Privacy Settings in Social Networking Sites: Is It Fair?*

Aleksandra Kuczerawy and Fanny Coudert

Interdisciplinary Centre for Law & ICT (ICRI) – K.U. Leuven – IBBT,
Sint-Miechielsstraat 6, 3000 Leuven, Belgium
aleksandra.kuczerawy@law.kuleuven.be,
fanny.coudert@law.kuleuven.be

Abstract. The present paper examines privacy settings in Social Networking Sites (SNS) and their default state from the legal point of view. The analysis will be conducted on the example of Facebook as one of the most popular –and controversial- SNS and one of the most active providers constantly amending its privacy settings. The paper will first present the notion of privacy settings and will explain how they can contribute to protecting the privacy of the user. Further on, this paper will discuss the general concerns expressed by users and data protection authorities worldwide with regard to the changes of Facebook's privacy settings introduced in February 2010. Focus will be put on the implementation of the fairness principle in SNS. This principle implies that a person is not unduly pressured into supplying his data to a data controller, and on the other hand that the processing of personal data is transparent for the data subject.

Keywords: Social Networking Sites, privacy, data protection, privacy settings, fairness principle.

1 Introduction

In 2009 a Canadian lady lost her health benefits when her insurance company discovered 'happy' pictures of her on her Facebook profile. She was on a sick leave due to a long term depression and following an advice of her doctor, she was trying to get engaged in fun activities. Pictures of her smiling on a beach in Cancun or during a night out were taken by her insurance company as a proof that she is no longer depressed and able to work. Although the company did not confirm that the decision was taken solely on the basis of the pictures it admitted that it uses the popular site to investigate clients [1].

* Part of the research leading to these results has received funding from the European Community's Seventh Framework Program (FP7/2007-2013) under grant agreement n° 216483 (PrimeLife) and n° 248726 (+Spaces). The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

S. Fischer-Hübner et al. (Eds.): Privacy and Identity 2010, IFIP AICT 352, pp. 231–243, 2011.

Stories like this do not surprise anybody anymore as every few days there is a new one appearing in the news. With the explosion of the social networking tsunami the level of private life's exposure has dramatically increased within a short period of time [2]. In views of Mark Zuckerberg, the founder of Facebook, 'people have really gotten comfortable not only sharing more information and different kinds but more openly and with more people, and that social norm is just something that has evolved over time' [3]. The increase of public exposure Internet users seem to be willing to accept does not however always reflect a conscious choice, but can rather be explained by the false sense of intimacy given by the computer. The amount of highly personal data voluntarily posted by users on social network sites is enormous. Most of accounts on social networks contain data like birth names and dates, addresses, phone numbers, and pictures as well as 'sensitive' data such as sexual preferences, relationship status, political views, and health information. What is astonishing is the fact that users very often do not realize the consequences of making that much information available to the public, or to other unintended recipients such as parents, teachers, employers and many others. Important work in raising privacy awareness of users is done by increasing media coverage of privacy violations in social networks. However, cases such as the ones mentioned above prove how fragile this awareness still is.

It goes without saying that different people have different ideas on how much information they want to share with their friends, or how much information they want to hide from some of their contacts. After all, Facebook makes use of Internet a means of socialization. We shall however not forget that what is called Friendship within Facebook environment is not always the same as friendship in the off-line world. The contact list of almost every user is full of real friends, but also of acquaintances, colleagues from work, ex-lovers, friends of friends, and sometimes even people they do not really know. This compilation of different types of contacts often leads to an oversharing of information. Allowing equal access to all information on the profile to all contacts frequently results in unwanted disclosures for example when a grandma sees pictures from a drinking game at a college party [4] or when an employer finds out through a post that a sick leave is actually a nice time off in some exotic resort.

In the off-line world people function within different social contexts and roles. For each of those contexts (e.g. e-government, e-commerce, social networks, etc.) and roles (e.g. citizen, consumer, friend, student, employee, etc.) individuals assume different partial identity [5]. According to those contexts, roles and identities they also adjust their behaviour. Such segregation of the contexts, or of the targeted audience, prevents discrediting one role by the information related to another [5] [6]. To some extent this is also possible in SNS[1]. Just like we create different personas to interact at work and within the closest friends group, we can create different personas on the Facebook profile by creating lists of contacts and adjusting visibility of the profile depending on which persona we want to show to a different group [4].

All examples mentioned above show that most of conflicting situations occur when information posted online is taken out of context because addressed to the wrong recipient. Perfectly admissible behaviours in a close friends' environment may become totally inappropriate in a work environment. In the off-line world people

[1] Such segregation was done in the EU funded project PrimeLife, in the prototype application called Clique. See more at: `http://clique.primelife.eu`, and in [5].

learn to manage these subtle barriers by adjusting their behaviour to each situation. That way, they can reveal only a part of oneself in a certain context, and show different face in another context [6]. This social ability, however, seems to be a struggle to reproduce in online environments. Social networking sites, as socialization platforms, need to address these concerns and empower their users to reproduce their off-line behaviour in an online environment. This has given way so far to the emergence of technical tools that enable increased granularity in the information disclosed, often designated under the term of "privacy settings". However, privacy settings have often been criticized for not being easy to manage by users, requiring a complex learning process, and for serving other needs proper to the SNS provider not always in the benefit of users. The business model SNS currently rely on, the free advertisement-based model proper to Web 2.0 environments, push service providers to encourage users to make the more information publicly available to feed, amongst others, their advertisers' and third parties applications' needs. We explore in this paper whether the confusion created by not always transparent privacy settings, in addition to regular changes, complies with the fairness principle within the meaning of the 95/46/EC Data Protection Directive (hereinafter DPD).

The analysis presented in this paper is conducted on the example of Facebook, as the most popular –and controversial- SNSs worldwide. With 500 million active users [7], Facebook is also the most media-present SNS, and the recognition it gets is not always for positive reasons. Frequent changes of the privacy policy are always highly commented by users, journalists, watchdog organizations and regulators. For these two reasons Facebook constitutes a one of a kind case study providing enough stories to create its own 'shame chronicles'. Actually, testimonials of the most embarrassing posts and photos are already collected by independent sites like for example Lamebook [8] – a regularly updated proof of users' low privacy awareness. Despite the fact that this paper focuses specifically on Facebook's privacy architecture, the main question of the paper applies to all other SNSs which use the function of 'privacy settings' - a technical tool designed to allow users to control the amount of information they reveal on their SNS profile. Finally, because of the large popularity of Facebook both in the US and in the EU, similar concerns have arisen in both regions, leading to a common search for the best solution on how to tackle the problem.

2 Privacy Settings – Trick or Treat?

2.1 Privacy Settings: Empowering Users to Manage the Information They Share

Privacy settings, present in most of the major social networking sites can be used by the user to adjust the visibility of their profile or of certain information on the profile. As a result, this could eliminate a certain amount of unwanted disclosures and upgrade the level of privacy of the profile. It is however not clear whether users are actually making use of their privacy settings. Some surveys show that very few users decide to change their privacy preferences. Only 20% of them ever touch their privacy settings, according to Facebook Chief Privacy Officer Chris Kelly [9]. A study conducted in 2007 by a security firm confirmed that 75% of users never

changed the default settings [10]. Some of them are not even aware that it is possible. By contrast, other surveys appoint toward a greater use of privacy setting. Two Pew Research Center studies showed that 66% of teenagers and 60% of adults restrict access to their profiles so that only friends can view it [11].With the help of media, significant attention is given to the risks and benefits of privacy settings. It is in any case undeniable that after numerous articles about undesired effects of oversharing, including examples of disciplinary problems of college students, criminal charges pressed, evidence found for divorce cases and lost jobs, users start to realize that 'everything you post can be used against you' [12]. Thanks to these stories, SNS users are more often aware that they are able to adjust their profile and its visibility to better match their needs. The effectiveness of this type of warning can be seen in a growing trend to protect Facebook profiles by changing display names and tightening privacy settings to hide photos and wall posts [13].

Solutions therefore appoint towards an increase of users' awareness about the use of privacy settings, which should be sufficiently clear and granular to empower users to better manage the information they disclose by distinguishing between the recipients of this information – as they do in the off-line world.

Facebook actually offers a large amount of options to its users in the privacy settings to discriminate the recipients of the information uploaded. First of all, they can hide their profile from the public and make it visible only to their friends. Next, they can hide it from search engines, so their profile will not be indexed and will not come up in a Google or other search engine. Another option is a possibility to customize the visibility of certain parts of the profile by adjusting it according to the various audiences of the profile. Such audience segregation can be made by creating lists and grouping contacts depending on a type of relationship, or a level of intimacy. Facebook offers highly granular options in the privacy settings, which allow to adjust a specific visibility for each photo album, separate photo, and even for separate post. What is more, it offers also a possibility to control what a particular contact can see by impersonating that person and seeing the profile from his perspective [4][14]. The 'view as…' function is described as a type of a "privacy mirror" technology which provides a "useful feedback to users by reflecting what the system currently knows about them" [14], or in this case, what other users know about them.

2.2 Limited Uses of Privacy Settings

Why, despite all the possibilities to control the level of the information disclosure, are there still so many privacy incidents happening on Facebook? With such a powerful and highly granular technical tool, which allows specifying access controls different for each contact, it should be a very popular tool among the users. It enables them to avoid a decontextualisation of the information posted online. According to H. Nissenbaum, all arenas of life constitute contexts that are governed by norms of information flow, and the problems occur when individuals inappropriately transmit information and collapse contexts [15]. She identifies the lack of "contextual integrity" as the main reason of the privacy problems on SNS. Used as an impression management system, privacy settings can definitely allow users to regain the control over their information and eliminate most of the unwanted situations. It is however still not commonly used or understood, and it is often seen as a 'mysterious' part of

the profile. A reason for this could be that generally, regulating social behavior by technology seems to be problematic [5] [16].Some commentators, like Grimmelman, argue of social aspects, such as the fact that it is "deeply alien to the human mind to manage privacy using rigid *ex ante* rules" [16]. This of course depends on the manner it is conducted. Grimmelman was referring to a specific scenario when SNS providers design the entire complexity of social relationships for the users to group their contacts into [16]. Such approach indeed seems to be pointless as it is the users who should describe the categories of contacts they need [5]. An example of a successful attempt to use technology to allow users to segregate their audience groups can be found for example in the EU project PrimeLife and its prototype application Clique. According to Nissenbaum, a general reason why privacy settings are not used as often as we would expect, should be found in that people think about privacy in terms of social roles and not in terms of access-control lists and permissions [15][16].

Another likely explanation is that the privacy settings offered by Facebook are just too difficult to use. Numerous studies show that average users are often confused about them and about the final effects of their choices [17][18]. Most of them simply get lost between all the options. It is a sign that complex interfaces, when not explained properly, can be worse for privacy then less detailed ones [16]. According to Peterson, "superbly powerful and precise technical controls would be too unwieldy and difficult for anyone to use" [4]. It would be a shame however to throw the baby with the bathwater – but is the reconciliation of complexity and simplicity possible? This leads us to the core question dealt with by this paper, namely, whether the tool itself is designed to actually facilitate privacy management.

2.3 The Dark Side of Facebook's Improved Privacy Settings: Increased User's Visibility

Since the changes introduced in December 2009 and later in March 2010, it is hardly contestable that Facebook provides tools to adequately manage one's posts. Significant attention to the subject of privacy settings was firstly brought by the highly commented, and equally criticized amendments of privacy settings of Facebook from December 2009. According to Facebook officials, the introduced change provides more control to users and makes the privacy settings section more clear and user-friendly. This however did not manage to stop the flow of criticism by users and privacy organizations [19].

The improvement in privacy setting's management came with an increase of the data made publicly available by default. The introduced changes allowed access not only to friends or friends of friends, but to every Facebook user [20]. Moreover, such state was actually marked by Facebook as the "recommended" one, and had to be un-clicked to limit access to the profile. Another change introduced in December 2009 was the indexing of users' profiles in search engines. This as well was pre-selected and hidden in one of the sections of privacy settings, in a way that most of users did not realize they had to look for it and deselect it themselves. After a series of negative comments backed up by disappointed users whose mistrust was growing fast, ten major privacy groups filed a complaint to US Federal Trade Commission [21]. The complaint argued that the introduced privacy settings "violate user expectations, diminish user privacy, and contradict Facebook's own representations" [22]. The

response to this complaint is still to be seen but the amount of media attention reminds of what happened with Facebook Beacon[2], when massive protest led to its bitter end. This proves that the protests of the users can actually have a positive result and influence behaviour of SNS providers.

Despite critical reception of the mentioned changes Facebook did not hesitate to introduce even more 'improvements' in April 2010. Since then, a group of previously selected third parties is allowed to access users' accounts. This time again, the relevant box in privacy settings was pre-selected by default. The new feature, called 'Instant Personalization' allowed three outside partners of Facebook: Pandora, Yelp, and Microsoft Docs to access users' profiles. In order to disallow the feature users had to dig out the appropriate field and deselect it, and then block each site separately to make sure that no information is shared through profiles of friends who have not disabled this feature. This activity was complicated and only possible if a user knew what exactly he was looking for, and where. Introduction of the Instant Personalization and the manner in which it was done resulted in another complaint to FTC [23][24][25]. One of the arguments of the complainants was that Facebook's "privacy settings are designed to confuse users and to frustrate attempts to limit the public disclosure of personal information that many Facebook users choose to share only with family and friends"[26]. Facebook had, for instance, effectively concealed the process of disabling the feature, and only with the information provided by numerous outside articles could the users oppose to such processing [26][27].

Looking at the introduced changes, three groups of unwanted disclosure can be distinguished. First, data can be disclosed by Facebook to third party service providers. Second, users' data can be disclosed by making profiles public by default. Third, data can be disclosed inadvertently by users themselves. For instance, a user with a private profile might still share information with a broader audience than intended by failing to restrict access appropriately (e.g. due to the complexity of and/or technical difficulties surrounding the reconfiguration of privacy settings). Whereas in the first case, Facebook actively provides users' data to third parties, in the other two cases, the intervention of Facebook is more subtle. Users are apparently the ones empowered to share (or not) their information by managing their privacy setting, i.e. the tools put at their disposal to that effect by Facebook. However, as shown above, by designing the tool in such a complex fashion, and by marking some options by default or recommending specific configurations, Facebook can covertly influence users' behavior. As Grimmelman warns, "users are voluntarily, even enthusiastically, asking the site to share their personal information widely" [16]. It is however not clear to what extent they do so consciously, and when they are driven by Facebook privacy settings configuration. In the end Facebook needs users to make their data public to compete with other platforms such as Twitter[3] and feed the needs

[2] In 2007 Facebook introduced its new feature called 'Beacon'. Facebook formed partnerships with third party retailers which allowed it to obtain information about users' activities on these partner businesses and publish information about these activities in a way that would be publically visible. See more on: Facebook Halts Beacon, Gives $9.5M to Settle Lawsuit, PC World, 8 December 2009, http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_95m_to_settle_lawsuit.html; RIP Facebook Beacon, Mashable – The Social Media Guide, 19 September 2009, http://mashable.com/2009/09/19/facebook-beacon-rip/

[3] http://www.insidefacebook.com/2009/12/15/is-facebook-sacrificing-its-privacy-legacy-for-an-open-future/

of its advertisers and third parties applications. “Member-created data is the lifeblood of Facebook” [28]. "Facebook, and everybody else, uses all this data for marketing and advertising purposes," and "that's where it complicates things. Because our information, the public's information, is being sold left and right and reused for advertising purposes" [28]. Letting aside concerns raised by behavioural advertising that base web 2.0 successful entrepreneurs, question arise whether Facebook could be held liable for unclear privacy settings that push users to make their information publicly available, irrespective of the way how Facebook makes use of this information.

3 Looking for More Fairness in the Design of Privacy Settings: Is Privacy the Way through?

3.1 The Fairness Principle under the Data Protection Directive

The DPD requires that all processing of personal data must be fair (Article 6.1.a) [29]. The concept of fairness as such is not however further defined and should be looked for in other provisions of the text.

First of all, fairness means that data processing must be transparent to the data subject. Recital 38 of the DPD indicates that if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection. Strict compliance with the provisions contained in Articles 10 and 11 of the DPD about the information to be provided to data subjects seems crucial to ensure the transparency of the data processing. This requirement is however most often provided through long privacy policies written with the clear aim of protecting the company against potential lawsuits, rather than with the intention of providing clear and readable information to the data subject. Facebook does not escape this trend and the length of its privacy policy is often compared to the US constitution, which is shorter in number of words [30]. This phenomenon has already led data protection authorities, for instance in the case of collection of information from minors, to require that information should be provided in a clear and comprehensible way, taking into account the final recipient of the information. For example the Safer Social Networking Principles for the EU principles requires providers to “create clear, targeted guidance and educational materials designed to give children and young people the tools, knowledge and skills to navigate their services safely” [32]. Information designed for this group of users “should be presented in a prominent, accessible, easy-to-understand and practical format” [32].

Fairness also means that data subjects should not be unduly pressured into supplying their data to a data controller or accepting that the data are used by the controller for particular purposes [31]. This suggests a guarantee of certain protection to data subjects, whenever they are the weaker party in the relation, from abuse by data controllers of their monopoly position [31]. Fairness therefore means in this context that the consent provided to the data processing should be free in a way that users are not tricked into providing data. This was for instance one of the points of the investigation of Facebook by the Canadian Data Protection Authority [40]. During the investigation it became

evident that while consenting to use a third party application users were granting a virtually unrestricted access to their personal information. This forced Facebook to introduce changes to this practice. Currently, application providers must inform users about the categories of data they need to run the application and to seek prior consent from users [41].

Finally, a third implication of the concept of fairness could be found in the obligation for data controllers to take into account the interests and reasonable expectations of data subjects when processing their personal data. In other words, it means that "controllers cannot ride roughshod over the latter" [31]. As Bygrave explains, the collection and processing of personal data must be performed in a way that does not intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity [31]. In this sense, Grimmelmann observed that Facebook sudden changes in its privacy policy, and in the amount of information publically available by default "pulled the rug out from under users' expectations about privacy"[16].

3.2 The Approach of European Bodies

The Art.29 Working Party[4] and the European Commission have so far mainly tackled the problem of (lack of) fairness in Facebook's privacy settings advocating for the implementation of privacy-friendly default settings and the preference of opt-in rather than opt-out procedures.

The 2009 Pact on Safer Social Networking Principles for the EU first paid significant attention to the role of privacy settings. The document introduced specific principles recommending users' empowerment through tools and technology, or enabling and encouraging users to employ a safe approach to personal information and privacy [32]. Despite being a non-binding Code of conduct, it formally engaged Facebook to improve its privacy settings. However, the Pact was limited in its scope only to services targeted at minor users.

Following the Pact, Art. 29 Working Party issued an opinion on social networking in June 2009 [33]. In this document the Working Party stressed the importance of clear privacy settings to empower users to consent to the disclosure of his or her information beyond the members of their contact list. According to the Working Party "SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties"[33].

In February 2010, in reaction to the changes operated by Facebook in December 2009, the European Commission announced its plans to take an action and address the amendments introduced by Facebook in a broader scope [34]. Following this announcement, a letter was sent to Facebook by Art. 29 WP in May 2010. In the letter

[4] 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 as an advisory body. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection issues.

the Working Party underlined the importance of privacy friendly default settings and called for maximum of control by the user over who has access to his profile information and connections lists. It also stressed that any access by people beyond the members of contact lists should be an explicit choice by the user. Art. 29 WP therefore called for the generalization of opt-in procedures. The big concern was expressed about the effect that the changes may have on the use of Facebook by minors and a possibility of exposing them to severe threats by allow public access to their profiles. However, it was strongly highlighted that such control should be provided to users regardless of their age. In this context, the changes of Facebook default privacy settings were called unacceptable [35] [36].

3.3 Limits of the Privacy Approach

In the presented context, could we consider that Facebook complies with the fairness principle as outlined under the data protection framework? In the light of the last changes in the privacy settings that empower users to manage their online identities, the answer may not be that straightforward. Facebook tried to turn the privacy setting into a more friendly design, tackling most parts of the concerns raised by European bodies. At the same time, these improvements came with features inciting users to make more information public through the use of recommendation and opt-out procedures. It is not certain whether requiring Facebook to implement opt-in procedures would really change the situation. Such procedures are often presented to users in a way as to encourage them to make their information public.

As mentioned above, the business model of Facebook (free, advertisement based) does not provide sufficient incentives to force the company to better protect users' rights. Some commentators observed that their business model "forces them to leverage the size of the network, instead of monetizing on individual user value", putting them "in a balancing act where the advertisement capabilities need to outweight the individual user rights in order to keep a decent revenue stream" [37].

Another issue may stem from the design of the platform. As suggested by Bygrave, fairness should not only refer to informing about a specific data processing activity but rather, it should apply to the design and the structure of the information system supporting such operations. This would suggest that not only individual processing operations have to be fair but the whole system, also from the technical perspective, should be designed with underlying fairness principle. After all, since Lessig's introduction of the code concept, it's been already argued by various authors that adjusting software can be a far more effective privacy-protection mechanism than for example adjusting the text of contractual privacy policies, simply because that conditions of the code cannot be 'breached' [38]. According to Edwards and Brown, privacy is determined by the default settings coded into the software by the designers of the SNS [38]. More concretely, this means that SNS software, which defines what users can do with their data – so in our case the privacy settings, is not always consistent with the users' expectations. Edwards and Brown argue that "users are (…) often mislead as to what their 'reasonable expectation of privacy' are on an SNS by the way the code has been written and defaults set" [38]. Users mainly join Facebook to share information with their social network and communicate with their friends. It is clear that any 'reasonable' user, when he joins free services like Facebook, usually

expects that he may receive some ads to make it worthwhile to the service provider [38]. However, he probably does not expect though that access to his account will be given to unrelated service providers, or to all the people he is not friends with and that his information will be possible to find through search engines [38].

It seems that the main problem lays in "reconciling reasonable user expectations of data security and privacy with the 'disclosure by design' paradigm concerning personal data on SNSs" [38]. It is however not clear whether the actions undertaken by European bodies, mainly consisting in a set of recommendations, will form sufficient incentives to Facebook to introduce greater fairness in the design of privacy settings. A more promising solution may be found in the concept of unfair commercial practices. Such approach has been used in the complaints to the Federal Trade Commission lodged by the US privacy groups against the new privacy settings of Facebook. In these complaints the activities of Facebook were qualified as unfair and deceptive trade practices [26]. It is hence worth investigating whether a similar approach could be adopted in Europe. The Unfair Commercial Practices Directive [39] sanctions misleading commercial practices. An action is misleading if it contains false information and is untruthful or in any way deceives the average consumer (even if the information is factually correct) and causes him to take a transactional decision that he would not have taken otherwise. Information could also be misleading if it refers to either the nature of the product or, for example, benefits, risks, the results to be expected from its use, or the motives for the commercial practice [39]. Providing information in an unclear, unintelligible, or ambiguous manner may also qualify as misleading behavior. Finally, omissions can be misleading if the information omitted, or hidden, is the one that average consumer needs. Facebook's practices as regard privacy setting could possibly fall under this definition. Users would then be able to benefit from the protective Consumer law framework often supported by consumer organizations which have the resources and means to challenge unfair practices before Courts.

4 Conclusion

Facebook and its privacy settings are frequent guests in the news but they rarely get positive reviews. From what was said above, it can be seen that privacy settings can play a great role in privacy protection and give users a control over their information shared through SNS. It is clear that a necessary tool to prevent situations like the one mentioned at the beginning is already out there. The whole problem is the way the tool is used (or not used) by users, which is mainly a result of ambiguity of the privacy settings and the confusion stemming from regular changes. Users' unawareness together with complexity of the tool and lack of transparency are the three major factors shaping the current privacy challenging situation. Some dubious practices, like making profiles publically available on an opt-out basis or offering third parties access to the users' accounts, seriously undermine Facebook's attempts to convince the public that it designs its system with users' privacy in mind. At the same time, a closer look at Facebook business models strongly suggest that confusing users with information about available options in privacy settings is intentional as its commercial profit depends on the amount of disclosed users' data.

The fairness principle of the DPD indicates what should be a direction for all SNS providers to take. It also shows that users' expectations towards privacy cannot be

ignored and have to be always taken into account. However, this does not seem to be enough to make Facebook change its ways. The alternative solution could lay in unfair trade practices regulation. With much more developed doctrine on what is unfair, and with actual means to enforce it, this could be a way to assure more privacy on SNS. Using the 'consumer protection' approach is tempting because many SNS users, just like many consumers, are so technology-ignorant or vulnerable that some public protective measures should be extended [38]. It is a particularly relevant argument if we consider the amount of children and young people without necessary experience among the SNS users. The 2005/29/EC Directive contains provision about enforcement of its rules and it urges Member States to introduce penalties for infringements of national rules on unfair trade practices. Such penalties, which must be effective, proportionate and dissuasive, if used against SNS provider involved in unfair practices in the described context could be a way to ensure more privacy to the users of these services. This could be an alternative path to effectively achieve more privacy through a different set of rules and therefore it should be investigated further on.

References

1. Canadian Woman Loses Benefits over Facebook photo, http://abcnews.go.com/International/wireStory?id=9147300
2. Privacy chiefs keep watch over Facebook, http://www.reuters.com/article/idUSTRE63L0UB20100422
3. Facebook's Zukerberg Says the Age of Privacy is Over, ReadWriteWeb, January 9 (2010), http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php
4. Peterson, C.: Losing face: an environmental analysis of privacy on Facebook, draft paper (January 2010), http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=cpeterson
5. Leenes, R.E.: Context is everything: sociality and privacy in Online Social Network Sites. In: Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G. (eds.) Privacy and Identity. IFIP AICT, vol. 320, pp. 48–65. Springer, Heidelberg (2010)
6. Goffman, E.: The presentation of self in everyday life. University of Edinburgh, Edinburgh (1956)
7. Facebook Statistics, http://www.facebook.com/help/?ref=drop#!/press/info.php?statistics
8. http://www.lamebook.com (last checked on 01.07.2010)
9. Stross, R.: When Everyone's a Friend, Is Anything Private?, N.Y. TIMES, March 7 (2009), http://www.nytimes.com/2009/03/08/business/08digi.html
10. Sophos ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves, SOPHOS, August 14 (2007), http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html
11. As referred by EPIC in the complaint submitted to the FTC on the matter of Facebook, INC, May 5, 2010: Pew Internet and American Life Project, Teens, Privacy, and Online Social Network, http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1, Pew Internet and American Life Project, Social Networks Grow: Friending Mom and Dad, January 14 (2009), http://pewresearch.org/pubs/1079/social-networks-grow

12. Nelson, S., Simek, J., Foltin, J.: The Legal implications of Social Networking. 22 Regent U. L. Rev. (2009)
13. Goldberg, S.: Young job-seekers hide their Facebook pages, CNN Tech, March 29 (2010), http://www.cnn.com/2010/TECH/03/29/facebook.job-seekers/index.html
14. Hong, J., Iachello, G.: End-User Privacy in Human–Computer Interaction. Foundations And Trends In Human–Computer Interaction 1(1) (2007)
15. Nissenbaum, H.: Privacy as contextual integrity. 79 Wash. L. Rev., 119 (2004)
16. Grimmelmann, J.: Saving Facebook. 94 Iowa L. Rev., 1185 (2009)
17. Acquisti, A., Gross, R.: Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Danezis, G., Golle, P. (eds.) Privacy-Enhancing Tech.: 6Th Int'L Workshop, vol. 36 (2006), http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf
18. Livingstone, S.: Taking Risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy ad self-expression. New Media and Society 10 (2008)
19. The Facebook Privacy Fiasco Begins, TechCrunch, December 9 (2009), http://www.techcrunch.com/2009/12/09/facebook-privacy/
20. Facebook's New Privacy Changes: The Good, The Bad, and The Ugly, Electronic Frontier Foundation, December 9 (2009), http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly
21. Privacy groups file FTC complaint against Facebook, Guardian, December 17 (2009), http://www.guardian.co.uk/technology/blog/2009/dec/17/facebook-privacy-ftc-complaint
22. Ten Privacy Groups File FTC Complaint Against Facebook for Recent Privacy Changes, Inside Facebook, December 17 (2009), http://www.insidefacebook.com/2009/12/17/ten-privacy-groups-file-ftc-complaint-against-facebook-for-recent-privacy-changes/
23. Paul, I.: Facebook privacy complaint: a complete breakdown, PC World, May 6 (2010), http://www.pcworld.com/article/195756/facebook_privacy_complaint_a_complete_breakdown.html
24. Hachman, M.: Facebook targeted by new FTC privacy complaint, PCmag, May 7 (2010), http://www.pcmag.com/article2/0,2817,2363518,00.asp
25. Kafka, P.: Feds to Facebook privacy critics: let's talk, All Things Digital, January 19 (2010), http://mediamemo.allthingsd.com/20100119/feds-to-facebook-privacy-critics-lets-talk/
26. For the full text of the complaint see, http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf
27. Paul, I.: Facebook's new features and your privacy: what you need to know, PC World, April 23 (2010), http://www.pcworld.com/article/194866-3/facebooks_new_features_and_your_privacy_what_you_need_to_know.html
28. McCarthy, C.: press release, Facebook's privacy policies hit a language barrier, CNET News.com on July 12 (2010), http://www.zdnetasia.com/facebook-s-privacy-policies-hit-a-language-barrier-62201276.htm
29. Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) (OJ L 281, 23.11.1995)

30. Rosen, J.: The Web Mean the End of Forgetting, New York Times, July 19 (2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=3&pagewanted=1&hp
31. Bygrave, L.A.: Data Protection Law, Approaching its rationale, logic and limits (2002)
32. Safer Social Networking Principles for the EU, http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
33. Art. 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, adopted on 12 June (2009)
34. EU to slam new Facebook privacy settings: http://www.euractiv.com/en/infosociety/eu-slam-new-facebook-privacy-settings
35. EU Watchdog slams Facebook's privacy settings, http://www.euractiv.com/en/infosociety/eu-watchdog-slams-facebook-privacy-settings-news-494168
36. Letter of Art. 29 Wp to Facebook, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2010_05_12_letter_art29wp_facebook_en.pdf
37. Vanelsas, A.: The Facebook business model is the root cause of a lack of transparency, February 18 (2009), http://vanelsas.wordpress.com/2009/02/18/the-facebook-business-model-is-the-root-cause-of-a-lack-of-transparency/
38. Edwards, Brown, I.: Data Control and Social Networking: Irreconcilable Ideas? In: Matwyshyn, A. (ed.) Harboring Data: Information Security, Law and the Corporation, vol. 226 (2009)
39. Directive 2005/29/EC of the European Parliament and of the Council of May 11, 2005, concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (2005)
40. Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act, http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm
41. Gross, G., McMillan, R.: Canada ends Facebook privacy probe, Computerworld, September 22 (2010), http://www.computerworld.com/s/article/9187381/Canada_ends_Facebook_privacy_probe?source=CTWNLE_nlt_security_2010-09-23