References

Camp LJ (2004) Digital identity. IEEE Technol Soc Mag 23(3):34–41

Clarke RA (1988) Information technology and dataveillance. Commun ACM 31(5):498–512

European commission (1995) Directive 95/46/EC of the European parliament and of the council. Off J Eur Communities 1(281):31–50

European commission: "Proposal for a directive of the European parliament and of the council", 2012. Retrieved 18 Apr 2013 from http://eurlex.europa.eu/LexUriServ / LexUriServ .do?uri=com:2012:0010 : fin:en:pdf

Garfinkel S (2001) Database nation: the death of privacy in the 21st century. O'Reilly, Sebastopol

Gregorie TM (2001) Cyberstalking: dangers on the information superhighway. The stalking resource center, national center for victims of crime, Washington, DC. Retrieved 29 Oct 2013 from http://67.199.115.23/docs/src/cyberstalking---dangers-on-the-information-superhighway.pdf?sfvrsn=2.

Han J, Kamber M, Pei J (2011) Data mining: concepts and techniques, 3rd edn. Morgan Kaufmann, San Francisco

Kadushin C (2005) Who benefits from network analysis: ethics of social network research. Ethical Dilemmas Soc Netw Res 27(2):139–153

Kennedy N, Macko M (2009) Social networking privacy and its effects on employment opportunities, Chapter 12, In: Convenient or invasive – the information age, Ethica Publishing, Boulder

Kleinberg M (2007) Challenges in mining social network data: processes, privacy, and paradoxes. In: KDD, San Jose, pp 4–5

Krishnamurthy B, Wills CE (2010) On the leakage of personally identifiable information via online social networks. Comput Commun Rev 40(1)112–117

Lewisa K, Kaufmana J, Gonzaleza M, Wimmerb A, Christakis N (2008) Tastes, ties, and time: a new social network dataset using Facebook.com. Soc Netw 30(4):330–342

Moreno JL (1953) Who shall survive? Foundations of sociometry, group psychotherapy and sociodrama. Beacon House, New York

Rosen J (2010) The web means the end of forgetting. The New York Times, New York

Rosenblum D (2007) What anyone can know: the privacy risks of social networking sites. IEEE Secur Priv 5(3):40–49

Rubinstein IS, Lee RD, Schwartz PM (2008) Data mining and internet profiling: emerging regulatory and technological approaches. University of Chic Law Rev 75(1):261–285

Russell MA (2011) Mining the social web: analyzing data from Facebook, Twitter, LinkedIn, and other social media sites. O'Reilly, Sebastopol

Solove DJ (2006) The digital person: technology and privacy in the information Age. NYU Press, New York

Supreme Court of the United States: "Katz v. United States", No.35, Decided: December 18, 1967. Retrieved 18 Apr 2013 from http://www.law.cornell.edu/supct/ html/historics/ USSC_CR_0389_0347_ZS.html

Tavani HT (2007) Ethics and technology – ethical issues in an age of information and communication technology, 2nd edn. Wiley, New York

The fourth amendment (Amendment IV) to the United States constitution, bill of rights. Retrieved 18 Apr 2013 from http://www.law.cornell.edu/constitution/fourth_amendment

The U.S. Equal Employment Opportunity Commission (EEOC), http://www.eeoc.gov/eeoc/

Tuovinen L, Röning J (2005) Balance of power: the social-ethical aspect of data mining, ethics of new information technology. In: Proceedings of the sixth international conference of computer ethics: philosophical enquiry (CEPE2005), Enschede, pp 367–379

Turvey BE (2011) Criminal profiling: an introduction to behavioral evidence analysis, 4th edn. Academic Press, Waltham

Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev IV(5):193–220

Wasserman S, Faust K (1994) Social network analysis: methods and applications. Cambridge University Press, Cambridge

Zimmer M (2010) But the data is already public: on the ethics of research in Facebook. Ethics Inf Technol 12(4):313–325

Ethics

▸ Ethics of Social Networks and Mining

▸ Social History of Computing and Online Social Communities

▸ Sources of Network Data

Ethics of Social Networks and Mining

Kevin Macnish

Inter-Disciplinary Ethics Applied Centre, University of Leeds, Leeds, UK

Synonyms

Anonymization of data; Deleting data; Ethics; Ownership of data; Privacy; Social networking sites

Glossary

Company The organization or group of organizations that administer a social networking site. This includes owning the software, operating the servers, and managing the storage facilities. The company is typically motivated by a desire for profit

Front User The person who uploads information to a social networking site. The front user is normally an individual desiring to "share life" online with friends and family; however, front users include also charities and companies seeking to develop a fan base online

Known End User (KEU) The KEU is known to the front user and included in their list of friends on the social networking site. As such the KEU has greater access to the front user's information than a member of the general public

Unknown End User (UEU) The UEU is not personally known to the front user and is not included in their list of friends on the social networking site. The UEU will typically only have access to publicly available information regarding the front user. In some cases, though, such as hackers and state security organizations, the UEU may have access to all the front user's data on the social networking site

Definition

This entry will consider the ethics of social networking sites and data collection over the Internet. It focuses on questions of privacy and the treatment and ownership of information online. There are numerous other ethical issues surrounding social networking sites which go beyond these questions and which as such will not be considered here.

Introduction

There are a number of ethical concerns surrounding social networking sites (SNSs) and data collection, central to which is the issue of privacy. SNSs involve members of the public uploading, storing, and accessing personal data (emotional states, photos, political and religious affiliations, etc.) over the Internet. At the same time, personal data is a key aspect of privacy. Privacy regards the access one has to and control one has over one's "own" data. Hence, SNSs have a significant impact on privacy, and much of this entry will be concerned with the problems arising from privacy concerns regarding SNSs.

Privacy is an important value, recognized across societies and eras and listed as a human right by both the United Nations (Universal Declaration on Human Rights, Article 12) and the European Union (EU Convention on Human Rights, Article 8). Privacy gives one the space to be creative and to develop and practice one's autonomy. Furthermore, and of special significance to SNSs, privacy allows one to define intimacy in relationships (Rachels 1975). As a relationship becomes more intimate, so more information, and more personal information, is shared. It is not surprising that, at least in part, relationships are established and maintained online, as offline, through the sharing of personal data. Furthermore, different data is shared with different people, mirroring levels of intimacy offline. Hence, SNSs typically provide a public profile for all to see and a private profile which is only visible to those who have been confirmed as "friends."

Privacy therefore raises questions of control and access to personal data (Parent 1983; Nathan 1990; Boyd 2010; Tavani and Moor 2001). In establishing and building relationships, we relinquish control over that data by granting others access to it. That is, we experience less privacy.

A major concern regarding privacy over SNSs, as opposed to that in the offline world, is ownership of the data once it has been uploaded to the site. Many users who upload the data are likely to believe that they own the data. It is after all "their" data, their thoughts, opinions, and photos. However, they are uploading, and in a sense giving, that information to a private company (or possibly a government- or charity-controlled enterprise). The company or enterprise owns the

rights to the software and the server space to which the data is uploaded. Typically the user will have agreed to certain terms of service presented by the company or enterprise in order to use the social network. It is possible therefore that the data, once uploaded, becomes the property of the company or enterprise, rather than the user. A third possibility is that the data, once uploaded to the site, becomes the property of the public. There would be an analogy here with a published autobiography in which the information revealed therein becomes public property, irrespective of the author's or publisher's intent. The answer to this question of ownership is important in understanding the ethics of how that data is used and who ultimately has control over it. It will also affect who has the right to delete that information. However, it is worth bearing in mind that, as with patient records in hospitals, ownership does not bring with it an automatic right to use a person's information without their consent.

Ethical Issues

Introduction

In considering the ethics of SNSs and mining, there are four (groups of) agents to consider. First, there is the company or enterprise which owns the software, owns or rents the storage capacity, and operates the service. This might be one company or a number of companies, each providing a different aspect of the service. In either case, the interest of these agents will be similar in terms of seeking to profit from the service they offer. Second, there is the user who uploads data to the site in order to share it. I shall refer to this user as the front user to distinguish him or her from the recipient of the data, or end user. There are then two types of end user. The first is the known end user that is the person for whom the data is intended. Typically this will be someone in the front user's group of friends on the site. The second type is the unknown end user. This will include people who access the public areas of the front user's social network space but also hackers and law and security agencies who have access to the private space as well. To better understand these distinctions, I shall consider each of these groups in greater depth before turning to key ethical issues.

SNSs may be created by charitable enterprises or governments; however, they are more typically created and operated by private companies (Fuchs 2010). As such, the operator has a motive to make money through the operation of the service. This may occur in one of two ways. The first of these is the selling of membership, additional options (so-called "freemium" services) and/or space on the service to users. This creates a small but elite SNS defined by invitation or an ability to afford the service. Alternatively membership/options/space may be provided for free but funded by advertising through the service. This creates a much larger SNS which is of interest to advertisers both for its size and because the advertising can be targeted on particular groups as defined by demographic, ethnicity, religion, politics, etc.

Unlike the company, many if not most front users do not have a financial interest in the site. It may be used for meeting new business contacts, or for promoting a particular company or product, and so have a financial element to it. However, SNSs are more typically used for leisure and for "sharing one's life" with friends and family (Lenhart and Madden 2007). This usually means uploading photographs, sharing thoughts or incidents in one's life, and interacting with friends about what they upload to their site. It is hence a way of keeping up or reconnecting with friends and family, and also of meeting new friends.

The known end user (KEU) is the intended recipient for whom the front user uploads his or her data. The KEU is therefore assumed to have some interest in the front user either as family or a friend or is possibly interested in establishing a relationship. In some way they therefore have a desire to know what is going on in the front user's life such that they have an interest in connecting on the site. To ensure that they are known to the front user the KEU must be accepted by the front user as a friend, although there may be pressure deliberately or inadvertently applied to the front user to befriend someone they would rather not.

The unknown end user (UEU) is unknown personally to the front user. The front user may know of or suspect the UEU's existence but does not have a personal relationship with the UEU. There are two main groups of UEU which I shall address here: investigators and data miners. While each group is unknown to the front user, the investigator is interested in the front user as a person while the data miner is interested in the front user as part of a group. As we shall see the distinction is not as clear-cut as this, but it is a good starting point.

Investigators may be employed by individuals wishing to establish the credentials of a third party, by a company seeking to do the same for potential employees, or by a government for security, law enforcement, or repressive purposes (Albrechtslund 2008). This group would also include hackers who seek to gain access to a site by guessing or breaking a password. Non-governmental investigators seek to benefit from information on the public site of a front user or to exploit the poor privacy settings, or poor security, of the same. Governments may have established legal access to all areas of any user's account in order to allow the company to operate in that country. SNSs contain a rich store of information for such investigators, ranging from political and religious views to compromising photos or writings. As such they can help to reveal a more personal side than would normally be visible.

Turning to data miners, the second type of UEU to be examined here, these are usually groups of researchers working for academic or commercial organizations. As for investigators, SNSs contain a wealth of information which might otherwise be unavailable to researchers. The results of the research may then be of use in understanding social phenomena or designing and targeting products to particular market segments (Barnes 2006).

The Company

Key issues for the company include how to communicate with the user, duties of care, default settings, and deleting information. The company has a duty to educate the user such that it gains each user's informed consent to the terms and conditions. Lengthy terms of service may be more informative but may also remain unread owing precisely to their length. Shorter terms of service may elicit greater readership but be less informative. The company therefore has a duty to inform potential members how their information may be used. It also has an interest in not frightening away potential members by giving the impression of engaging in politics nor of willfully selling user's information to the highest bidder. However, some research has suggested that even if users are aware of the existence of a privacy policy, they may have an incorrect interpretation of its contents (Hoofnagle and King 2008; Turow et al. 2005). If this is the case then the company should investigate means to better educate their users as to the implications of the terms and conditions.

Related to the concern of informed consent is the duty of care that the company has to the user. For most users this will extend to presenting the terms and conditions, but additional safeguards may be required for the vulnerable, such as children. Some sites have added "panic buttons" to enable users, and particularly children, to inform the site or the police if they are contacted by a stranger or experience abuse on the site (Emery 2010). A closely related question is whether the company also has a duty to prevent the front user from uploading just any information. Such a prevention might be motivated by protecting the front user from possible harm or from causing harm to others by uploading offensive material.

A further problem is that of default settings. Should the default settings involve a high degree of privacy, so that users have to opt in to having their data shared with advertisers? If so, then the reduced information available to advertisers will mean that they have less to work with and be less attracted to use the networking site. By contrast, if the default settings have a low degree of privacy, then advertisers can access more information. This will enable them to target specific markets more directly and see a greater return for their investment. Such markets might include, for example, teenagers, working mothers, or Asian men living in the UK. This will render the networking site highly

attractive to the advertising community as targeted advertising will bring greater returns on the initial investment. However, low default privacy settings also risk leaving the users more vulnerable to invasions of privacy. Such settings mean that, unless the user goes through a number of steps to change their privacy settings, information which they might reasonably have presumed was restricted to friends is in fact publicly available.

A further problem with default settings concerns the location of the front user when data was uploaded to the SNS. The SNS may by default publish the location from which information was uploaded along with the information itself. This is typically the case when the information was entered on a mobile phone with a geolocation facility, which may again be active by default. Unless the default settings are changed by the front user, this data gives KEUs and possibly UEUs information about a front user's physical location at a particular time. Such information may then be used in crimes against property and as such presents a security concern (Roberts 2010).

Finally, there is also a concern about deleting information and accounts (Mayer-Schonberger 2011). Once a front user has determined that they do not wish to continue with an account, they might choose to deactivate it, but does it follow that the company must then delete all the data submitted and if so, how soon? Some companies will keep an account open for a limited duration in case the front user changes his or her mind and chooses to reactivate the account. This enables the front user to do so without losing any data. Companies may also have legal obligations to retain information for law enforcement or security purposes beyond the timescale desired by the front user.

Front User

There are a number of ethical issues facing the front user. Perhaps the most important of these concerns what it is reasonable for him or her to believe about the service. Should he or she be expected to know that the company exists for profit through paid membership or through advertising? Should she or he be expected to read through and understand the full terms of service offered at registration? More than this, does the front user have a moral duty to read and understand the terms and conditions to which they are signing up? It seems as if there is a dual responsibility in this area between the company's reasonable duty to educate the user and the user's reasonable responsibility to be and remain informed.

A second issue, as indicated above, is whether the front user should reasonably presume to retain control over access to the data he or she enters into a service or should it be seen rather as publishing that data for the company's own use. There is a criticism leveled at some SNSs that a person choosing to "like" a particular product can find their endorsement being made public to their friends as part of an advertising campaign without their explicit consent.

Thirdly, there may be social pressures to join or engage in particular SNSs. If private parties are arranged solely through a SNS, then non-membership can lead to social exclusion. Similar exclusion may be experienced if one does not regularly interact with friends online and share information which might be better kept offline (such as embarrassing pictures). Pressure may also be attendant on whom is accepted or rejected as a friend. Should bosses, parents, or work colleagues be invited into the same arena of intimacy as close friends? It may be insulting and damaging to a relationship to deny access, but compromising if it is agreed to.

A fourth area concerns the data a front user uploads to the service. Typically this is, as noted, personal information of potential interest to friends. However, SNSs may also be used to deliberately release information to the general (global) public, especially if normal journalistic access to a situation is prohibited. The sites may also be used to rally and organize protests. If these turn violent or involve crime, then those posting relevant data to the sites might be accused of incitement to violence or crime. On a more personal level, one front user may

post information pertaining to themselves and a second front user. This information may prove to be detrimental to the second front user, who has little control over the information being made available either to the friends of the first front user or the general public. This scenario illustrates that privacy does not necessarily concern data referring to just one person, but that it may be shared between two or more users. As such the decision to upload the information to a SNS, and who should have access to that information, should be mutual rather than made by just one of the parties.

End User (Known)

The relationship between the known end user (KEU) and the front user is similar to a friendship offline. The KEU is presumed to respect the data of the front user by not republishing it or using it to in some way embarrass or humiliate the front user. As in the offline world, there is nothing to physically prevent the KEU from doing this, and it is this vulnerability to the KEU which establishes intimacy with the front user. If the KEU does abuse the relationship through either of these means, then, as in the offline world, the front user may "unfriend" them so that they are no longer privy to such information.

A second problem is that of not genuinely knowing the KEU. Researchers posing as real or fictitious people have successfully befriended people through online SNSs (Lenhart and Madden 2007). If a front user finds it relatively easy to befriend a person (or at least hard not to befriend them), then their area of intimate contact online may be far less secure than they realize. They may believe they are publishing information to just "friends" when in fact their circle of friends is only marginally more restricted than their public site (Haddadi and Hui 2010).

End User (Unknown)

As noted above, there are at least two types of unknown end user (UEU): the investigator and the data miner. I say at least two as there may be further divisions and subdivisions depending on whether, for example, the UEU has access to the public face of a person's SNS or to their private space, normally restricted to friends and family. While the former might include private investigators or companies researching candidates, the latter would include police and security services with legal access to the account and hackers who have gained illegal access.

An obvious concern regarding UEUs is whether they should have this level of access to personal data. Exploiting lax security by, for example, guessing passwords is at least prima facie wrong, but what if exploiting information made public as a result of low default privacy settings? This information is, after all, in the public domain. Through exploiting the access to the information, is the investigator also exploiting a weakness of the front user, and hence the front user himself? Government access may also be provided by default through company agreements with a particular state, such that users do not know that it exists, or have to read through long terms of service to find reference to its existence. Even if the front user does agree to this level of government access, it seems reasonable to ask whether it is good for a state to have that much information about its citizens easily accessible. There are also questions to be raised at the international level regarding which government has access to which files. Can, for instance, the US government access private data about UK citizens if their information is held by a US company or stored on servers in the USA? Furthermore, can the UK government access the same information or does a situation exist in which the US government has greater access to the data of UK citizens than their own government?

Moving to data mining of SNSs, there are several issues. The first of these is the question of how the data is accessed. This became an issue in a 2008 project in which research was carried out on students' use of a SNS at a particular university. The data was then anonymized and published online. Despite the supposed anonymity, within 48 h the university had been identified and at least some of the data linked to individual students. In defense of the project and the fact that

Ethics of Social Networks and Mining, Table 1 User summary

The company	Front user	Known end user	Unknown end user: investigator	Unknown end user: data miner
Gaining informed consent	Reasonable beliefs about the service	Abuse of data accessed	Correct level of access to data	How data is accessed
Duties of care	Control of data	Unknown end user posing as friend	Correct authority accessing data	Problems with anonymizing data
Default settings	Pressures to join SNS		Exploiting the front user	Intersection between general and specific data
Deleting information	Pressures to befriend on SNS			
	Consequences of uploading data			

the research had taken place without gaining the prior consent of the students, the research team responded that the information they had accessed was in the public domain. However, it transpired that as many of the researchers and the students belonged to a subnetwork (that of students at the university), the former were likely able to access information which might have been restricted from general public access (Zimmer 2010). As such the researchers had access to more intimate information on their subjects' sites than would have been the case had they restricted themselves to just publicly available data. In this respect, although the researchers were potentially known end users (they were in the same subnetwork), the use to which they were putting the data was unknown to the front user. This might be seen as an abuse of the network, or as introducing a third category of end user of whose existence the front user may be aware, but of whose activities the front user is not aware. This leads to the intimacy levels of a KEU without the end user having the same level of accountability to the front user as a genuine KEU would have.

Attempts at anonymizing data are fraught with difficulties as any individual's social network is likely to have certain unique qualities. It is improbable that any two people have exactly the same friends, still less the same friends and the same preferences in terms of politics, religion, films, and music. As such even data which has been made anonymous through disassociating the subject's name and obviously personal details (age, sex, etc.) may still be traceable to the originating source (Barbaro and Zeller 2006).

An additional problem is the intersection between the general and the specific in data mining. In 2007 research was performed on people who had openly homosexual friends on Facebook (Jernigan and Mistree 2009). This concluded that men with more openly homosexual friends on their SNS were more likely to be homosexual themselves than those with fewer openly homosexual friends. Hence even when a person does not publicize certain private information, in this case regarding sexual orientation, it may nonetheless be predictable through correlating publicly available data. As such it is possible that the correlation of information through data mining techniques could reveal more than the sum of its parts. The various users are summarized in Table 1.

Summary of Ethical Issues

In summary, there are numerous ethical issues surrounding the use of social networks. Many of these concern the access to and control of information, raising issues of privacy. However, the ethical concerns extend beyond privacy. I have argued that there are four main agents involved in social networks: the company, the front user, the known end user, and the unknown end user.

It is worth noting that these are not mutually exclusive: a front-user is likely to be a known end user and may also be an unknown end user and/or a member of the company.

There are a number of ethical concerns related to the context of each agent. The company has issues of relating to the users of the service, particularly duties of care to those users and duties to gain informed consent from the users as to the use of their information. The front user similarly has duties of care when it comes to joining the service and uploading data but may also face pressures to join and befriend on particular services which do not make his or her use of that service entirely voluntary. Known end users should protect the information they glean from front users with the same respect as they would had that information been given in a more traditional context. Finally, unknown end users fall into at least two categories: investigators and data miners. For the former there are questions of exploiting front users with poor knowledge of security and of determining what is the correct level of access to front users' data. Data miners face similar concerns when accessing data but also problems relating to the consequences of how that data is to be presented such as anonymization and the intersection between general information and specific applications of that information.

Social networking sites are therefore not morally neutral spaces, nor are they directly similar to traditional places for socializing. They provide a unique place for people to meet and maintain relationships, which bring with them a unique set of ethical concerns.

Cross-References

▸ Anonymization and De-anonymization of Social Network Data
▸ Collection and Analysis of Relational Data from Digital Archives
▸ Collection and Analysis of Relational Data in Organizational and Market Settings
▸ Community Evolution
▸ Dark Sides of Social Networking
▸ Data Mining
▸ Ethical Issues Surrounding Data Collection in Online Social Networks
▸ Facebook's Challenge to the Collection Limitation Principle
▸ Human Behavior and Social Networks
▸ Modeling Social Preferences Based on Social Interactions
▸ New Intermediaries of Personal Information: The FB Ecosystem
▸ Online Privacy Paradox and Social Networks
▸ Online Social Network Phishing Attack
▸ Online Social Network Privacy Management
▸ Privacy and Disclosure in a Social Networking Community
▸ Privacy in Social Networks, Current and Future Research Trends on
▸ Privacy Preservation and Location-Based Online Social Networking
▸ Privacy, Dataveillance, and Crime Prevention
▸ Probabilistic Analysis
▸ Social Engineering/Phishing
▸ Trust in Social Networks
▸ User Behavior in Online Social Networks, Influencing Factors

References

Albrechtslund A (2008) Online social networking as participatory surveillance. First Monday 13(3). Available at: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949. Accessed 24 Oct 2011

Barbaro M, Zeller T Jr (2006) A face is exposed for AOL searcher No. 4417749. New York Times. Available at: http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63&pagewanted=all. Accessed 24 Oct 2011

Barnes SB (2006) A privacy paradox: social networking in the United States. First Monday 11(9). Available at: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312. Accessed 24 Oct 2011

Boyd D (2010) Making sense of privacy and publicity. In: SCSW, Austin. Available at: http://www.danah.org/papers/talks/2010/SXSW2010.html

Emery D (2010) Facebook agrees to "panic button." BBC. Available at: http://www.bbc.co.uk/news/10572375. Accessed 1 Nov 2011

Fuchs C (2010) studiVZ: social networking in the surveillance society. Ethics Inf Technol 12(2):171–185
Haddadi H, Hui P (2010) To add or not to add: privacy and social honeypots. In: IEEE first international workshop on social networks, Cape Town
Hoofnagle CJ, King J (2008) What Californians understand about privacy online. SSRN eLibr. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130. Accessed 24 Oct 2011
Jernigan C, Mistree BFT (2009) Gaydar: facebook friendships expose sexual orientation. First Monday 14(10). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302. Accessed 24 Oct 2011
Lenhart A, Madden M (2007) Teens, privacy & online social networks. Pew Internet. Available at: http://www.pewinternet.org/ Reports /2007/Teens-Privacy-and -Online -Social -Networks / 1-Summary-of-Findings.aspx. Accessed 24 Oct 2011
Mayer-Schonberger V (2011) Delete: the virtue of forgetting in the digital age. Princeton University Press, Princeton
Nathan DO (1990) Just looking: voyeurism and the grounds of privacy. Public Aff Q 4(4):365–386
Parent WA (1983) Privacy, morality and the law. Philos Public Aff 12(4):269–288
Rachels J (1975) Why privacy is important. Philos Public Aff 4(4):323–333
Roberts L (2010) Facebook status "risks burglary." BBC. Available at: http://www.bbc.co.uk/news/uk-england-birmingham-12062331. Accessed 2 Nov 2011
Tavani HT, Moor JH (2001) Privacy protection, control of information, and privacy-enhancing technologies. Comput Soc 31(1):6–11
Turow J, Feldman L, Meltzer K (2005) Open to exploitation: American shoppers online and offline. Annenberg Public Policy Center, University of Pennsylvania. Available at: http://www.annenbergpublicpolicycenter.org
Zimmer M (2010) "But the data is already public": on the ethics of research in facebook. Ethics Inf Technol 12(4):313–325

Recommended Reading

Grimmelmann J (2009) Saving facebook. Iowa Law Rev 94:1137–1206

Ethno-Racial Discrimination

▸ Demographic, Ethnic, and Socioeconomic Community Structure in Social Networks

Evaluation Approaches

▸ Relative Validity Criteria for Community Mining Algorithms

Event Analysis on Social Media

▸ Twitris: A System for Collective Social Intelligence

Event Detection

▸ Disease Surveillance, Case Study
▸ Querying Volatile and Dynamic Networks
▸ Social Networks in Emergency Response

Evolutionary Communities

▸ Community Evolution

Evolution of Communities

▸ Dynamic Community Detection

Evolution of Privacy Settings

▸ Graphical User Interfaces for Privacy Settings

Evolving Communities

▸ Dynamic Community Detection

Evolving Community Detection

▸ Evolving Social Graph Clustering