

Nothing to hide? The need for simple, transparent and reliable privacy settings on Facebook

Abstract

Facebook, the most popular website in the United States, faces heavy complaints because of its unclear privacy policy and privacy settings. Facebook currently has 50 settings with more than 170 options, making it increasingly difficult for its users to find the appropriate settings. While the debate about protecting privacy has not yet reached a definitive conclusion, this paper identifies four moral reasons to protect privacy. One of these moral reasons leads to the theory about spheres of access: a user's information may only be shared with those in the sphere, and the information may not be transferred across the boundaries of the sphere. Using two examples this theory is applied to Facebook, which leads to a clear need for simple, transparent and reliable privacy settings. Finally, a solution of a single privacy control with the option to fine-tune detailed settings is proposed.

Introduction

Facebook is one of the most popular social network sites today and the most popular website in the United States – even more popular than Google (Nuttall and Gelles 2010). Its popularity is based on its user base and, more importantly, on the amount of information those users share with their friends and the rest of the world. This sharing of information fuels the debate about Facebook's privacy policy and privacy settings, so much even that several American privacy organizations recently filed a complaint against Facebook before the Federal Trade Commission, stating that Facebook "violate[s] user expectations [and] diminish[es] user privacy" (EPIC 2010). Facebook responded to the recent discussion by announcing that the website would review its privacy policy (NRC Handelsblad 2010).

A review of Facebook's privacy policy and settings would be one of many in recent years. As Figure 1 clearly shows, the amount of information that is made public by the default privacy settings of Facebook has grown tremendously in the past five years. Furthermore, Facebook's privacy policy is now lengthier than the United States Constitution without amendments (The New York Times 2010). At the same time, Facebook has also given users more freedom to determine how much information is to be made public, but the amount of privacy settings is now so large – 50 settings with more than 170 options (The New York Times 2010) – that it becomes increasingly difficult for users to find the appropriate settings.

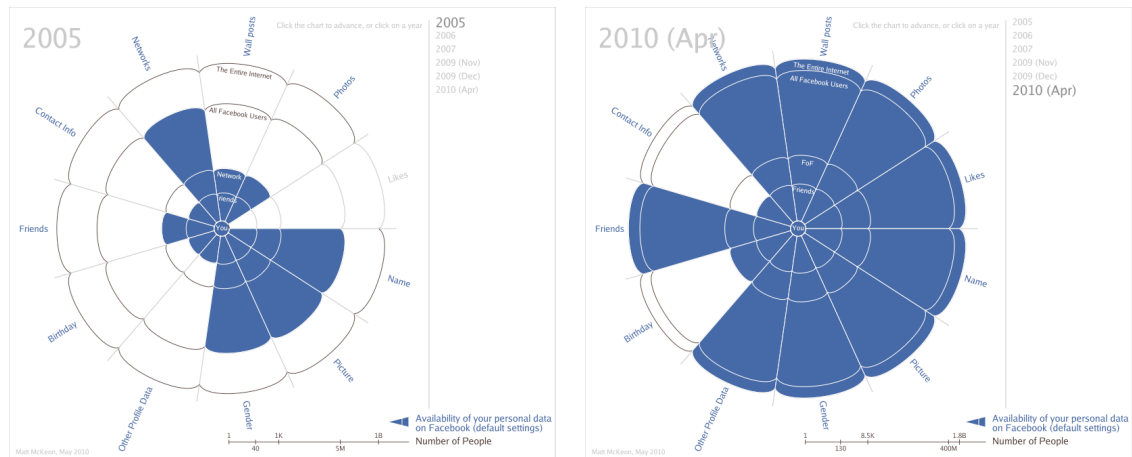


Figure 1: Change in default privacy settings of Facebook between 2005 (left) and April 2010 (right); blue segments indicate information that is made public by default (McKeon 2010)

All these developments raise the question whether all these detailed privacy settings are necessary, and if so, why. In this paper I will argue that using the theory of spheres of access Facebook needs privacy settings, and these settings should be simple, transparent and reliable.

I will start with explaining why it is morally justified to protect privacy, even while this infringes on the freedom of others. Next, I will apply the theory of spheres of access to Facebook using two examples. After this, I will explain the need for simple, transparent and reliable privacy settings and propose a solution. This paper ends with some conclusions.

Privacy vs. freedom: four moral reasons for protecting privacy

The debate about protecting privacy often revolves about the discussion whether a *right to privacy* would mean a loss of freedom. After all, when your privacy is protected, the freedom of someone else to gather information about you is restricted. As *freedom* is a very important moral value (for instance in Common Morality (Hoven 2005)), this clearly would argue against protecting privacy. On the other hand, a loss of privacy can be seen as a loss of freedom (Hoven 2005). This can be explained by the example of the *Panopticon*. The Panopticon is essentially a prison where the prisoners can be watched by the guards at all times, but not necessarily are. In such an environment, “a complete absence of privacy will stimulate socially acceptable behaviour” (Schermer 2007), and thus limit the freedom of the people being watched to determine their own behaviour.

(Hoven and Weckert 2008) differentiate between two different views on this discussion about ‘privacy vs. freedom’. The first viewpoint can be classified as *communitarian*: communitarians see a danger for society in limiting the freedom to observe individuals, and argue that protecting privacy and anonymity would lead to *free riding* (e.g. tax evasion or fraud). In this view, anonymous free riders harm society because, for instance, they do not pay enough taxes. The second viewpoint is more *liberal*: liberals argue that the right to privacy is more important, and thus that individuals should be protected from information gathering governments, corporations or other individuals.

Up to this day, there is no conclusive end of the discussion between the communitarian and the liberal point of view. However, (Hoven and Weckert 2008) present four moral reasons to protect privacy regardless of such a definitive outcome. In other words: four reasons that would justify limiting the freedom of others to gather information.

- 1 The first reason is the *prevention of harm*. It can be argued that a violation of someone's privacy causes harm to that someone. For instance, stalkers and even murderers have approached their victims by infringing on their privacy online (NRC Next 2010). Another, less horrible example is about the Irish tax authorities, which trawl online social network profiles to check on people's tax filings (Independent.ie 2008). A final example is the firing of several employees by Virgin Atlantic, their employer, for comments they made on Facebook (Telegraph 2008). These are all examples where the violation of someone's privacy has caused harm.¹
- 2 The second moral reason is *informational inequality*, which concerns the transaction of personal data. For instance, in the case of Facebook, a user can use online applications and games by 'paying' by giving the application and its developer access to its personal data. The associated inequality in this transaction is the absence of a fair market mechanism – to the contrary, it is not clear what the user gets in return for sharing huge amounts of personal data on Facebook, while Facebook profits from this data by targeted advertising or selling it to third parties (Holland 2008).
- 3 The third moral reason is about *informational injustice*. This has to do with *spheres of access*. For example, most people are okay with the fact that their personal medical data is used for medical purposes. This medical data then stays within the 'medical sphere'. However, if an employer would use this medical data for recruiting purposes, it would be a violation of privacy because the data leaves the sphere; there is a "morally inappropriate transfer of personal data across the boundaries" of the spheres of access (Hoven and Weckert 2008). The concept of informational injustice and spheres of access is very relevant to the discussion about privacy on Facebook, therefore I will return to this subject in the next section.
- 4 Finally, the fourth moral reason for protecting personal data is about *moral autonomy*. Basically, this means that everyone has the right to form her own image and to present herself the way she wants. Or in other words: "Privacy isn't just about hiding things. It's about self-possession, autonomy, and integrity." (Garfinkel 2001) This also relates to the previous discussion about the Panopticon, where the absence of privacy forces a certain socially acceptable behaviour on individuals.

Of these four reasons, especially the one about informational injustice is relevant to the discussion about Facebook's privacy settings. This is because the spheres of access that are introduced in this argument can be applied very

¹ While communitarians would certainly agree that stalking and murdering should be prevented and avoided, they may not agree that the other two cases are classified as harmful. After all, from a societal perspective, tax evasion (an example of free riding) and anonymous gossiping should be avoided, and this may thus justify checking someone's Facebook profile. However, the main point – prevention of harm is a moral reason to protect privacy – still stands.

well on several situations that often occur on Facebook. The next section will elaborate on two of these examples.

Spheres of access and Chinese walls applied to Facebook

As mentioned before, the third moral reason to protect privacy is about informational injustice. Such injustice can be prevented if information is only shared with those that are allowed by the owner. This can be made tangible by the spheres of access: if you are in the sphere, you have access to the information; if not, you cannot access the data. So, users with equal rights to certain sets of information are in the same sphere. The boundaries of these spheres should be impenetrable, (Wiegel 2007) therefore calls them *Chinese walls*.

To define the spheres of access, and to build the Chinese walls between those spheres, users need *settings*. These settings define the boundaries of the spheres of access and thus determine the access one has to someone's information, for instance on Facebook. I will explain the need for privacy settings using two examples.

ex. 1 An example, applied to Facebook: when I upload my holiday pictures to Facebook, I want my family and friends to be able to view them. However, I do not want my boss, who is also a friend on Facebook, to view them. And I most certainly do not want random strangers (e.g. advertisers or my insurance company) to see those pictures.

Clearly, this example explains the need for (detailed) privacy settings. I do not only need to specify that these pictures should not be shared with non-Facebook users (the random strangers); I also need to distinguish between certain categories of friends (friends, family, work).

What if the setting to block access by random strangers is not available? Then I could do two things: I could share my photos with the rest of the world, or I could not share them at all. Sharing my photos with the rest of the world, for instance with advertisers, will result in unrequested ads. This is an example of informational inequality. On the other hand, my other option would be to simply not share my pictures. However, this would limit my moral autonomy. Thus, based on moral reasons 2 and 4, it is preferable to have a setting to block access to random strangers.

What if the setting to distinguish between different groups of Facebook friends is not available? Here, I have three options: I could not upload the photos, again limiting my moral autonomy. Alternatively, I could share the photos with all my friends, including distant relatives and colleagues from work. However, this would lead to informational injustice: my colleagues may not share their personal holiday pictures, online or offline, while (in general) I would share a lot of personal information on basis of reciprocity with my close friends and family. The third option is to *de-friend* my colleagues and distant relatives, so they are removed from my list with Facebook friends. This would also be an unwanted effect, and may be classified as a limitation of moral autonomy. So, again referring to the four moral reasons, it is preferable to have a setting to differentiate access to my holiday pictures.

ex. 2 A second example deals with users' status updates on Facebook. These are messages that frequently reveal information about the user's activities on a certain moment. When I publish a status update, I want to be able to shield

this from the rest of the world. So, also regarding status updates there is a need for a privacy setting.

What if this setting is unavailable? Then I have two options: not publishing status updates, or publishing them for the whole world to read. Not publishing status updates would limit my moral autonomy. Publishing them for everybody to read would increase possibilities for harm: for instance, when a thief would read my status update that I am enjoying a holiday, he knows that my house is uninhabited, and this would thus increase chances that my house is broken into, which would constitute harm. So, again referring to the four moral reasons, also for this example there is a clear need for the appropriate privacy settings.

In conclusion, the two examples show that there is a clear need for a range of differentiated and clear privacy settings. In the next section I will argue that these privacy settings should be simple, transparent and reliable.

The privacy paradox and the need for simple, transparent and reliable settings

As stated in the introduction, the popularity of Facebook is increasing enormously. But also the amount of information shared by default with the outside world and the complexity of the privacy settings increases. Apparently, users are willing to sacrifice some privacy to be able to use Facebook. This is called the *privacy paradox*: there is a growing concern and discussion about privacy online, but at the same time people are sharing more information online (Barnes 2006). Also the founder of Facebook has declared that he believes that people are willing to share more and more and care less about privacy (The Economist 2010).

However, the fact that people are sharing information on Facebook does absolutely not authorize the use of this information outside the realm of Facebook; the information must stay in the Facebook sphere of access, as argued in the previous section. The consequence of this is the need for privacy settings. These settings should be simple, transparent and reliable.

Simple, because every Facebook user should be able to control her privacy settings in an accessible way, because otherwise she is unable to make a good decision whether or not to share information on Facebook.

Transparent, because for a Facebook user to make a sound decision about which information to share with who, she needs to know the consequences of the privacy settings.

Reliable, because a Facebook user should be able to trust her decision to share or not share information with others to be fixed, and only hers to change. If the privacy settings of Facebook would change continuously, this would not be the case and a user cannot know if her decision to not share her holiday pictures with her colleagues is the same tomorrow.

Clearly, Facebook's current privacy settings do not adhere to these three conditions. With a list of 50 settings and 170 options, the privacy settings are definitely not clear and transparent. Moreover, the settings are unreliable as Facebook often makes changes in the privacy settings, so that previously private data may now be shared publicly while the user is unaware of this.

A solution to this would be one, simple privacy control: a *privacy dial* that lets the user choose between four or five levels of privacy, from 'private' to 'everything public' while still allowing for fine-tuning detailed privacy settings (Manjoo 2010). This would be a big improvement over the current situation because such a privacy dial would satisfy the conditions of simplicity and transparency. It is then up to Facebook to uphold the reliability of the settings. This privacy dial would thus satisfy the requirements for simple, transparent and reliable privacy settings set out in this paper and would thus solve the problem of a Facebook user being dazzled by the enormous amount of privacy settings.

Conclusion

In this paper I have explained that, while there is no definitive conclusion to the debate about privacy, there are four moral reasons to protect privacy. These moral reasons lead to the theory about spheres of access: information may only be shared with those in the sphere, and the information may not be transferred across the boundaries of the sphere.

Applied to Facebook, this theory leads to a clear need for privacy settings for users, so that users can decide for themselves what information they share, and with who they share it. I have also argued that these settings should be simple, transparent and reliable, and proposed a solution for one general privacy dial with the option to fine-tune detailed settings.

List of references

- Barnes, S. B. (2006). "A privacy paradox: Social networking in the United States." *First Monday* 11(9).
- EPIC (2010). Complaint, Request for Investigation, Injunction, and Other Relief In the Matter of Facebook, Inc.
- Garfinkel, S. (2001). *Database nation : the death of privacy in the 21st century*. Cambridge, Mass., O'Reilly.
- Holland, H. B. (2008). Social Distortion: Privacy, Consent, and Social Networks.
- Hoven, J. v. d. (2005). "Applying our Common Morality: The Case of Privacy." *Australian Journal of Professional and Applied Ethics* 7(1): 38-43.
- Hoven, J. v. d. and J. Weckert (2008). *Information technology and moral philosophy*. Cambridge ; New York, Cambridge University Press.
- Independent.ie (2008). "Taxman admits to facebook 'trawl'." Retrieved May 19, 2010, from <http://www.independent.ie/national-news/taxman-admits-to-facebook-trawl-1297118.html>.
- Manjoo, F. (2010). "Can We Get Some Privacy?" Retrieved May 27, 2010, from <http://www.slate.com/id/2253827>.
- McKeon, M. (2010). "The Evolution of Privacy on Facebook." Retrieved May 19, 2010, from <http://mattmckeon.com/facebook-privacy/>.
- NRC Handelsblad (2010). Facebook werkt aan nieuwe privacy-instellingen.
- NRC Next (2010). "Nona werd via Facebook vermoord." Retrieved May 19, 2010, from <http://www.nrcnext.nl/blog/2010/05/18/nona-werd-via-facebook-vermoord/>.
- Nuttall, C. and D. Gelles (2010). Facebook becomes bigger hit than Google. *Financial Times*.
- Schermer, B. W. (2007). Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance. Leiden, Universiteit Leiden.
- Telegraph (2008). Virgin sacks cabin crew for insulting passengers on Facebook.

The Economist (2010). A special report on social networking.
The New York Times (2010). Price of Facebook Privacy? Start Clicking.
Wiegel, V. (2007). SophoLab. Experimental Computational Philosophy. Delft,
TU Delft.