novática
Revista de la Asociación de Técnicos de Informática

Novática, founded in 1975, is the oldest periodical publication amongst those specialized in Information and Communications Technology (ICT) existing today in Spain. It is published by **ATI** (*Asociación de Técnicos de Informática*) which also publishes **REICIS** (*Revista Española de Innovación, Calidad e Ingeniería del Software*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI is a founding member of **CEPIS** (Council of European Professional Informatics Socities), an organization with a global membership of above 200,000 European informatics professionals, and the Spain's representative in **IFIP** (International Federation for Information Processing), a worldwide umbrella organization for national societies working in the field of information processing. It has a collaboration agreement with **ACM** (Association for Computing Machinery) as well as with **AdaSpain**, **AI2**, **ASTIC**, **RITSI** and **Hispalux** among other organisations in the ICT field.

Editorial Office, Advertising and Madrid Office
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Layout and Comunidad Valenciana Office
Av. del Reino de Valencia 23, 46005 Valencia; Tlfn. 963740173 <novatica_prod@ati.es>
Accounting, Subscriptions and Catalonia Office
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>; <novatica.subscripciones@atinet.es>
Aragon Office
Lagasca 9, 3-B, 50006 Zaragoza Tlfn./fax 976235181 <secreara@ati.es>
Andalucía Office <secreand@ati.es>
Galicia Office<secregal@ati.es>
Advertising Plaza de España 6, 2ª planta, 28008 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Legal deposit: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Cover Page: Dancing House - Concha Arias Pérez / © ATI
Layout Design: Fernando Agresta / © ATI 2003

Special English Edition
2012/2013 Annual Selection of Articles

summary

Massimo Ragnedda
University of Northumbria, Newcastle (United Kingdom)

<ragnedda@gmail.com>

Social Networks and the Protection of Personal Information. When Privacy Is Not Perceived As a Right

Abstract: *On Social Networking Sites (SNS), users freely and without anxiety give sensitive and private data about which they might previously have jealously guarded. The research that I conducted at the University of Sassari (n = 1047), suggests that students have a different approach to the protection of Personal Information: lascivious online and protectionist offline. Students seem to underestimate the risk of posting data because they are unaware of the phenomenon of dataveillance. In fact, 86% said that the main visitors of their personal profile are friends, so they do not worry about data because they have nothing to hide from friends. This makes the perception of SNS more familiar and intimate and lowers social and cultural defenses against the possible intrusion of strangers in their digital world. Only 29.4% said that they often or always heed the privacy policy before registering for a site, and 54% never or rarely read the privacy policy. The role of marketing agencies that scan, match and connect data of individual users with the goal of building an accurate e-profile profile of individual users, seems not be perceived by the students. In fact only 3% imagine that those who visit personal profiles are strangers.*

Keywords: *Dataveillance, e-Profile, Privacy, Social Networking Sites, Surveillance.*

Author

Massimo Ragnedda is a Ph.D. in Theory of Communication and Intercultural Studies at the University of Sassari (Italy). In the academic year 2003/2004 he was a Visiting Researcher at the Institute of Communication Studies of Leeds University (UK), in the academic year 2006/2007 he was an affiliated visitor at the Department of Sociology, University of Cambridge (UK) and he was Academic Visiting at the Oxford Internet Institute (University of Oxford). Currently he teaches Mass Communications at Northumbria University (UK). He is author of 6 books and several articles in Italian, English and Spanish.

1. Introduction

The last decade has been characterized by the enormous development of Social Networking Sites (SNS), able to offer a range of new opportunities for communication and exchange of information of any kind, in real time, unimaginable until recently [1].

The incredible success of sites like Facebook reveals a radical change in the public accessibility of personal data of users. Facebook users extend their social circle and share data and information with their community and their friends, regardless that such information is distributed through third parties who collect them and gather in large databases [2]. Users produce content and add data by clicking the "Like" button on the content of others, regardless it comes from a friend or from external websites. Those "Like" clicks help to enrich the map of relationships (social graph) with multiple demographics that then help in locating the most suitable target for advertisements.

Using the SNS raises, therefore, a whole set of questions about the possible risks that their use leads to violation of privacy [3a][3b][3c]. Users of social networks do not always perceive the risk to their privacy [4]. The network is, in fact, an irreplaceable instrument of collective memory, capable of reflecting and building digital identities of users that are present online. Privacy becomes, thus, a key element for the construction of personal identities [5a][5b].

These dynamics, typical of the digital age, introduce profound and irreversible changes in our way of living and relating. With the advent of SNS it is changed, for a relevant part of the population, the way they relate to others, some fundamental principles of social life, and the conception and perception of privacy.

The Internet users in general and the users of the SNS in particular, tend to give freely, and without hesitation, the personal data about which they were once zealously guarded. But free does not mean, however, "at no cost": in fact, many SNS reuse the data entered into the personal profiles and sell them for marketing activities [6].

The act of sharing photos, political or religious views, sexual orientation and other private data, gives the possibility to create an increasingly defined electronic profile. The growing need for finance services and benefits is a stimulus for the collection, processing and use of user data. In fact, the information in "private" profiles is the only real heritage asset managers of SNS have, so the risk that these data are picked up, analysed and used, is increasing [7].

The hypothesis we propose here is that the right to privacy seems to be perceived, especially by Internet users as a right that is becoming less important and less valued. However, we are talking about a vitally important right in a democracy, because the protection of personal data guarantees the individual freedom [8]. Having the right to privacy means preserving social capital created in private, invested in relationships and friendships, and the lack of which can compromise social relations [9]. The right to privacy is a value [10] that must be defended [11] as an intrinsic value for the society [12]. Although the concept of "privacy" is imprecise [13a][13b], Turn stressed [14] that it should be considered as the right of individuals to the collection, processing, dissemination and use of their personal information.

At the same level as public monitoring, also the large corporations use surveillance for private purposes [15]. Private companies are interested in developing consumer profiles, and to build it, day after day, they use personal data which users type in the SNS and that are publicly (and globally) accessible in unknown terms and quantities. Peter Von Zschunke, for example, has been identified in a sample of the most popular SNS, about 120 personal attributes in user profiles: an impressive amount of personal data available with a mouse click [16].

The idea of controlling and gaining the maximum amount of data on citizens is not new. In fact, and as stressed by David Lyon, the creation of personnel files and the need to collect information on individuals gradually extended from military fields to all sectors of public and civil life, to become one of the elements that characterize the modern state [17].

Modernity is based in the process of bureaucratization and rationalization which Weber described, and that has characterized the historical process, also in the collection of data and information about individual users. This collection of information has become something that is increasingly present and yet invisible, which serves the principles of the

> "What sets this current model is the incredible amount of information that can be collected today from citizens and the relationship that individuals have with their own personal data"

Panopticon, the model prison that was first developed in 1791 by Jeremy Bentham and adopted by Foucault as a metaphor to describe and explain the operation of discipline and surveillance of individuals throughout the modern era.

What sets this current model is the incredible amount of information that can be collected today from citizens and the relationship that individuals have with their own personal data.

We all become the subject of attention. We live in a kind of cyberpanopticon [18], or superpanopticon [19], in an electronic surveillance system [20], in which the jailer's eyes constantly watch us. As in the panopticon, where the watchful eye is unverifiable, but always potentially present, the ability to record and reconstruct the individual profile of each individual "navigator" allows the Internet to go a step further than the Bentham project. The centre controls the periphery, which is controlled from the top down, but also reconstructs the individual's profile, linking a set of data and images for each individual user.

Based on these assumptions I have developed a research that aims to find out how the "digital natives" [21] perceive the risks of losing privacy while using social networking sites.

Specifically, the question that has guided this research project, conducted with students of the University of Sassari (Italy), that it will be discussed in this article is: How is our relationship to privacy changing? And on this question: Do we act differently in online and offline environments? What are the risks facing this difference to privacy?

2. Methodology

Sassari University has over 15,000 students divided into 11 different faculties [22]. We contacted participants through the mailing list of the Secretariat of Students, who sent the questionnaire via e-mail to all students of the University of Sassari. The questionnaire was tested on a sample of 15 students and was available online (after some modifications), for two months, from 14 September to 12 November 2011.

1,068 students responded, but 21 questionnaires were incomplete or were totally incomprehensible and were discarded. The 1,047 valid questionnaires constituted a representative sample of the University of Sassari. The most active Faculty was the Faculty of Literature (belonging to Area Social and Humanistic), with 38%, followed by the area of Law and Political Science with 23.7%, and the physical and medical sciences to 20.8%. There were a greater participation of women (54.5%) than men (45.5%).

The questionnaire includes 40 questions and is divided into four sections: the first on registry data, a section on the online habits of students, a very specific perception of privacy and surveillance, and finally, a section focused on the relationship between social and political networks. The results have been elaborated with SPSS 18.0 for Windows.

3. Main Results

In the context of this research, what stands out is the absolute confidence that students have with the Internet as the medium that has revolutionized the way they express themselves and that helps them to enter into the labour market: in fact, 46.9% say that the Internet has increased their chances of finding jobs, as well as has increased the opportunity to be found on the network on which they have, or should have, an appropriate profile that gives a good impression of themselves.

In fact, according to research cited by the Guarantor for the Protection of Personal Data, the administrative authority which protects access to user data in Italy, 77% of recruiting staff check on Internet seeking potential candidates and 35% say have eliminated candidates based on information discovered in the network.

Caring for one's image and reputation online is becoming very important as more and more companies in the pursuit of personal support or reject candidates thanks to the information that can be found on the network.

In order to understand the perception that students have of this phenomenon, I have asked the following question: "*Will entrepreneurs increase the use of Facebook to manage their current and potential employees?*". 58.6% of the sample agree or absolutely agree with this statement, and only 19.3% said they disagree or strongly disagree. Most respondents have, therefore, the perception that Facebook, and the vast amount of personal data it contains, could be used to select or monitor employees.

However and here it comes the first contradictory data: Indeed only 37.8% of the sample believes that the profile gives an accurate picture of them. In other words, despite being aware that potential employers can use Facebook to select or control their workers, most of the students seem not to worry about how they build them online profile and how accurate is. In fact, only 0.3% (ie, only 3 people in 1,047), believes that those who visit their profile is a possible recruiter.

Slightly better is the fact that references to (the future, that is), who will be the main visitor in the future: only 2.2% of the responded said the potential recruiters. A very low percentage comes out even for cases in which we talk about the potential of state surveillance. In fact, only 0.7% believes the government visits their profile and only 3.7% think that it will do so in the future.

These data demonstrate that students underestimate the long memory of the network and how data can be purchased by individuals who are not part of their group of friends, that 86.3% are the main visitors of the profile.

Probably the term "community" confuses the point of view and makes us believe that the data is shared "only" with the reference community. Actually, you never know for sure who is the public with whom data are shared, unlike offline life, where it is well known to those who hear our conversations, who are watching us and those around us. While we are online we do not know who is on the other side recording or collecting information.

From the data obtained by the research, there emerges a main difference in the management of privacy online and offline. Indeed, the research shows that students, overall, are very attentive to their offline privacy, to act accordingly, and they have an absolute protection of personal data.

We cannot say the same for their online activities. In particular, 37.9% of students who responded to the questionnaire said they always destroy their private documents when no longer useful, to which must be added 19.1% who do it sometimes. More than half of respondents, 57.0% destroy often or sometimes, forever and without proper backup, personal documents. Only 22.4% said no and 20.6% rarely do (see **Figure 1**).

This denotes a personal data protection which is very high, precisely to prevent others from accessing them. On the Internet, however, they neglect the possibility that the data can be forgotten or destroyed. Once published, and

> “These data demonstrate that students underestimate the long memory of the network and how data can be purchased by individuals who are not part of their group of friends”

Figure 1. Do you shred/burn your personal documents when you are disposing of them?

even if they are deleted from the page in which they were originally inserted, there is no certainty that these data finally disappear.

Returning to the offline sphere, 80.8% say they protect or hide, usually or always PIN credit card when they use it. This means that 4 out of 5 people protect this important data. Only one in 20 (5.3%), never fail to protect their PIN (see **Figure 2**). Most respondents show prudent behaviour in this regard.

We cannot say the same, although this is not as important as data PIN credit card, the behaviour of these same students in managing their data online. For example, only 34.9% of students are registered, usually or always, exclusively on websites that have a privacy policies, while 39.7% never do or do so rarely, and 25.4% do so sometimes. (see **Figure 3**).

There is more. Only 25.9% said they always or sometimes read the privacy policy if present. In fact, 54.0% never read, or rarely read the rules that protect their own right to privacy, and 20.1% do it once (see **Figure 4**).

In other words, more than half of the sample gives personal information without knowing how that data will be used, and this reflects the idea that they are not interested in managing and protecting personal data. To this we should add that one in four people always read the policy. It seems that the right to privacy does not interest them so much, that the perception of privacy as a right is disappearing, and they do not pay attention to the consequences that could result from the publication of personal data in a private profile that is only partly private.

Using a pseudonym to register on a website, without having to reveal the true identity to the other service users or the general public, can help to manage personal data. Only a quarter of respondents, 24.6% stated that never or almost never complete certain information when registering on a SNS. More than half of the sample, 51.6% always or often does, and the remainder, 23.7%, sometimes does.

Among the most regularly published data on SNS users, we can find the real name (84%), followed by the date of birth (81.5%), favourite links (74.9%) and favourite music bands (73.3%). On the other side, the data published in the SNS less published are: embarrassing photos of themselves (88.9%), telephone number (87.8%) and home address (87%). An interesting aspect to underline is that only 37.9% post their curriculum online, although it may be one way to get noticed.

Not only in the SNS we leave traces about ourselves: every move on the net leaves a trail behind it, a small sign but a really important sign for those who want to rebuild our profile and understand our tastes and preferences. As experts of the Electronic Privacy Information Centre underlined it is important to delete cookies [23] and clean regularly the visiting history, precisely because this gesture makes it more difficult to collect data from our online tour. Only 40.8% of the students interviewed stated that always or often they delete cookies. This finding is particularly significant because college students have, at least it should have, better computer skills than the rest of the population, and therefore we can assume that this data should be significantly higher than the rest part of population. The same statement we can assume about the habit to regularly clean visiting history: 43.1% say they rarely or never do it.

Managing and protecting personal data also involves respecting the privacy of others, especially when publishing personal data or photographs without permission. In this study we

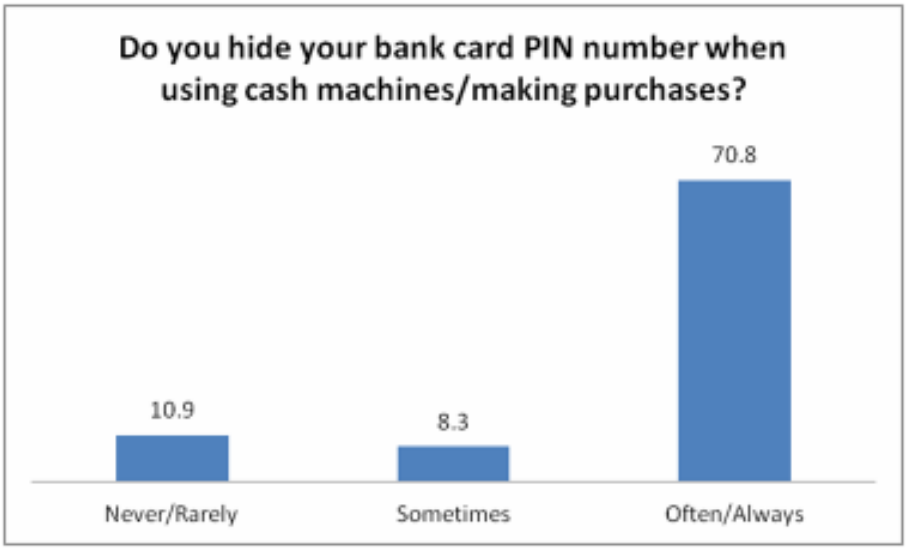

Figure 2. Do you hide your bank card PIN number when using cash machines/making purchases?

> “Not only in the Social Networking Sites (SNS) we leave traces about ourselves: every move on the net leaves a trail behind it”

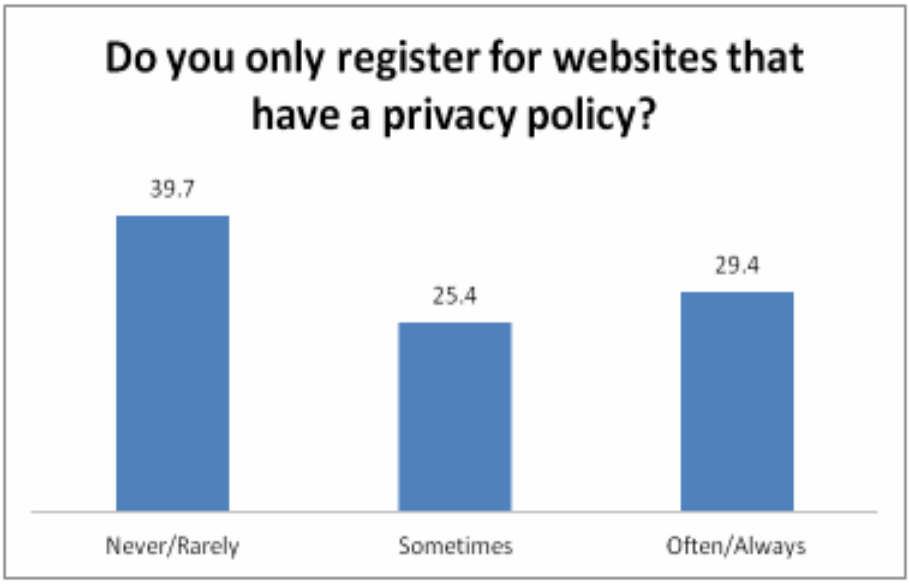

Figure 3. Do you only register for websites that have a privacy policy?

found that only 42.2% of the students always or almost always ask permission to others before posting a photo or video in which they appear. The risks are significant. Photos can, for example, thanks to the increasingly sophisticated technologies and through facial recognition software, turn into biometric identifiers. All these aspects can compromise the privacy and security of other users. And despite this, 37.1% of the sample, more than one person out of three, says that never ask permission to publish photographs or videos of others.

The practice of publishing news and personal information on others, although not usual, is present. In fact, 19.5% of respondents said that they sometimes publish information about others, and 6.6% do so often. Thus published information can damage privacy.

4. Notes for Reflection and Conclusion

The SNS questions the concept of "personal space" in its social meaning and personal and private data becoming public data through initiative coming from the users. To be more precise, as Royer, Deuker and Rannenberg say [23], the concept of privacy is moved from a static that affects only the privacy, to a dynamic process control limit that operates between subject and that which surrounds it. This significantly complicates the legislation of privacy protection. So far the privacy legislation protects the right to live in peace and from unfair treatment of personal data. Now, however, is the same user who voluntarily gives up their data, and there are few rules governing the publication of personal data in the context in which this transfer occurs with the consent of the citizens.

In this regard, two issues stand out clearly: the digital natives, born and raised in a computerized environment, are less aware of the risk to their privacy than those who come as adults to the world of Internet. The second point to be drawn from all this is that the same person is more careful of his/her privacy offline than online. In the network the citizen has less concerns to make public personal information. And yet, the online and offline worlds interpenetrate and interact with each other with continuous references.

Students underestimate the danger of privacy violation and the transfer of personal data because no attention is paid to the phenomenon of surveillance data-network [24]. The fact that the vast majority declare that the main visitors of their profile are their friends underline that they are not too worried about hiding information, so they do not worry about data because they have nothing to hide from friends. This makes the social network perceived as an instrument familiar and intimate and the cultural defences against the possible intrusion of strangers into their world, tends to decrease.

In this study, the students completely underestimate the role of marketing agencies that collect, analyse and link user data to build an online profile as faithful as possible. Less than one student in three noted that they always or almost always read the privacy policy before registering on a website. Two people out of three don’t show any interest in how their personal data will be treated and in the rules to manage their right to privacy.

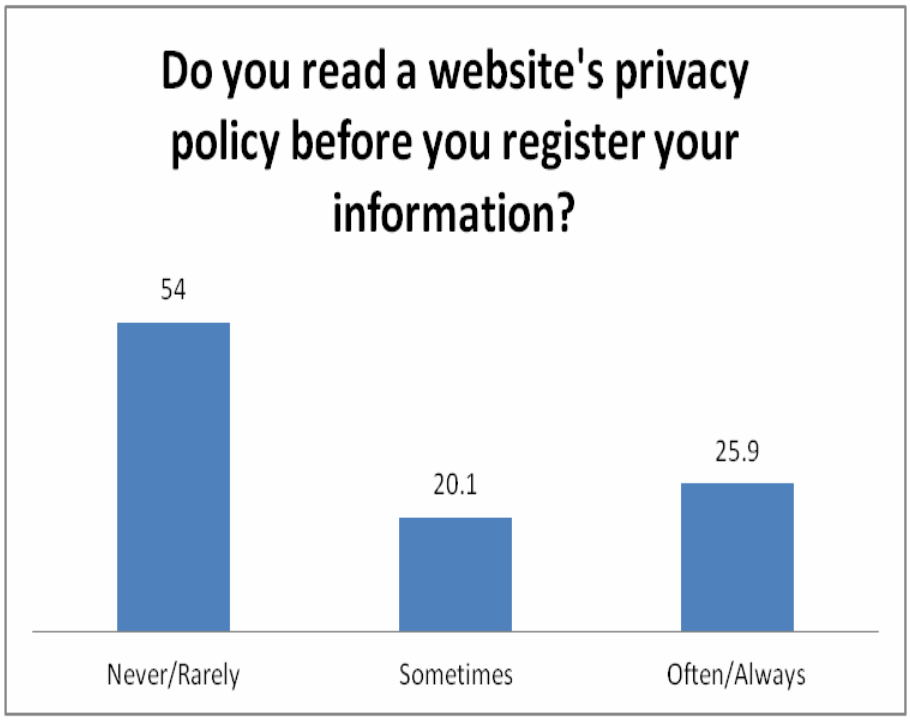

Figure 4. Do you read a website’s privacy policy before you register your information?

> "Two people out of three don't show any interest in how their personal data will be treated and in the rules to manage their right to privacy"

This research also reveals that there are two different ways of managing and protecting the privacy: lewd online and worried offline, as if the two worlds were far away, as if the data collected online were not useful for the surveillance system, that is more and more inclusive, and for the construction of an e-profile constantly informed by the citizens and the consumers. The new surveillance system keeps under observation, not only the people at potential risk, but all those who in some way release, voluntarily or not, personal data in the network.

Regardless of what this violation of privacy is, we are running the risk of turning our private lives in a "continuous public life" [25]. It is losing the separation between public life and private life, we are becoming vulnerable and we risk losing an important capital that gives value and importance to ourself and our relationships. The information we create and we give for free makes us controllable. It is the loss of the right to privacy that makes us more vulnerable and it makes difficult to build trust between individuals [26].

References

[1] D.M. Boyd, N.B. Ellison. "Social network sites: Definition, history, and scholarship". *Journal of Computer-Mediated Communication*, 13(1), 2007. Article 11, <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html> (Feb 27, 2012).

[2] R. Gross, A. Acquisti. "Information revelation and privacy in online social networks". *Proceedings of WPES'05* (pp. 71-80). Alexandria, VA: ACM, 2005, <http://rio.ecs.umass.edu/~lgao/ece697_10/Paper/privacy.pdf> (Feb 27, 2012).

[3a] S. Barnes. "A privacy paradox: Social networking in the United States", *First Monday*, V.11, N.9-4 Sept. 2006, <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312> (Feb 27, 2012).

[3b] F. Stutzman. "An Evaluation of Identity-Sharing Behavior in Social Network Communities". *International Digital and Media Arts Journal*, 3(1), pp. 10-18.

[3c] M.J. Hodge. "Comment: The Fourth Amendment and Privacy Issues on the 'New' Internet. Facebook.com and Myspace.com." *Southern Illinois University Law School Journal*, 2006, 31, pp. 95–122.

[4] A. Ho, A. Maiga, E. Aimeur. "Privacy protection issues in social networking sites". *Computer Systems and Applications*, Seventh ACS/IEEE International Conference, pp. 271-278, 2009.

[5a] W.S. Brown. "Ontological Security, Existential Anxiety and Work place Privacy". *Journal of Business Ethics 23*: pp. 61–65, 2000.

[5b] D. Nye. "The 'privacy in employment' critique: a consideration of some of the arguments for 'ethical' HRM professional practice". *Business Ethics: A European Review* (11:3): pp. 224–232, 2002.

[6] C. Fuchs. "Web 2.0, prosumption, and surveillance". *Surveillance & Society* 8 (3): pp. 288-309, 2011.

[7] J. Lawford. "Confidence, privacy and security". *OECD-Canada Technology Foresight Forum*, Session 4b, 2007, <http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf>. (Feb 27, 2012).

[8] P. Brey. "Disclosive Computer Ethics". En R.A. Spinello, H.T. Tavani (eds.): *Readings in Cyberethics*. Sudbury, Massachusetts et al.: Jones and Bartlett: pp. 51–62, 2001.

[9] L. Introna. "Privacy and the Computer - Why We Need Privacy in the Information Society". En R.M. Baird, R.R. Ramsower, S.E. Rosenbaum (eds.): *Cyberethics - Social and Moral Issues in the Computer Age*. New York: Prometheus Books: pp. 188–199, 2000.

[10] J. Rachels. "Why is Privacy Important," *Philosophy and Public Affairs,* vol. 4, 4, 1975.

[11] R. Spinello. *Cyberethics: Morality and Law in Cyberspace*. London: Jones and Bartlett, 2000.

[12] H. Tavani. "Privacy and Security". En D. Langford (ed.): *Internet Ethics*. London: McMillan: pp. 65–89, 2000.

[13a] D. Solove. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

[13b] F. Stalder. "Opinion. Privacy is not the antidote to surveillance". *Surveillance & Society* 1 (1): pp. 120-124, 2002.

[14] R. Turn. "Privacy Protection in Information Systems". En M.C. Yovits (ed.) *Advances in Computers*, 1977, p. 242.

[15] M. Ragnedda. "Social control and surveillance in the society of consumers". *International Journal of Sociology and Anthropology* Vol. 3(6), pp. 180–188, June 2011, <http://www.academicjournals.org/ijsa/PDF/pdf2011/June/Regnedda.pdf> (Feb 27, 2012).

[16] V.P. Zschunke. "*Mehr Informationen als die Stasi. Millionen von Internetnutzern drängen in soziale Netzwerke wie StudiVZ und Facebook*", *Berliner Morgenpost*, 23th January 2008, p. 9. <http://www.morgenpost.de/printarchiv/wissen/article160543/Mehr_Informationen_als_die_Stasi.html> (Feb 27, 2012).

[17] D. Lyon. *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Feltrinelli, Milano, 1997.

[18] G. Bousquet. "Space, Power, Globalization: The Internet Symptom". *Societies*, 4: pp. 105-113, 1998,

[19] M. Poster. *The mode of information: Poststructuralism and social context*. Chicago: University of Chicago Press, 1990.

[20] D. Lyon. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London–New York: Routledge, 2002.

[21] U. Gasser, J. Palfrey. *Born Digital - Connecting with a Global Generation of Digital Natives*. Perseus Publishing, 2008.

[22] epic.org. *Online Guide to Practical Privacy Tools*, <http://epic.org/privacy/tools.html> (Feb 27, 2012).

[23] D. Royer. A. Deuker, K. Rannenberg (Eds.). *The Future of Identity - Challenges and Opportunities*. Springer, Heidelberg, Germany, 2009.

[24] R. Clarke. "*Introduction to Dataveillance and Information Privacy, and Definitions of Terms*", 15th August 1997, <http://www.rogerclarke.com/DV/Intro.html>.

[25] S. Rodotà. *Intervista su privacy e libertà*, Laterza, Roma-Bari, 2005.

[26] D.G. Johnson. *Computer Ethics*. 3rd edition Upper Saddle River, New Jersey: Prentice Hall, 2001.