order to collect information regarding the response of the users and the degree of personal information they were willing to divulge. A total of 87 of the 200 Facebook users contacted responded to Freddi, with 82 leaking personal information (41 per cent of those approached), while 72 per cent of respondents divulged one or more e-mail address and 78 per cent of respondents listed their current address or location (www.sophos.com/pressoffice/news/articles/2007/08/facebook.html).

The ease with which users reveal personal information in social networking services, as well as the simultaneous lack of awareness and understanding regarding the threats and dangers lurking in such disclosure of personal information, alarmed International and European agencies, data protection and privacy advisory bodies. The European Network and Information Security Agency (ENISA) published a position paper informing the users of online social networks on security issues and gave recommendations regarding their use (ENISA, 2007). The International Working

Group on Data Protection in Telecommunications (IWGDPT) adopted a report and guidance on Social Network Services, commonly known as "Rome Memorandum" (IWGDPT, 2008). The working group made recommendations for regulators, providers of social networking services and users, in an attempt to raise awareness on privacy issues in social networking services. The Rome Memorandum was followed by a Resolution on Privacy Protection in Social Network Services that was adopted by the 30th International Conference of Data Protection and Privacy Commissioners in 2008, which also contained recommendations for users and providers of social networking services (International Conference of Data Protection and Privacy Commissioners, 2008). In response to the heated debate on the protection of the privacy of the European users of social networking services, the Article 29 Working Party[1] adopted an opinion on social networking services, in which it included key recommendations on the obligations of providers of social networking services, so that they comply with the European regulatory framework on the protection of personal data (Article 29 Data Protection Working Party, 2009).

3. Providers of social networking services under data protection scrutiny

A major issue arises with regard to safeguard of European Union (EU) citizens' privacy rights and the applicability of the European Data Protection Framework on providers established outside the EU, This issue is very important as the European data protection framework sets high standards with regard to the protection of individuals relating to the processing of their personal data and imposes strict obligations to entities that process personal data. The Article 29 Data Protection Working Party is of the opinion that the provisions of the Data Protection Directive[2] apply to the providers of social networking services "in most cases", even if they are located outside the EU (Article 29 Data Protection Working Party, 2009). The Article 29 Working Party sees two potential bases for the applicability of the Data Protection Directive:

(1) the Social Networking Services provider have an establishment in the territory of an EU Member State; or

(2) although the Social Networking Services provider does not have an establishment within the EU, he makes use of equipment situated on an EU Member State (Article 29 Data Protection Working Party, 2008).

In this paper, we make the assumption that the Data Protection Directive applies to providers of social networking services, whose headquarters are established outside the EU[3].

The Data Protection Directive defines two basic categories of parties, which are relevant to be identified in the context of social networking services. On the one hand, there is the data subject, who is the individual to whom the personal data relate: in the case of social networking the users of the services. According to the Data Protection Directive, the individual shall be identified or at least identifiable. Anonymous individuals do not qualify as data subject in the scope of the European Data Protection legal framework. On the other hand, there is the data controller, who is a person (natural or legal), which alone or jointly with others "determines the purposes and means of the processing of personal data"[4]. The classification of a person as "data controller" is of great importance, as he exercises the decision making both on the purposes for which personal data are collected and processed, as well as on the means

to be used for a specific processing. The Data Protection Directive also foresees specific obligations for the data controllers regarding the processing of personal data, the respect of the rights of the users and their responsibility in case of breach of the law.

The definition of the data controller in social networking is a very complicated and heavily debated issue. The introduction of new communication channels in the Web 2.0 era facilitates interactive information sharing and collaboration between various actors over social networking sites, who do not always fit in the traditional communications models. According to the Article 29 Working Party the providers of the social networking services are the ones who determine the means for the processing of the user data, as they provide the social networking platform and all the basic tools regarding the user management, such as the registration and the deletion of the user accounts. The providers of social networking services also determine some of the purposes for which the data will be used, especially for advertising and marketing purposes (Article 29 Data Protection Working Party, 2009). It shall also be noted that the providers of social networking services set the general frame regarding the purposes for which users can process their data and the data of their contacts and friends. Although it seems more or less clear that the providers of social networking services function as data controllers, the situation is much more complicated with regard to the users of social networking services.

4. Users of social networking services as data controllers

The users of social networking services have a high degree of choice regarding the information they disclose. They share their personal information with their contacts and friends but often they share also information of other individuals. Users may also usually decide on the specific application they use in order to reveal this information in a social networking service. Therefore, the user can be considered a data controller at least "with regards to the content he chooses to provide and the processing operations he initiates" (van Alsenoy *et al.*, 2009).

Before examining if the users of social networking services may serve as data controllers and if they must fulfil the obligations that are foreseen by the Data Protection Directive for data controllers, it must be studied whether their actions fall within the scope of the Directive. Even when processing of personal data takes place, the Directive does not apply, when the processing is done by a natural person in the course of a purely personal or household activity (commonly known as "household exemption")[5]. It is to be examined at this point whether the user of social networking services can justify that they process personal data for a purely personal activity. Recital 12 of the Data Protection Directive clarifies that such activities shall be "exclusively personal or domestic" and mentions as examples the private correspondence or the holding of records of addresses. The European Court of Justice (ECJ, 2004a, b) in its ruling on the Lindqvist case expressed its thoughts on the household exemption. The ECJ expressed the opinion that the household exemption:

> [...] must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.

The ECJ considered the publication on the internet as not falling under the household exemption, as the data are made accessible to an indefinite number of people.

Wong and Savirimuthu (2008) came also to the conclusion that it is unlikely for the household exemption to apply in the case of users of social networking services (Wong, 2008). In the context of social networking, the Article 29 Working Party considered the status of a user account as private or public as a very important element in order to define a user as data controller. In line with the argumentation of the ECJ, the Article 29 Working Party considered that when the information of a user profile can be accessed by all members of a social networking service or when the data can be indexed by search engines, then the user does not benefit from the household exemption. According to the Article 29 Working Party the same shall be the approach when the user makes no selection in accepting contacts and connects to people regardless of any possible link to them (Article 29 Data Protection Working Party, 2009). Following the argumentation of the Article 29 Working Party a user with a private profile is not a controller, if the same user opens up his profile to the public becomes a controller. And if this user decides to makes his profile private again, does he stop being a controller? And what about users who make only partial information from their profile public? In any case, it is too arbitrary to consider as the decisive criterion in order to decide on the applicability of the Data Protection Directive the mere choice of a user to make his account public or his wish to accept as many friends as possible (van Alsenoy *et al.*, 2009).

5. Data protection implications – the example of tagging

If the household exemption does not apply to the users of social networking services, besides enjoying their rights as users, they need to comply with the obligations for data controllers that are defined in the Data Protection Directive in order to ensure that the processing of personal data is compliant with the data protection legislation[6]. Therefore, the controller must ensure that the processing is fair and lawful; that only the necessary and relevant to the purposes data will be processed, that the data are kept accurate and if needed updated; that the data shall not be kept longer than necessary for the fulfilment of the purposes, that the right of the data subject regarding the processing of the personal data are respected (right of access, rectification, erasure or blocking); that the data are kept in a secure way (van Alsenoy *et al.*, 2009; Edwards and Brown, 2009).

A user that wishes to publish information about third people on his profile shall obtain, for instance, the unambiguous consent of the person before posting any information about the third person and shall remove any information relating to third persons upon their request. Currently social networking services allow the dissemination of information about other people without their consent, which is problematic in various cases.

Let us take a closer look into the popular function of tagging pictures (tagging). Tagging allows users to "tag" a person that appears on a picture uploaded to a social networking services indicating the name of the person and possibly also his e-mail address. If the tagged person is also user of the specific social networking service, he is normally allowed to remove the tag, but he is not allowed to remove the picture. However, if the person is not a registered member of the social networking service, he will have no possibility to delete the tag. The situation becomes even more complicated if we take into account that any other user of the social networking service has the possibility to "tag" faces that appear on other users' photos. Respect to the data

protection principles requires that the person who appears on a picture shall give his prior consent not only for the tagging, but also for the uploading of his picture. This means that before uploading a photo and eventually adding tags to it, a user shall acquire the consent of the persons that appear on the photo, unless he can base his actions on another ground for legitimate data processing. Failure to do so would be interpreted as violation of the obligations of the data controller under the European data protection legislation.

The negative implications for the user are obvious from such an approach. During their interaction on social networking services, the users exchange personal information and upload pictures from events they attended with their friends, usually tagging the latter. Currently social networking sites allow the dissemination of information about other individuals without their consent, which is problematic in various cases. From the example of photo uploading and tagging it becomes obvious that there is a need for further refinement of the legal obligations and rights of the users of social networking services.

6. Privacy-friendly default settings and beyond

While law and regulations are necessary in describing the proper framework for the protection of privacy, two main drawbacks still exist. Privacy is a global and multifaceted issue that needs global interventions for finding a holistic solution. However, regulatory frameworks are geographically limited, while the web is a global world without geographical limitations. Another main technological difficulty that today's researchers and developers deal with is the way of transforming these regulations into system policies using the recent technological solutions.

From the implementation point of view, the protection of user privacy falls into two main categories: security-oriented requirement engineering methodologies and privacy enhancing technologies. The former focus on methods and techniques for considering security issues (including privacy) during the early stages of system development and the latter describe technological solutions for assuring user privacy during system implementation. However, in the context of social networks a blending of solutions from both categories is used. The main issue that arises is that besides the development of new technologies aiming at privacy protection, social network service providers avoid using and applying them since they prefer to keep control of user's personal data. On the other hand, users (either acting as data controllers or simply as members of a social network) cannot choose an implementation technique for protecting their data but they are forced to choose among specific "privacy oriented" options that the social network service provider offers.

Specifically, in the context of social networking services, the providers of these services are taking steps towards revealing more private information rather than protecting it. Current privacy settings of social networking services are formulated and designed in such a way that users carry the majority of the burden for managing their privacy. A recent example is the one of Facebook, which changed the way its privacy settings operate. The new default privacy settings of Facebook (www.facebook.com/press/releases.php?p = 133917) are set in a way that most people's personal information is made far more public than in their previous privacy settings. If we keep in mind that most users skip the process of managing their privacy settings either because they "trust" the provider or because they do not realise to what extent their

personal information is endangered, Facebook's new privacy settings "have created new and serious privacy problems for users of the popular social network service" according to Bankston (2009), a senior staff attorney with the Electronic Frontier Foundation.

It is thus essential to rebalance the rights and obligations of both the providers of services and the users, to empower the user via technological tools and to create privacy-friendly default settings. The default privacy settings must protect users' personal information and not expose it. In particular, setting by default full profiles to "private" or to the user's approved contact list may reduce the risk of unwanted exposure of private information. The default setting of the user profile status to "private" should mean that the full profile cannot be viewed by anyone or at least by those not belonging to the user's contact list. A list of non-privacy oriented options should be presented and only the users will be responsible to choose which data -and to what extent- will be exposed to the rest of the social networking community.

Users shall also be able to report inappropriate behaviour of another user so as to help the providers in deactivating users who act improperly. Providers should include mechanisms for reporting inappropriate behaviour, which shall be easily accessible to the users at all times with an understandable procedure of using them. Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled shall be included (European Social Networking Task Force, 2009).

The number of internet users joining a social network raises exponentially in a daily basis. However, along with this number the percentage of privacy violations among these networks raises proportionally as well, since most users are unaware of the privacy dangers the are getting into. For this purpose, social network service providers should provide users technological solutions for protecting their private information and specific role as data controllers to control themselves how and to what extent their data will be disseminated. Social networks should provide privacy awareness methods for their users and offer them a number of tools so as to be able to form their own privacy policy always ensuring that it is based on the respective legal and regulatory framework. Social network service providers must provide the tools for the handling of every piece of private user information, as the only responsible for the private data set is the respective data subject.

7. Conclusions

Social networking is one of the most remarkable cultural phenomena that blossomed in the Web 2.0 era. They enable the connection of users and they facilitate the exchange of information among them. However, the users reveal vast amounts of personal information over social networking services, without realising the privacy and security risks arising from their actions. The European Data Protection legislation could be used as a means for protecting the users against the unlawful processing of their personal information, although a number of problems arising regarding its applicability.

The European Commission set up in April 2008 a European Social Networking Task Force in the context of its safer internet programme (http://ec.europa.eu/information_society/activities/sip/index_en.htm). Main goal of this task force was the development of guidelines for the use of social networking services by children (European Social Networking Task Force, 2009). These guidelines are currently

voluntarily adopted by 17 leading social networking services, such as Facebook, Bebo and MySpace[7] and will be evaluated a year after their adoption, i.e. in February 2010. In this way, the European Commission promoted a solution of self-regulation in a first attempt to protect the minor users of social networking services.

Notes

1. Under Article 29 of the Data Protection Directive, a Working Party on the protection of individuals with regard to the processing of personal data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.
2. Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereinafter the "data protection directive", O.J. L 281/31, 23.11.1995.
3. For an analysis of the applicability of the Data Protection Directive in the context of search engine providers with similar argumentation applicable to social networking services providers see Kosta *et al.* (2009).
4. Article 2 (d) Data Protection Directive.
5. Art. 3(2) 2nd indent Data Protection Directive.
6. For a comprehensive analysis of the obligations of the data controller see Kuner (2007).
7. A full list of the signatories and their self-declarations are available at: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl

References

Anderson Analytics (2009), "Social network service (SNS) A&U profiler", *eMarketer*, available at: www.emarketer.com (accessed 13 July 2009).

Article 29 Data Protection Working Party (2008), "Opinion on data protection issues related to search engines" (WP 148, 4 April 2008).

Article 29 Data Protection Working Party (2009), "Opinion 5/2009 on online social networking" (WP 163, 12 June 2009).

Bankston, K. (2009), *Facebook's New Privacy Changes: The Good, The Bad, and The Ugly*, EFF Deeplinks Blog. available at: www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly (accessed 9 December 2009).

Data Protection and Privacy Commissioners (2008), "Resolution on privacy protection in social network services", paper presented at 30th International Conference of Data Protection ad Privacy Commissioners, October 2008.

ECJ (2004a), *C-101/01, Bodil Lindqvist*, European Court of Justice, Luxembourg, available at: www.curia.europa.eu (accessed 6 November 2003).

ECJ (2004b), *O.J. C 7/3*, European Court of Justice, Luxembourg, available at: www.curia.europa.eu (accessed 10 January 2004).

Edwards, L. and Brown, I. (2009), "Data control and social networking: irreconcilable ideas?", *Matwyshyn Andrea Harboring Data*, Stanford University Press, Stanford, CA, pp. 202-27.

ENISA (2007), *Security Issues and Recommendations for Online Social Networks*, The European Network and Information Security Agency, Heraklion.

European Social Networking Task Force (2009), *Safer Social Networking Principles for the EU*, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf (accessed 10 February 2009)

Facebook (2009), "Facebook asks more than 350 million users around the world to personalize their privacy", press release, www.facebook.com/press/releases.php?p=133917 (accessed 9 December 2009).

IWGDPT (2008), *Report and Guidance on Social Network Services – Rome Memorandum*, International Working Group on Data Protection in Telecommunications.

Kosta, E., Kalloniatis, C., Mitrou, L. and Kavakli, E. (2009), "Search engines: gateway to a new "Panopticon"?", in Fischer-Hubner, S., Lambrinoudakis, C. and Pernul, G. (Eds), *Trust, privacy and Security in Digital Business, 6th International Conference, TrustBus, Linz, Austria, Proceedings LNCS*, Vol. 5695, Springer, Heidelberg, pp. 11-21.

Kuner, C. (2007), *European Data Protection Law – Corporate Compliance and Regulation*, 2nd ed., Oxford University Press, Oxford.

van Alsenoy, B., Ballet, J., Kuczerawy, A. and Dumortier, J. (2009), "Social networks and web 2.0: are users also bound by data protection regulations?", *Identity in the Information Society*, Vol. 2 No. 1, pp. 65-79.

Wong, R. (2008), *Social Networking: Anybody is a Data Controller*, Nottingham Law School, working paper, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668 (accessed October 2008).

Wong, R. and Savirimuthu, J. (2008), "All or nothing, this is the question: the application of Article 3(2) data protection directive 95/46/C to the internet", *The John Marshall Journal of Computer & Information Law*, Vol. 25 No. 2, pp. 241-66.

Corresponding author
Eleni Kosta can be contacted at: eleni.kosta@law.kuleuven.be