IRIE
International Review of Information Ethics Vol. 16 (12/2011)

Richard A. Spinello:

Privacy and Social Networking Technology

Abstract:

This paper reviews Facebook's controversial privacy policies as a basis for considering how social network sites can better protect the personal information of their users. We argue that Facebook's architecture leaves its users too exposed, especially to online surveillance. This architecture must be modified and Facebook must be more proactive in safeguarding the rights of their customers as it seeks to find the proper balance between user privacy and its commercial interests.

Agenda:

Author:

Associate Research Professor Dr. Richard A. Spinello:

- Carroll School of Management, Boston College, Chestnut Hill, MA, USA
- ☎ 1-617-552-11898, ✉ spinello@bc.edu💻 www.bc.edu/csom_spinello
- Relevant publications:
  - Spinello, R. A. (2010) Informational Privacy. In Brenkert, G. and Beauchamp, T (eds.) *The Oxford Handbook of Business Ethics*, Oxford: Oxford University Press, 2010, pp. 366-388.

Introduction

One of the most powerful innovations in the Internet's short history is the World Wide Web, which has evolved into a vast public space where people engage in a wide range of social interactions. Some Web applications, however, have exacerbated the problem of privacy, opening up an intense debate with huge commercial interests at stake. Privacy erosion certainly did not originate with the introduction of the Web, which has made possible the surveillance of the browsing and searching habits of users as they move from site to site. Rather, each generation of technology has created new and unprecedented problems for the preservation of personal privacy. Thus, it should be no surprise that the latest technology of social networking will be accompanied by a fresh set of privacy concerns.

In this paper we will briefly review the historical background about privacy issues in order to provide some context. We then consider how Facebook, the paradigm social networking application, has significantly compromised user privacy. Even more ominously, this company has sought to orchestrate an attitudinal shift about the value of privacy. After investigating how social networking is transforming the privacy landscape, the paper proceeds to a normative analysis which includes a definition of privacy along with a terse defense of a universal right to privacy. Finally, we offer some possible resolutions of the problem, concluding that while more stringent regulation may be inevitable, all parties would benefit from ethical self-regulation that gives social network users the necessary technical capability to protect their personal information.

Historical perspective

Successive technological architectures dating back several decades have put personal privacy in jeopardy. The first such architecture was data base technology which made it possible to collect, store, and retrieve, copious amounts of digitized information efficiently and economically. During this period, most personal data was transferred to computerized records which became the foundation for consumer profiles or "digital dossiers." As more and more organizations turned to electronic record-keeping, and as databases became interconnected, the threat to privacy grew almost exponentially.

The second architecture was the Internet itself, which enabled the easy transmission of digital information. However, the Internet's primitive architecture based on the TCP/IP protocol initially supported anonymity: information was sent enclosed in packets to an IP address that did not identify either the sender or recipient. But the innovation of the Web and associated architectures like cookies changed all that. Web technology facilitated on-line business models even as it posed a substantial threat to privacy, since Web servers could deposit these cookie files on client computers and collect all sorts of information. Since the dawn of the Web's commercialization, Web-based tools like cookies and web bugs have created an environment hostile to privacy interests, where on-line surveillance has become the norm.

These cookies contain information such as passwords, lists of pages within the web site that have been visited, and the dates when those pages were last examined. Through cookies, vendors can monitor clickstream data, the information generated as a user surfs the web. Often this data is collected by third parties who place this uniquely identifying cookie file on a user's computer in order to track that user's movements. Social network sites such as Facebook build on cookie technology through devices such as social plug-ins which enable more sophisticated tracking of their users along with an exchange of information with "friends" and other web sites. The end result is the user's inability to surf the web anonymously. Social networks have also exploited opportunities to disseminate personal information to a user's network of friends (usually without permission) through mechanisms like News Feeds.

The principal objective for the collection of this fine-tuned data collection is personalized marketing. Targeted advertising campaigns based on behavioral data are more efficient because they appreciably increase the probability of a positive response. This preoccupation with the predictive power of information is a permanent feature of modern commercial transactions. As many privacy experts have pointed out, however, the manifest danger here is that personalization can easily slide into manipulation – marketing approaches based on one's past on-line behavior can be used for subtle exploitation of a user's needs and desires.

Privacy spotlight for social networks

An online social network is defined as a web-based service that enables individuals to "construct a public or semi-public profile within a bounded system; articulate a list of other users with whom they share a connection; and view and traverse their list of connections and those made by others within the system" (Boyd and Ellison 2008). A social networking web site, such as Facebook, allows its users to create their own personal web site that is centered around their personal profile, which is used to generate a community of "friends" who interact with one another. This interactive environment is enhanced through the integration of these sites with email and other communications applications.

The social networking business model is based on a clear *quid pro quo*: millions of people expose highly personal information about themselves in exchange for the ability to communicate with their friends, family members, and colleagues. This formula sets the stage for complex privacy tradeoffs. In order to monetize this "free" technology Facebook uses this consumer data so that its advertisers can deliver targeted online ads and marketing messages. Facebook encourages users to reveal to the public as much information as possible since the lower the level of privacy, the more its business interests are advanced. It has also repeatedly constructed its architectures to favor open disclosure rather than privacy. Facebook's controversial history about privacy suggests an insensitivity regarding the privacy rights of its users. It has repeatedly adopted policies infringing on privacy only to retreat in the face of strident criticism; it has argued that the social norm of privacy needs to be transformed, and it still has a number of problematic privacy policies. Let us consider each of these areas in more detail, beginning with its history.

In 2007 Facebook initiated its Beacon program which reported information about Facebook users' activities on third party web sites. A user's purchases were reported to their friends' News Feed after the conclusion of a purchase or other transaction. Users were not aware of this tracking mechanism and the initial privacy settings did not provide the opportunity to opt-out. Facebook eventually allowed users to opt-out of this feature, but the program was terminated in 2009 after mounting criticism from privacy groups such as the Electronic Privacy Information Center (EPIC).

In 2009 Facebook provoked the ire of privacy activists when it changed its privacy settings so that a user's name, profile picture, and gender were made public by default. In its defense, the company contended that this change reflected a societal shift toward more openness and that any user could override the default setting. But in the wake of EPIC's complaint to the Federal Trade Commission (FTC) and growing public criticism Facebook again altered its policies in 2010, giving users more control over access to their personal information. Despite these changes, Facebook's reactive approach to privacy issues does not augur well for the future.

In addition, there are still a significant number of outstanding privacy issues. By default, a Facebook user's profile is available to someone who enters that user's name in a search engine like Google. However, this "public search" function can now be disabled. Also, users can opt out of participation in platform applications, games and third party web sites, which prevents access to their personal data. On the other hand, Facebook still plans to proceed with a plan to disclose the home addresses and mobile phone numbers of its users to third-party application developers (EPIC 2011).

In 2010 the company took public its "instant personalization" scheme which allows partner web sites to access Facebook information as soon as a Facebook user visits the site. This all happens by default before the user gives consent to the sharing of his or her information. In that same year the company introduced social plug-ins, including a social widget known as the "Like" button, that appeared on other web sites (like amazon.com) – if a user likes an item she sees, she clicks on this button and the item appears in a list of things she likes in her profile. This plug-in architecture, a further evolution of cookie technology, functions as follows. When a user logs into a social networking site like Facebook the site sends a cookie to the user's browser which is disabled only when the user logs out of his or her Facebook account. As the user visits various web sites, the Like architecture will report back to Facebook whether or not the user has clicked on the Like button (even if the user doesn't click on this button, Facebook knows that you've been to this site and looked at this item). This social widget provides a history of a user's Web-browsing habits that can be linked to personally identifiable information. The social plug-in architecture has the potential to be an especially powerful mechanism for behavioral advertising, though Facebook claims that (at least for the present) it anonymizes this tracking data after 90 days (Efrati 2011).

Another controversial policy is Facebook's facial recognition program whereby Facebook uses the photos of their users to build a biometric database so as to implement a facial recognition technology. Despite calls for the program's suspension and an FTC investigation, Facebook has not backed down though users can now opt out of this facial recognition scheme by changing their privacy settings.

Thus, Facebook's current architecture is still too oriented to self-exposure. At the same time, the company philosophy goes too far in its efforts to lower expectations of privacy. Facebook executives like Zuckerberg have opined that privacy expectations are changing and that users *should* make more information about themselves publicly available: "people have gotten really comfortable not only sharing more information and different kinds, but more openly and with more people. . .that social norm is just something that's evolving" (Menn 2010). Facebook's privacy policies and architectures clearly reflect this tendency to nudge its customers toward the unveiling of their personal information for all to see.

Normative analysis

Before we address the normative dimension of this problem, we must be clear about the nature of privacy. Informational privacy is best defined in terms of "restricted access/limited control" (Tavani and Moor 2001). Restricted access implies that the condition of privacy exists where there is a capacity to shield one's personal data from some parties while sharing it with others. According to this perspective, an individual has privacy "in a situation with regard to others if and only if in that situation the individual is normatively protected from intrusion, interference, and information access by others" (Moor 2004). A "situation" can be described in terms of a relationship, an activity of some sort, or any "state of affairs" where restricted access is reasonably warranted. Individuals also need *limited control* over their personal data to ensure restricted access. That control can take the form of informed consent. In situations where a user provides his or her personal information to a vendor or a professional party, the user will be informed when that information will be shared with a third party and will have the capacity to limit the sharing of that information. The restricted access/limited control theory signifies that one cannot possess informational privacy without restrictions on information dissemination about oneself and without some control (as warranted by the particular situation).

Thus, privacy is a condition or a state of carefully restricted accessibility. But is privacy an interest, a personal predilection that can be superseded by utilitarian concerns, or is it a fundamental human right? In our estimation, it can be plausibly argued that people have a right to privacy because it is a vital instrumental good, which supports irreducible human goods such as friendship (or sociability), security and bodily well-being, knowledge, and freedom. These and other basic goods constitute human flourishing and therefore form the foundation for prescribing moral norms and rights. Without the instrumental good of privacy, our capability to sustain participation in certain basic goods such as security and intimate friendship is easily thwarted. Privacy is also an important condition of freedom (or autonomy): a shield of privacy is essential in most societies if one is to freely pursue his or her projects. Sensitive information collected without one's permission and knowledge can be used to disrupt an individual's free choices by depriving her of opportunities and necessities vital for the pursuit of her goals. Personalized marketing information can also be deployed for the purpose of manipulation – a steady stream of cleverly designed "personal" ads designed to wear us down into buying things we don't need. Since privacy is a necessary condition for the goods that constitute our integral well-being such as freedom and security, privacy warrants the status of a moral right, for rights are grounded in necessity, in what human persons need and rationally desire "for the exercise and development of distinctive human powers" (Hart 1983).

A Prescription for privacy protection

Given this definition of privacy and its status as a moral entitlement, it logically follows that responsible social networking companies are morally obliged to respect this right. Furthermore, it also follows from the nature of privacy as a condition of restricted access that users must be given the proper controls to limit access to their information as they deem appropriate. With a business model predicated on getting people to disclose details about their personal lives, social networks like Facebook need to be hypersensitive to the privacy concerns of those users

What specific steps can Facebook take to safeguard the privacy rights of their users, that is, to make certain that their users can control their information and restrict access according to their needs and preferences? Above all, Facebook should presume that each of its users favors a high level of privacy protection, and its architecture should reflect this presumption. Accordingly, Facebook should transparently maximize the opportunity for each user's control over his or her personal information. With these principles in mind, a morally responsible privacy policy for Facebook should have the following features:

- There should be no "publicly available" fields unless the user explicitly chooses otherwise. The default privacy settings should protect user information from public view and an opt-in system should always be the norm so that users have discrete control over the disclosure of their personal information. There should also be an opt-in regime for the company's facial recognition program accompanied by a clear explanation of how this data will be used in future applications; a user's "informed consent" cannot be valid in the absence of such specific information. In addition, Facebook's instant personalization should also be made opt-in by default; and users should have the option to select this feature for each particular web site which they visit. And Facebook should offer its users the opportunity to opt in to disclosure of their data by third parties and to opt in to the public search option by making explicit choices for these options (EPIC 2011).
- Facebook should alter its privacy-infringing policy for social plug-ins: it should not track or retain information about user visits to partner web sites unless that user explicitly clicks the "Like" button on that particular site; web surfing data for users who choose to use a plug-in should be expeditiously deleted or anonymized.
- Facebook should not disclose users' addresses and mobile phone numbers to third party application developers; it has offered no justification for such a policy aside from purely commercial gains and no viable plan to monitor how this data will be utilized by these third parties or recombined with other data.
- Finally, given the moral status of privacy, Facebook should adopt a more proactive approach to the safeguarding of this right rather than the reactive one that has so far shaped its brief history. The company could easily get advice from privacy and consumer groups such as EPIC before it introduces new technologies with privacy implications.

These and other prudent policies will return to social network users the *control* they need to *restrict access* to their information and provide for a reasonable level of personal privacy even in this pseudo-public network space.

The bottom line is that the Facebook architectures should default to embed privacy protection rather than expose the personal data of Facebook users who are often inattentive to privacy settings, though not indifferent to threats to their personal privacy. The company should operate on the assumption that users want to maintain their privacy unless those users indicate otherwise and take explicit steps toward greater self-disclosure. The privacy conundrum of social networking can largely be resolved by architecture, by giving users simple, high-level controls to determine how much information they want to share. Market forces are not likely to demand these changes, though there may be a market for a social network that gives greater emphasis to privacy matters. The question is whether or not companies like Facebook will recognize their ethical obligation to treat privacy as a serious moral entitlement and act accordingly. Tighter legal regulations may ultimately be necessary, but this option is not optimal for several reasons. Regulations tend to be reactive and this technology changes quite swiftly. Also, there may be a tendency to over-regulate in ways that would impair future innovation. What is optimal is ethical self-regulation which can be easily implemented by building into code a more pronounced partiality toward privacy and confidentiality.

Conclusions

Given that the social networking architecture is predicated on self-disclosure, the preservation of privacy will always be an intricate challenge for those users who want to limit information about themselves by managing the tradeoff between privacy and communication. Social networks, however, should give users the capability to calibrate "the presentation of self" that is fundamentally enabled by their networks (Goffman, 1959). The right to privacy, to restrict self-disclosure, should not be unduly mitigated by social networks despite the constant temptation to do so for commercial reasons.

One danger of social networking technology is that users may inevitably come to regard self-transparency as the norm and pay less attention to defensive mechanisms designed to safeguard their privacy. As companies like Facebook deliberately lower privacy expectations to advance their own business interests there is a grave danger that users will come to disvalue their own privacy interests and easily concede to those constant efforts to collect and aggregate their personal information. Given the potential for harm from the unwarranted exposure of one's personal profile information to employers, law enforcement authorities, and commercial enterprises, this attitudinal shift and concomitant lack of vigilance would be an unfortunate development. Hence companies like Facebook should not only strive to construct more responsible, privacy-enhancing architectures, they should also recognize their lack of objectivity and refrain from self-serving efforts to deliberately modify long-standing social norms that safeguard personal privacy. Facebook must be more sensitive to the privacy rights of their users even if those users are sometimes inattentive to privacy matters.

References

Boyd, D and Ellison, N. (2008). "Social Network Sites: Definition, History, Scholarship," 13 Journal of Computer-Mediated Communications 210.

Efrati, A. (2011). "'Like' Button Follows Web Users," Wall Street Journal, May 18: B2.

Electronic Privacy Information Center (2011). In re Facebook; http://epic.org/privacy/facebook/in_re_facebook.

Goffman, E. (1959). The Presentation of Self in Everyday Life. Doubleday.

Hart, H.L. (1983) Essays in Jurisprudence and Philosophy. Oxford University Press.

Menn, J. (2010). "Virtually Insecure." Financial Times, July 29: 7.

Moor J. (2004). "Towards a Theory of Privacy for the Information Age," in Readings in CyberEthics, R. Spinello and H. Tavani. (eds). Jones & Bartlett: 407-417.

Tavani, H. and Moor, J. (2001)."Privacy Protection, Control of Information,and Privacy-Enhancing Technologies," Computers and Society 31: 6-11.