

Vol. 16 (12/2011)

## **Ethics of Online Social Networks**

edited by Antonio Marturano

### **Editor of this issue:**

**Dr. Antonio Marturano**

Sacred Heart Catholic University of Rome,  
Largo Francesco Vito, 1, I-00169 Rome, Italy

Email: [antonio.marturano@rm.unicatt.it](mailto:antonio.marturano@rm.unicatt.it)

### **Editors of IRIE**

**Prof. Dr. Rafael Capurro (Editor in Chief),**  
International Center of Information Ethics (ICIE)  
Redtenbacherstr. 9, D-76133 Karlsruhe, Germany  
E-Mail: [rafael@capurro.de](mailto:rafael@capurro.de)

**Prof. Dr. Johannes Britz,**  
University of Wisconsin-Milwaukee, USA and  
University of Pretoria, South Africa  
E-Mail: [britz@uwm.edu](mailto:britz@uwm.edu)

**Prof. Dr. Thomas Hausmanninger,**  
University of Augsburg, Germany,  
Universitätsstr. 10, D-86135 Augsburg  
E-Mail: [thomas.hausmanninger@kthf.uni-augsburg.de](mailto:thomas.hausmanninger@kthf.uni-augsburg.de)

**Dr. Michael Nagenborg,**  
IZEW, University of Tübingen,  
Wilhelmstr. 19, D-72074 Tübingen, Germany  
E-Mail: [michael.nagenborg@izew.uni-tuebingen.de](mailto:michael.nagenborg@izew.uni-tuebingen.de)

**Prof. Dr. Makoto Nakada,**  
University of Tsukuba, Japan,  
Tennodai, Tsukuba, 305-8577 Ibaraki  
E-Mail: [nakadamakoto@msd.biglobe.ne.jp](mailto:nakadamakoto@msd.biglobe.ne.jp)

**Dr. Felix Weil,**  
QUIBIQ, Stuttgart, Germany,  
Heßbrühlstr. 11, D-70565 Stuttgart  
E-Mail: [felix.weil@quibiq.de](mailto:felix.weil@quibiq.de)

Vol. 16 (12/2011)

**Content**

Editorial: On IRIE Vol. 16	1
Antonio Marturano: The Ethics of Online Social Networks – An Introduction	3
Caroline Rizza, Paula Curvelo, Inês Crespo, Michel Chiaramello, Alessia Ghezzi, Ângela Guimarães Pereira: Interrogating Privacy in the digital society: media narratives after 2 cases	6
Andrew A. Adams, Kiyoshi Murata, Yohko Orito and Pat Parslow: Emerging Social Norms in the UK and Japan on Privacy and Revelation in SNS	18
Daniel Skog: Ethical Aspects of Managing a Social Network Site: a Disclosive Analysis	27
Juan José Prieto Gutiérrez: Herramientas para el análisis y monitoreo en Redes Sociales	33
Richard A. Spinello: Privacy and Social Networking Technology	41
Sami Coll, Olivier Glassey and Claire Balley: Building social networks ethics beyond “privacy”: a sociological perspective	47
Michelle Kilburn: Why Individuals Choose to Post Incriminating Information on Social Networking Sites: Social Control and Social Disorganization Theories in Context	54
Eric Kyper and Roger Blake: Understanding the role of ethics in the intention to share files using P2P networks	60
Rafael Capurro: Never Enter Your Real Data	74
Sara L. Puotinen (Opinion Paper): Twitter Cares? Using Twitter to Care About, Care for and Care With Women Who Have Had Abortions	79
William Bülow (Opinion Paper): Pluralism about the Value of Privacy	85

## Editorial: On IRIE Vol. 16

What will go online next? That is a question many people ask for very different reasons. And the answers the short history of the internet has given to this question during the last years were very different as well. Different from what we expected. And even different from what we thought that would be possible to go online. Social relationships are a very good example for that. When the first connection between computers via the telephone net was established in 1969 and the word 'login' was wired from Stanford to UCLA (apparently the connection crashed on the letter 'g') no one has dreamt of a network that would be able to build and reflect social relationships. But exactly that is what social networks in the internet do. And don't get it wrong. It is not that social networks extended one's relationships to the net, made it easier to foster them or allow for a more efficient communication within relationships. It is the relationships themselves that went online and exist in and are constituted by the networks. Or, in allusion to McLuhan: 'The medium is the relationship'.

Social networks essentially consist of representations of their users (often a profile), his/her social links and a variety of additional services to facilitate the exchange of information between them. Most online social networks are web based and provide means for users to interact over the internet, such as e-mail (often in-build services), postings of various media content (pictorial, film, audio, textual etc.) and instant messaging. Although online communities are sometimes considered as a kind of online social network in a broader sense, online social networks usually mean an individual-centred service whereas online communities are group-centred. Such group-centred networks go back to 1979 when the first usenets were built. They were theme based and mainly impersonal. Social networks are very different.

Social networking sites allow users to share their personal ideas, activities, events, and interests with 'friends' – yes, in quotes as the meaning of friend did change from a very intimate one-to-one relationship to a connection established in a social network. The main types of social networking services are those which contain category places (such as former school-year or classmates), means to connect with friends (usually with self-description pages) and a recommendation system linked to trust. Popular methods now combine many of these; the most popular are Facebook, Twitter, MySpace and LinkedIn. Over the last few years, online social network sites became the most important phenomenon in the internet, in particular the explosion of Facebook, brought these new communicative ways to the edge of public opinion.

Accordingly, online social networks raise a variety of ethical and political concerns. Some of them are rather classical ones like privacy, access to information, potential for misuse, risk for child safety or censorship. Some of them are rather new like trolling, cyber bullying and cyber stalking or identity theft. And as usual the opinion is voiced loudly that relationships are compromised by the development outlined above and deteriorate increasingly. Thus, we see it as our foremost duty to first analyze, understand and explain the development before taking a moral stand. And we think this issue can shed some light on the questions concerned and bring some rationality into the debate. In any case we hope that it can contribute to your academic reasoning on the subject and we would be more than glad if it contributes to the fostering of our relationship as editors, authors and readers, as members of the academic community doing research in Information Ethics.

With regards to this we would like to introduce 2 new forms of publication that we want to offer in the future: Opinion Papers and Comments/Letters to the Editor:

- **Opinion Papers** will provide readers with focused coverage of topical issues in Information Ethics, which are of high current interest and potential. They need not fit into the subject of a current issue. We rather publish them with regards to their topicality. Thus, such Opinion Papers should be limited in length (~1.500 words including references) and need not take all relevant literature into account.
- **Comments/Letters to the Editor:** Comments/Letters to the Editor can be submitted anytime. They may not exceed 500 words and should focus on a specific article published in the current issue of IRIE. The authors of the article cited will be invited to reply. Letters and replies will be published simultaneously.

We are very happy to have already two very interesting Opinion Papers in this issue. And we do invite and encourage you to make further use of these additional offerings and look forward to your upcoming contributions.

And finally you may have noticed that we changed the format of the publication from two to one column; not because we changed our aesthetic concept. It is the technological development that triggered this modification. We were induced to the fact that the format consisting of two columns is not readable very well on e-book readers. Thus, while this kind of device is becoming more and more common on the one side and on the other side, it seems not to make any significant difference to classical readers if the format is not two columned anymore, we do not want to further disregard the needs of the users of these new kind of displays. If you disagree send us a comment and if you agree please let us know as well.

*Sincerely yours,*

*The editors.*

Antonio Marturano:

## The Ethics of Online Social Networks – An Introduction

According to a pioneering study,

*"When a computer network connects people or organizations, it is a social network. Just as a computer network is a set of machines connected by a set of cables, a social network is a set of people (or organizations or other social entities) connected by a set of social relationships, such as friendship, co-working or information exchange"<sup>1</sup>.*

The study of online social networks starts back to the beginning of the '90s when computer-mediated communications were then a cutting edge in growing computer-related research in LAN-networked organizations.

Unfortunately, most works focused on the social impacts of such technology and their ethical dimension did not meet much interest and still is not raising much interest beside privacy-related problems. Since these first studies, interests in online social networks have followed the fast expansion of the Internet and some ethical issues emerged. In his pioneering work, Howard Rheingold (1993) raises some ethical questions about online social networks such as right to privacy, net-dependence, how to build a social network's communitarian rules, intellectual property rights, personal identity, private firms intrusion into the Internet government<sup>2</sup>. Especially the latter problem has increasing importance and it is widely discussed outside the online social networks field, too<sup>3</sup>.

In 2008, the booming of Facebook and other popular social networks such as Twitter all over the world, has started to raise scholarship interests especially when Facebook and Twitter eventually became the standards for online social networking. While such phenomenon was studied only at the level of developed countries, ethical and political analyses were limited to the nature of social exchanges in such online social networks, too. In this context, according to Candler

*"Network websites are popular for two key reasons: firstly offering convenience and accessibility to large groups of people, and secondly their ability to define, promote and control perception of identity. It seems Facebook has provided the opportunity to maximise quantity and dilute quality as we hurriedly reach our social 'orgasm' through 15 second status updates, disingenuous photo comments and the ever superfluous 'poke'".<sup>4</sup>*

Marturano and Bellucci, on the other hand, argued that

*"Facebook is realizing what Guy Debord calls 'the invasive forces of the 'spectacle' - 'a social relation between people that is mediated by images': Facebook is seen as an alternative tool able to amplify an individual's alienation and narcissism, which, are a consequence of the mercantile form of social organization which has reached its climax in capitalism. Under Marxist theory, Facebook does not appear what Jaron Lanier claims to be collaborative communities".<sup>5</sup>*

The authors finally argue that, in mature capitalistic countries "Facebook is not (as Tapscott and Williams claim) a promising example of a new shift from capitalism to a new form of economy based on openness,

---

1 Garton, Haythornthwaite & Wellman, 1997

2 Rheingold (1993), cit., ch. 3.

3 For a good updated discussion, see Jack Goldsmith and Tim Wu (2008): *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford UP.

4 Candler (2010)

5 Marturano and Bellucci (2009)

peering, sharing and global action - which they called Wikinomics (Tapscott and Williams, 2006); but rather new disguised forms of advanced capitalism aimed at eroding space to more challenging modes of Internet collectivism". In fact, no revolution happened in any country with mature capitalistic economic system (such as Italy) despite the violent economic contraction caused by the continuing financial crisis and, at least in Italy, to the deep political corruption.

Many authors have, on the contrary, argued that online social networks have played a fundamental role in the recent North African revolutions and therefore boosted social collectivisation in those totalitarian countries. In most countries in the Arab world, Facebook is now one of the 10 most-visited Web sites, and in Egypt it ranks third, after Google and Yahoo. About one in nine Egyptians has Internet access, and around 9 percent of that group are on Facebook — a total of almost 800,000 members (Shapiro, 2009). According to Eunice Crook

*"the Jasmine revolution, a term rejected by Tunisians, but in fact it was and is a Facebook revolution ... everyone in Tunisia, from grandmothers down, now has a Facebook account. One colleague told me last week that everyone was so busy talking to their friends on Facebook each night that face to face family conversation had almost come to an end".<sup>6</sup>*

This flare-up of political activity coincided with the moment North-Africans were starting to gain access to the Internet in large numbers. Home computers and Internet cafes were becoming more popular, and the cost of getting online was dropping. Very importantly, new technologies and political movements grew symbiotically; Facebook and other online social networks became the main source of information for people's activism, which were largely ignored by the state-run media (Shapiro, 2009). Finally, social networking turned disaffected young Egyptians into a force for democratic change.

Such different outcomes in online social network uses are likely a reflection of different levels of totalitarianism and difference in culture, morality and religious framework. However an analysis of these phenomena falls outside the scope of this introduction which has the scope of offering new insights for debates in this area.

In this special issue I hope to have offered a place to bridging this ethical gap as we have collected here a huge number of papers which topics range from the problem of privacy to surveillance, from ethical issues of managing online social networks to file sharing ethical problems. While not exhaustive of the magnitude of ethical problems online social networks can offer, this selection will offer a close look to the most popular ones.

## Acknowledgments:

I would like to thank the following individuals who have kindly served as reviewers for this special issue:

Andrew Adams, Andy Bissett, Rafael Capurro, Gianmaria Greco, Fran Grodzinsky, Kenneth Himma, Soraj Hongladarom, Maosen Li, Marco De Marco, Keith Miller, Michael Nagemborg, Andrea North-Samardzic, Ugo Pagallo, Miguel Angel Perez Alvarez, Andrea Rossetti, Toni Samek, Ed Spence, Richard Spinello, Herman Tavani, Giuseppe Vaciago, Felix Weil, Pak Hang Wong, Michael Zimmer

## References

Rosanna Marie Candler (2010): *Facebook is to socialising what masturbation is to sex, Debating Communities and Networks 2010, Online Conference on Networks and Communities, Department of Internet Studies, Curtin University of Technology, Available at:*

---

<sup>6</sup> Eunice Crook (2011)

- <http://networkconference.netstudies.org/2010/04/facebook-is-to-socialising-what-masturbation-is-to-sex/>  
*Eunice Crook (2011): Tunisia: The Facebook Revolution, Available at:*  
<http://blog.britishcouncil.org/2011/02/tunisia-the-facebook-revolution/>  
*Laura Garton, Caroline Haythornthwaite and Barry Wellman (1997): Studying Online Social Networks, Journal of Computer-Mediated Communication, 3 (1) Available at:*  
<http://jcmc.indiana.edu/vol3/issue1/garton.html>.  
*Antonio Marturano and Sergio Bellucci (2009): A Debordian Analysis of Facebook, ACM SIGCAS Computers and Society, 39(3), p.59-68.*  
*Howard Rheingold (1993): The Virtual Community: Homesteading on the Electronic Frontier, Boston (MA): Addison Wesley.*  
*Samantha S. Shapiro (2009): Revolution, Facebook-Style - Can Social Networking Turn Young Egyptians Into a Force for Democratic Change?, New York Times, New York Edition, p. MM34, 25.01.2009. Available at:*  
<http://www.nytimes.com/2009/01/25/magazine/25bloggers-t.html?pagewanted=all>  
*Dan Tapscott and Anthony D. Williams, (2006): Wikinomics 2.0, London: Penguin*

Caroline Rizza, Paula Curvelo, Inês Crespo, Michel Chiaramello, Alessia Ghezzi, Ângela Guimarães Pereira:  
**Interrogating Privacy in the digital society: media narratives after 2 cases**

**Abstract:**

The introduction of information technology (IT) in the society and its pervasiveness in every aspect of citizens' daily life highlight societal stakes related to the goals regarding the uses IT, such as social networks. This paper examines two cases that lack a straightforward link with privacy as addressed and protected by existing law in Europe (EU) and the United-States (USA), but whose characteristics, we believe fall on other privacy function and properties. In Western societies, individuals rely on normative discourses, such as the legal one, in order to ensure protection. Hence, the paper argues that other functions of privacy need either further framing into legislation or they need to constitute in themselves normative commitments of an ethical nature for technology development and use. Some initiatives at the EU level recall such commitments, namely by developing a normative discourse based on ethics and human values. We argue that we need to interrogate society about those normative discourses because the values we once cherished in a non-digital society are seriously being questioned.

**Agenda:**

Models of Privacy and/in Legal Provisions	8
Beyond personal data: two tales in the news media	11
Weinergate	12
Puddick "Online Harrassment"	13
Discussion: privacy concerns in the two cases	14
Making a case for privacy in the two cases	14
Technologies of privacy	15
Towards an ethics of social networks	15

**Authors:**

Dr. Caroline Rizza

- European Commission, Joint Research Centre (JRC), Institute for the Protection and the Security of the Citizen (IPSC). Via Enrico Fermi 2749 - I-21027 Ispra (VA) – Italy.  
 ☎ + 39 - 0332 - 78 97 46 , ✉ [caroline.rizza@jrc.ec.europa.eu](mailto:caroline.rizza@jrc.ec.europa.eu), 🌐 <http://ipsc.jrc.ec.europa.eu/>
- Relevant publications:
  - Rizza, C. (2012, forthcoming), "Digital competences", Encyclopedia of Quality of Life Research, Springer.
  - Rizza, C. (2012, forthcoming), "Digital divide", Encyclopedia of Quality of Life Research, Springer.
  - Rizza, C. & Mahmoud, S. (2011). « Les potentialités du web 2.0 dans le domaine de l'apprentissage : simple effet de mode ou véritable enjeu pour l'éducation ? », in Apprentissage Ubiquitaire et Web 2.0 , Bonfils, P., Pieri, M. , & Dumas P. (Ed.), Paris, L'Harmattan.

Paula Curvelo

- European Commission, JRC, IPSC. Via Enrico Fermi 2749 - I-21027 Ispra (VA) – Italy.
- ☎ + 39 - 0332 - 78 94 01, ✉ [paula.curvelo@jrc.ec.europa.eu](mailto:paula.curvelo@jrc.ec.europa.eu), 🌐 <http://ipsc.jrc.ec.europa.eu/>

## Inês Crespo

- European Commission, JRC, IPSC. Via Enrico Fermi 2749 - I-21027 Ispra (VA) – Italy.
- ☎ + 39 - 0332 - 78 91 55, ✉ [ines.crespo@jrc.ec.europa.eu](mailto:ines.crespo@jrc.ec.europa.eu), 💻 <http://ipsc.jrc.ec.europa.eu/>
- Relevant publications:
  - De Sousa Brilhante Pedrosa T., Orfao Crespo I., and Guimarães Pereira Â. (2009). Media Analysis: EMM Application to CPSI Framework. EUR 23778 EN. Luxembourg (Luxembourg): OPOCE; 2009. JRC50765

## Michel Chiaramello

- European Commission, JRC, IPSC. Via Enrico Fermi 2749 - I-21027 Ispra (VA) – Italy.
- ☎ + 39 - 0332 - 78 57 81, ✉ [michel.chiaramello@jrc.ec.europa.eu](mailto:michel.chiaramello@jrc.ec.europa.eu), 💻 <http://ipsc.jrc.ec.europa.eu/>

## Alessia Ghezzi

- European Commission, JRC, IPSC. Via Enrico Fermi 2749 - I-21027 Ispra (VA) – Italy.
- ☎ + 39 - 0332 - 78 92 44, ✉ [alessia.ghezzi@jrc.ec.europa.eu](mailto:alessia.ghezzi@jrc.ec.europa.eu), 💻 <http://ipsc.jrc.ec.europa.eu/>

## Dr. Ângela Guimarães Pereira

- European Commission, JRC, IPSC. Via Enrico Fermi 2749 - I-21027 Ispra (VA) – Italy.
- ☎ + 39 - 0332 - 78 53 40, ✉ [angela.pereira@jrc.ec.europa.eu](mailto:angela.pereira@jrc.ec.europa.eu), 💻 <http://ipsc.jrc.ec.europa.eu/>
- Relevant publications:
  - Guimarães Pereira, Â. and Funtowicz, S. (2009). Science for Policy. Oxford: Oxford Univ. Press.
  -

*The content of this paper does not reflect the official opinion of the European Commission. Responsibility for the information and views expressed lies entirely with the authors.*

In the Western digital society, many initiatives to protect privacy are being set either through regulatory mechanisms, practice or just changes of “jargon” in order to align the legal discourse with other normative discourses. Concurrently, the news media often report cases where many functions, properties and dimensions of privacy are not being adequately resolved by current provisions in law; most importantly is that those would need thorough societal reflection before being transposed into the legal discourse. A myriad of authors (e.g. De Hert and Gutwirth, 2006; Pouillet, 2010; Andrade, 2011) have devoted a great deal of attention to study current provisions of European Union (EU) law on privacy matters. We found through two recent cases of social media usage that many privacy functions and properties are neither contemplated in the law nor even articulated in the normative discourses that permeate society, namely those echoed by news media.

This paper first offers a brief review of models and foundations of privacy, followed by a description of legal provisions both in the EU and United States of America (USA); it then looks at the two cases that have inspired this work, the Weiner case in the USA (e.g. Klein, 2011; Pershing, 2011) and the Puddick case in the United Kingdom (UK) (e.g. Blake, 2011a; Davies, 2011). Albeit those are different stories about technology usage, they share that none of them has been framed in the media’s narratives as a privacy case. For the former the media concentrated on IT operational aspects which compromised Mr. Weiner’s public image whereas in the latter case, the news media mainly focused on the results of the court case arising from the use of social media by Mr. Puddick.

However, when looking at privacy foundations literature, we are surprised that many of these functions have been disregarded along the storyline of the cases and not even being alluded to by news media. Hence, in this paper we describe what the media discourses were for the two cases. We argue that those narratives are not contemplate issues of privacy. Moreover, we also suggest that the existing EU legislation could have been used to address the Puddick court case. Finally, we argue that, as in many other fields, a thorough discussion of values and ethics that we as humans want to preserve or develop within the technological endeavour needs to be settled and the trinomial technology-law-ethics needs urgent articulation.

## Models of Privacy and/in Legal Provisions

The concept of privacy constitutes a relatively new concept in the development of contemporary law (De Hert and Gutwirth, 2006) even if it has broad historical roots in philosophical, political, sociological and anthropological discussions (DeCew, 2008). Two important theories have been influencing the meaning and value of privacy within the western political tradition, which are considered to be the most authoritative by several authors (Pedersen 1999; Carew and Stapleton 2005; Joinson and Paine 2007; Margulis 2011).

The first one, developed by Westin (1967), defines privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (*Idem*). This conception focuses on informational privacy (a subset of social interaction) and includes “the voluntary and temporary withdrawal of a person from the general society through physical or psychological means” (*Ib. idem*). For Westin, the concept of privacy, i.e. the need for the ‘opacity’ of the individual, is not an end in itself, but a means to achieve the overall end of self-realisation. According to this conception, Westin postulates four functions and four states of privacy, as presented in Figure 1.

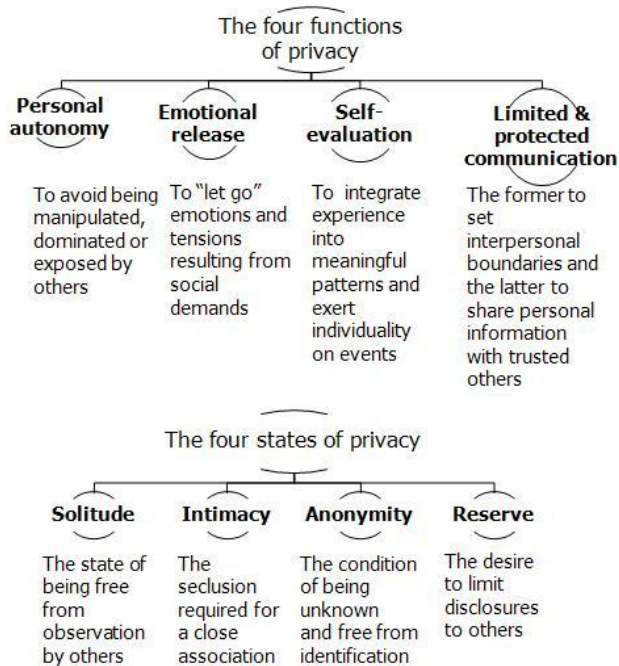


Figure 1. Westin's conception of privacy (1967): the four functions and states of privacy

The second theory, developed by Altman (1975), defines privacy as "the selective control access to the self" (1975, p. 24). The social interactions, the social and physical environment and the cultural context are considered fundamental features to understand the different properties of privacy and the multiple behavioural mechanisms for its regulation. Carew and Stapleton (2005) show that in Altman's theory, privacy has five properties, among which the "units of privacy" referring to two levels of privacy can apply: individual or group (Figure 2).

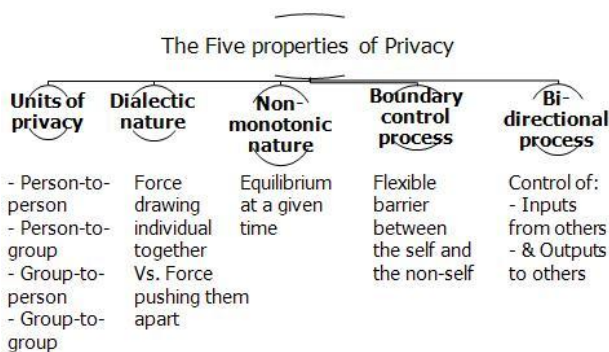


Figure 2. Altman's conception of privacy (1975): the five properties of privacy

The main difference between these two theories results from the emphasis that Altman gives to social interaction, which leads to a more inclusive conception of privacy. Besides that, these two theories share several commonalities (see Margulis, 2011, p.15).

In the present paper, these theories serve the purpose of introducing the discussion around the dominant conception of privacy in a digital society and how this conception has been changing with the pervasiveness of information technology (IT) in the society, e.g. social networks. It is a truism that IT has been impacting citizens' daily life but the privacy meanings need to be interrogated. In particular, the means so far implemented to defend and protect what we could call an "ethical" conception of privacy.

According to De Hert and Gutwirth (2006) the development of the democratic constitutional state has led to the invention of two complementary legal tools of power control: 1) the normative opacity tools that draw the limits of interference with individuals, and 2) the transparency tools that organize the channelling, control and restraint of power. For the authors, privacy is an example of an opacity tool, which sets normative limits to powers, while data protection can be mainly seen as a transparency tool, which regulates and channels necessary, reasonable and legitimate power.

Whilst data protection is a pragmatic concept in its nature and a means to protect individuals' privacy (De Hert and Gutwirth, 2006; Pouillet, 2010) protecting the value and interest of privacy as it protects the value and interest of identity, security and freedom of information, among others (Andrade, 2011, p.98), it also constitutes a limited proxy to address other functions and properties of privacy. As we will see much of the current EU and USA legal discourses are based on data protection as a proxy for privacy protection.

In the remaining of this section we look at how models of privacy have been articulated in the legal systems of both EU and USA for online communications. The way legislation defines and protects privacy differs strongly among those regions, and in particular for the former there are great differences between the Member States (MSs). Referring to the theoretical models of privacy presented earlier, this distinction is easily understandable since the conception of privacy, as an "opacity tool", has been constructed in diverse social, physical and cultural contexts. Therefore, resulting differences of privacy conceptions have also influenced the "transparency tools" adopted, such as personal data protection legislation, implemented to protect privacy or other values.

In the USA, privacy is not explicitly protected by the Constitution or by one unique federal law but it is considered as a valued right (Strauss and Rogerson, 2002; KWR GmbH, 2006). The Privacy Act (1974) regulates how the government can collect American citizens' personal data. At the level of the State, only California has enacted a set of laws protecting its residents' privacy such as the "California Online Privacy Protection Act" (2003) that requires the publication of a privacy policy by operators collecting personal data through Internet (KWR GmbH, 2006). For the IT private sector, a few narrow industry-specific federal laws can be applied. Especially, the "Fair Information Principles" or "Practices" guide privacy policy for this sector. These principles cover five aspects: "notice", "choice", "access", "security" and "contact" (Strauss and Rogerson, 2002, pp. 177-178) – see Figure 3. Organizations are not required to observe these principles; nevertheless they are used as benchmarks for evaluating data collection and privacy protection since 1980.

<b>At the Federal Level</b>	The Privacy Act (1974)
	Sectorial approach (specific Laws) for the private sector
<b>The fair Information Principles (or Practices) For the Private sector but has also influenced the Privacy Act</b>	<b>"Notice":</b> "a data-collector clearly tells the subject exactly what information is being collected, how it is collected, how that information will be used, and with whom it will be shared";
	<b>"Choice":</b> "allows consumers to actually exercise control over the use of their data"
	<b>"Access":</b> "allows individuals to easily review the information that has been collected about them. (...) The privacy policy should describe how an individual could request a correction".
	<b>"Security":</b> "requires data collectors to protect their gathered information, both during transmission and storage"
	<b>"Contact":</b> "fair information practices require that collectors provide subjects with reliable "contact" information"
<b>At the States' level</b>	The California Online Privacy Act (2003) and others specific laws - <i>California is the only State having enacted such kind of law.</i>

Figure 3. Personal data protection in the United-States

In the EU, personal data protection is both regulated and institutionalized (Strauss and Rogerson, 2002). The regulation has been implemented since 1981 with the convention for the "Protection of individuals with regard to automatic processing of personal data" by the Council of Europe. A set of European Directives have followed as a way to respond to the progress in the technological field, and have been covering a set of principles, all presented in the Figure 4. These Directives respectively aim to provide a uniform level of

data protection in the European Union and in particular of privacy, as well as to facilitate the free flow of personal data in Europe (Strauss and Rogerson, 2002; Kuczerawy, 2010; KWR GmbH, 2006).

The EU Directives	<p><b>The Directive 95/46/EC</b> on the "Protection of individuals with regard to the processing of personal data and on the free movement of such data" (1995);</p> <p><b>The Directive 2002/58/EC</b> (the E-Privacy Directive) on the specific problems &amp; risks of personal data processing in connection with electronic communication;</p> <p><b>The Directive 2009/136/EC</b> on "Processing of personal data and the protection of privacy in the electronic communications sector and Regulation".</p>
The core Principles of the Directives	<p><b>Identical to the Fair Information Principles:</b> Notice - Choice - Access - Security - Contact</p> <p><b>Adequacy objectives/means:</b> Personal data processing shall be accurate, adequate, relevant and not excessive in relation to the purposes for which it is processed;</p> <p><b>Specific to EU context</b></p> <p><b>Duration:</b> Personal data processed shall not be kept longer than necessary;</p> <p><b>Nature of the data:</b> The grounds to rely on when processing personal data differ depending if the data is sensitive or not;</p> <p><b>Competent Authority:</b> Processing shall be notified to and/or authorized by the relevant Data Protection Authority;</p> <p><b>Transfer:</b> Personal data, after processing, shall not be transferred to countries outside the EU (and the EEA) without adequate protection, unless permitted by law and/or by the Data Protection Authority.</p>
At the Member States Level	<p><b>Responsibility</b> of each Member State for the implementation of the directives</p> <p><b>A national agency</b> is responsible for the respect of the minimum level of protection ensured by these principles.</p>

Figure 4. Personal data protection in Europe

The institutionalisation in each MS is ensured by the establishment of a data protection commissioner, assigned to a ministry or agency that implements at national level the set of regulations and principles (Strauss and Rogerson, 2002; KWR GmbH, 2006).

In the UK, the Data Protection Act (1998) implements the Directive 95/46/EC. It has been amended in by the Freedom of Information Act (2000) to give a right of access to personal data held by public authority, subject to exemptions (KWR GmbH, 2006). Other legislation is relevant to the use of personal data, as shown in Figure 5.

The United-Kingdom	<b>The Data Protection Act (1998)</b> implements the Directive 95/46/EC
	<b>The Human Rights Act (1998)</b>
	<b>The Freedom Protection Act (2000)</b>
	<b>The Regulation of Investigatory Powers Act (2000)</b> about personal data used in telecommunications
	<b>The Privacy and Electronic Communication (EU Directive) Regulation (2003)</b> has provisions dealing with monitoring telecommunications such as the use of Internet

Figure 5. Personal data protection in the United-Kingdom

The recent revision of the e-privacy Directive and the current revision of the Directive 95/46/EC shed light on the difficulties to address the stakes related to technology pervasiveness and daily privacy concerns. Additionally, it addresses the difficulties to express privacy resonating the specificity of emerging Internet applications, and social networks, in particular (Poullet, 2010).

## Beyond personal data: two tales in the news media

The two cases chosen to illustrate our research are strongly related with inter-personal communication supported by social networks. These are the so called, Weinergate (e.g. Klein, 2011; Pershing, 2011) and

the Pudick case (e.g. Blake, 2011a; Davies, 2011). We consider that these two cases have raised privacy issues with regard to the Westin's conception of privacy presented earlier.

The stories in these cases are being looked at from the point of view of the news media narratives, i.e. what the media echo and comment. The cases were heavily reported in the news media, commented in the blogosphere and the kinds of reactions that those stories provoked in the media and in the public ultimately resonate the ways in which technology, in particular "social networks" are raising awareness of how ethical and moral values that once were taken for granted became now moot questions, e.g. privacy (Walther, 2011), reputation (Solove, 2007), etc.

Through these cases we are looking at the narratives about privacy and ethics as portrayed by the news media embracing van Dijk's idea that "the construction of news is most of all a reconstruction of available discourses" (van Dijk, 1983, p. 28).

The 2 case studies have been picked up from the European (UK) and USA contexts. In order to determine how the media has treated them, we selected three national (on-line versions) newspapers: The Independent, The Guardian, The Financial Times for the United-Kingdom and The New York Times, The International Herald Tribune and the Washington Post for the USA. We collected news using keyword search in the newspapers sites. The public commentary to the news articles has also been scrutinised.

## Weinergate

Anthony Weiner is a former U.S. Democratic Congressman, serving New York's 9th District from 1999 until 2011. On May 2011, the congressman mistakenly published in his public Twitter account a lewd picture of himself. Weiner deleted the picture after some minutes, but it was long enough for a conservative group to discover it and publish it in Andrew Breitbart's blog<sup>1</sup>. After several days of denying he had posted the image and saying his account had been "hacked", he admitted to having sent sexually explicit photos and messages to about six women over a three-year period, both before and during his marriage. He denied having met, or having had a physical relationship with any of the women. On June 16, 2011, Weiner announced his resignation from Congress.

### THE FRAMING OF THE CASE IN THE MEDIA

In Weiner's case, the technology potentiated and facilitated diverse steps of the case.

First, Twitter facilitated Weiner's affairs, which decades back would have demanded a different process, longer times, and reflections.

*"So where does Anthony Weiner fit in? A generation ago, we couldn't have had a sex scandal based on Facebook messages, tweets and e-mails. That's progress, of a sort." (Klein, 2011).*

Second, Weiner's use of Twitter intertwined his personal (private) and professional life. While his Twitter name related to his profession - @RepWeiner, and included links to his campaign website, Weiner was using the technology to carry out personal relationships.

"Like many lawmakers, Weiner tweets a mix of personal and political observations. His Twitter user name — @RepWeiner — identifies him as a member of Congress. But his Twitter page links to his campaign Web site, not his official House site" (Pershing, 2011).

Third, Twitter potentiated error. A basic flaw (leaving out a "d") transformed a private message in a public one.

---

<sup>1</sup> Andrew Breitbart is a conservative blogger, publisher and commentator for the Washington times.

"Here we see a character flaw meeting a design flaw. The mistake was Weiner's – he hit the wrong key, an "@" instead of a "D," and thus sent the lewd photo to tens of thousands of people instead of one. But a good technology assumes operator error, and has built-in corrections or failsafes. A robust system presumes that dopes will grab the controls" (Achenbach, 2011).

Fourth, Twitter enabled user's activities tracking.

"Conservative group #BornFreeCrew had for weeks before the "Weinergate" scandal closely monitored who the congressman was following on Twitter, and even urged young women to stay away from him, according to Slate. (...) Dan Wolfe, the man who discovered Weiner's crotch shot and sent it to conservative blogger Andrew Breitbart (...) [had] for weeks promised that a scandal was coming" (Flock, 2011).

Fifth, Twitter facilitated the perverse proliferation of posts about the case, multiplying the number of people looking at his private life (Sargent, 2011a; Petri, 2011).

"I enjoy Twitter as much as the next fellow, but if there's one conclusion you can draw from Weinergate, it's that Twitter — in addition to all its virtues — can encourage and reinforce pack journalism's very worst instincts. The unfolding of Weinergate on Twitter was a deeply dispiriting spectacle. There were times when the wall of puerile and adolescent Tweets about Weiner grew impenetrable. Anyone reporting and Tweeting on any other topic could be assured that it would get entirely lost." (Sargent, 2011b).

*"A generation ago, we would've been doing something more productive than looking at Weiner's Facebook posts, tweets and e-mails." (Klein, 2011).*

Last, but not least the private pictures were sent to these women in a private context (even though using Twitter), but IT potentiated the exposure of private life with consequent damage for Weiner's reputation.

### **Puddick "Online Harrassment"**

Ian Puddick, a self-employed plumber from Enfield, north London, UK was accused of "online harassment" after using a variety of social networks and a series of websites to expose his wife's affair with her boss (Mr. Haynes), a director from a leading global reinsurance company. The prosecution claimed that Ian Puddick's actions to expose his wife's affair forced the director to resign from his post. After a three-day trial at the City of Westminster Magistrates' Court, Ian Puddick was cleared of two charges of Internet harassment. This recent case was followed by legal and media experts, since it raised important questions over the limits of online freedom of speech and the regulation of what is disseminated through Internet and, particularly, via social network websites.

The framing of the case in the media

In the Puddick case, social networks were used to damage the reputation, to distress and to shame a man involved in adultery.

First, the media describes a clash between technology and regulation, equating discourses of freedom of speech and Internet regulation.

"The case is being followed by legal and media experts as the battle to regulate what is disseminated through websites and on Twitter is waged in the courts. Recent cases involving injunctions have also raised questions over freedom of speech and the regulation of the internet" (The Guardian, 2011)

"Lawyers believe the three-day hearing could help define the limits of free expression online" (The Independent, 2011)

"The landmark case has renewed interest in the clash of technology and the legal system as information is spread via unregulated social media sites." (Blake, 2011a).

Second, technology is not deemed protective of all users; reach out and speed at which Internet proliferates information, appropriation of identity, etc. As for the Weinergate case, IT potentiated the exposure of private life with consequent damage for the actors involved.

"Mr. Haynes told the court: 'I think most of the country, thanks to the Internet, is aware I had an affair'." (Blake, 2011a)

"[Mr Haynes] 'embarrassment and shame' after (...) clients were contacted through fake profiles on social networking site LinkedIn." (Idem.)

Third, the media is not concerned with the moral of Mr. Puddick's endeavour to get his wife back. The title of a photo published in Davies (2011) suggests that any purpose justifies the means. In fact Mr. Puddick was cleared from two harassment charges.

"It is absolutely a victory for free speech and the small man. I'm a plumber and drive a Transit." (Davies, 2011).

Finally, the media takes stock of the case inspiring government to take action regarding cyberstalking, as well as social networks regulation.

"outdated cyberstalking laws [... this] was prompted by a flurry of recent cases in which stalkers have used texts, tweets, chatrooms and sites such as Facebook to intimidate their victims" (Blake, 2011b).

## Discussion: privacy concerns in the two cases

### Making a case for privacy in the two cases

The media discourses did not use the "privacy" lens in both cases; they seem to be centred on moral aspects, as well as on vulnerabilities of people grappling with the effects of unregulated and un-discussed ethics of social networks.

Westin's (1967) conception of privacy, which distinguishes four functions and states of privacy, interest both cases. In the Weinergate case, privacy was put at jeopardy with Weiner's involuntary misuse of technology: the "reserve state" defined as "the desire to limit disclosures to others" was defied due to mistaken use of Twitter. Twitter is not deemed ergonomically respectful of one's "limitation and protection of communication", one of Westin's privacy functions. In the Puddick case, three of Westin's states of privacy were put at jeopardy when Mr. Puddick published his wife's affair in an attempt to ruin her lover's reputation through social networks: "solitude" – the state of being free from observation by others, anonymity and reserve, "anonymity" – the condition of being unknown and free from identification – and the state of "reserve". We argue that Mr. Puddick's wife and her lover have been deprived from their "personal autonomy" (one of the functions of privacy) since they were "manipulated, dominated and exposed" by him.

One of the outstanding issues in these cases is that neither Mr. Weiner nor Mr. Haynes could control both the disseminated information and subsequent interaction. In Altman's (1975) properties of privacy, this maps on "non-monotonic nature of privacy" and "boundary regulation process" since in both cases the technology caused either involuntary error, or unawareness about publication of one's private facts, or even identity theft. Moreover, as far as units of privacy are concerned we have here a conflict between the person-to-person unit and person-to-group one. In the Puddick case, this arises because he decided to make public a private matter involving three people. In the Weiner case, media news considered naïf Weiner's expectations that online private conversations could remain that way.

Yet, narratives of privacy are not used in the relevant media news regarding the two cases; a possible explanation is that current privacy does not contemplate further functions or units of privacy other than those expressed in data protection initiatives. Having said that, we find it interesting that at the light of existing EU regulation the Puddick's court case were not treated as a privacy matter for two reasons. First, if

someone's identity is falsified or an erroneous public image of his/her personality is conveyed to others, we have a case for identity infringement (Andrade, 2011) - Mr. Puddick had created a false identity in LinkedIn to connect to Mr. Hayne's acquaintances and further defame him. Andrade and other authors argue that privacy is infringed "if true private facts related to a person are revealed to the public". Mr. Puddick was "cleared of harassing his wife's millionaire lover on the Internet" (Davies, 2011); he was absolved on the grounds that he had published true facts about his wife's lover, which therefore made it a case for free speech under UK law.

Second, given that Directive 95/46/EC automatically qualifies any person as a data controller when he/she publishes personal data about others in social networks, Mr. Puddick could have been qualified as such. Hence, all provisions regarding personal data processing could apply. And were the blogger in Mr Weiner case in Europe, the same reasoning could apply.

Even if the media accounts of those two cases were not framed in privacy narratives, we would argue that they are strongly framed in privacy issues, and at least the Puddick case could have been already addressed through existing regulation. Finally, it should be interesting to investigate why other less articulated ethical framings (e.g. reputation, identity, etc.) did not emerge in the media news. A likely possibility is that our conceptions of privacy are being questioned and are no longer warranted.

### **Technologies of privacy**

Poullet (2010) illustrated that in order to ensure proper protection of values such as privacy, an alignment of technology and regulation has to be sought. In these two cases the technology did not provide mechanisms to the users to protect their privacy – e.g. providing functionality to give consent to others to publish about oneself and redundancy or "undo" functions. Some could think that the technology is not at stake here, since people should be knowledgeable of its workings, before using it. But we sustain that this type of idea is a shift of burden, since the technology should be conceived from the start to comply with users' expectations of (privacy) self-protection.

Walther (2011) argues that there are three factors that are confronting online users and their expectations: 1) misplaced presumption that online behaviours are private; 2) that the Internet nature is incommensurate with privacy as we know it; and 3) that one's faith that private online "conversations" remain as such. Whether or not we concur with these ideas, technology is not to be taken for granted as far as protection of privacy is concerned; the two cases illustrate that technology did not protect the actors involved. In other words, it did not shield them from involuntary exposure due to either mistaken IT use, or to lack of control of published personal information.

### **Towards an ethics of social networks**

Scholars of science and technology studies have long demonstrated the co-evolution of technology and society (e.g. Latour, 1992; Jouët, 1993; Jasanoff, 1995). Feenberg (2010) articulates this as a democratic paradox: "the public is constituted by the technologies that bind it together but in turn it transforms the technologies that constitute it". With this realization, von Schomberg (2007) argues that the classical ethical theory and the conventional ethical practice do not address both aspects of unintentional side consequences and collective decisions that should be taken into account while considering the issues of ethical responsibility in scientific and technological developments. Hence, as with many emergent technologies, we are left with old narratives, meanings and rules to deal with quite different phenomena and their anticipated and unintended effects.

There are some initiatives attempting to deal with current critique of technology contempt of ethical and societal concerns. For example, in the EU, proposals for developing technology embodying "ethics by design" or "privacy by design" paradigms (European Commission, 2010, p. 12), or proposals for placing changes in regulation that currently implement traditional ethical concerns, such as Poullet's (2010) ideas of Internet as virtual dwelling. Von Schomberg (2007) proposes an ethic of co-responsibility, that should arise

from reflection on the social processes in which technological decision making is embedded and which presupposed the following four requirements: public debate; technology assessment; constitutional change; and foresight and knowledge assessment.

Therefore, we reckon we need a deeper interrogation of the current meanings of privacy and other ethics, how they map onto the information and communication narratives, their function in society as well as their stakes. Thorough discussions on ethics of IT and in particular of social networks need to be urgently set.

## References

- Achenbach, J. (2011). "Anthony Weiner: Character flaw meets design flaw". *The Washington Post Blogs*, available at: [http://www.washingtonpost.com/blogs/achenblog/post/anthony-weiner-character-flaw-meets-design-flaw/2011/06/09/AGZci8MH\\_blog.html](http://www.washingtonpost.com/blogs/achenblog/post/anthony-weiner-character-flaw-meets-design-flaw/2011/06/09/AGZci8MH_blog.html). Published: June 9.
- Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, and crowding*. Monterey, Brooks/Cole Publishing Company.
- Andrade, N.N.G.d. (2011). "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights". *Privacy and Identity Management for Life - IFIP Advances in Information and Communication Technology*, 352: 90-107.
- Blake, M. (2011a). "'Online harassment' over affair leads to landmark court case". *The Independent*, available at: <http://www.independent.co.uk/news/uk/home-news/online-harassment-over-affair-leads-to-landmark-court-case-2298064.html>. Published: June 16.
- Blake, M. (2011b). "Government to launch inquiry into 'outdated' cyberstalking laws". *The Independent*, available at: <http://www.independent.co.uk/news/uk/crime/government-to-launch-inquiry-into-outdated-cyberstalking-laws-2299286.html>. Published: June 18.
- Carew, P. J. and L. Stapleton (2005). *Towards a Privacy Framework for Information Systems Development. Information Systems Development: Advances in Theory, Practice and Education*. O. Vaselicas, A. Caplinskis, W. Wojtowski et al. New York, Springer Science + Business Media: 77-88.
- Davies, C. (2011). "Plumber Ian Puddick cleared of harassing wife's lover on internet". *The Guardian*, available at: <http://www.guardian.co.uk/uk/2011/jun/17/ian-puddick-internet-cleared-twitter>. Published: June 17.
- DeCew, J. (2008). "Privacy" *The Stanford Encyclopedia of Philosophy*, available at: <http://plato.stanford.edu/archives/fall2008/entries/privacy/>.
- De Hert, P. and Gutwirth, S. (2006). *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*. In *Privacy and the criminal law*. E. Claes, A. Duff and S. Gutwirth. Antwerp/Oxford, Intersentia: 61-104.
- European Commission. (2010). "A comprehensive approach on personal data protection in the European Union". Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final. Available at: [http://ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf).
- Feenberg, A. (2010). "Ten paradoxes of Technology." *Techné* 14(1): 3-15.
- Flock, E. (2011). "#BornFreeCrew: The group who warned about Weiner". *The Washington Post*, available at: [http://www.washingtonpost.com/blogs/blogpost/post/bornfreecrew-the-group-who-warned-about-weiner/2011/06/20/AGE8L2cH\\_blog.html](http://www.washingtonpost.com/blogs/blogpost/post/bornfreecrew-the-group-who-warned-about-weiner/2011/06/20/AGE8L2cH_blog.html). Published June 21.
- Jasanoff, S. (1995). *Science at the Bar: Law, Science, and Technology in America, a Twentieth Century Fund book*. Cambridge, MA: Harvard University Press.
- Joinson, A. N. and Paine, C. B. (2007). *Self-disclosure, privacy and the Internet*. In *The Oxford Handbook of Internet Psychology* A. N. Joinson, K. McKenna, T. Postmes and U.-D. Reips. New York, Oxford University Press: 237-252.
- Jouët, J. (1993). « Pratiques de communication et figures de la médiation ». *Réseaux*, 11/60, 99-120.
- Klein, E. (2011). "A techno-history of Congress". *The Washington Post Blogs*, available at: [http://www.washingtonpost.com/business/economy/a-techno-history-of-congress/2011/06/13/AGwLBITH\\_story.html](http://www.washingtonpost.com/business/economy/a-techno-history-of-congress/2011/06/13/AGwLBITH_story.html). Published: June 14.

- KWR Gmbh. (2006). *Data Protection in the European Union and other Selected Countries: A New Comparative Study*. [http://www.kwr.at/fileadmin/res/pdf/publikationen/mag-arno-cichocki/10541\\_Data\\_Protection\\_Austria.pdf](http://www.kwr.at/fileadmin/res/pdf/publikationen/mag-arno-cichocki/10541_Data_Protection_Austria.pdf) [October, 20th, 2011]
- Kuczerawy, A. (2010). "Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS\*." M. Bezzi et al. (Eds.): *Privacy and Identity, IFIP AICT 320*: 75–85.
- Latour, B. (1992). "Where are the Missing Masses? The Sociology of a Few Mundane Artifacts", in: *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Bijker, W.E. and Law, J. (Eds), MIT Press, USA, pp. 225-258.
- Margulis, S. T. (2011). *Three Theories of Privacy: An Overview*. *Privacy Online, Perspectives on Privacy and Self-Disclosure in the Social Web*. S. Trepte and L. Reinecke. Berlin, Heidelberg, Springer-Verlag: 9-17.
- Pedersen, D. M. (1999). "Models for types of privacy by privacy functions." *Journal of Environmental Psychology* 19(4): 397-405.
- Pershing, B. (2011). "A Weiner ethics case would cover uncharted ground". *The Washington Post*, available at: [http://www.washingtonpost.com/politics/a-weiner-ethics-trial-would-cover-uncharted-ground/2011/06/09/AGbG6dNH\\_story.html](http://www.washingtonpost.com/politics/a-weiner-ethics-trial-would-cover-uncharted-ground/2011/06/09/AGbG6dNH_story.html). Published: June 9.
- Petri, A. (2011). "The hypocritical Weiner furor and the Laws of the Internet". *The Washington Post Blogs*, available at: [http://www.washingtonpost.com/blogs/compost/post/the-hypocritical-weiner-furor-and-the-laws-of-the-internet/2011/03/03/AG4WUbXH\\_blog.html](http://www.washingtonpost.com/blogs/compost/post/the-hypocritical-weiner-furor-and-the-laws-of-the-internet/2011/03/03/AG4WUbXH_blog.html). Published: June 16.
- Poullet, Y. (2010). *About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? Data Protection in a Profiled World*. S. Gutwirth, Y. Poullet, P. De Hert, Springer Netherlands: 3-30.
- Sargent, G. (2011a). "Weiner resigns, and Twitter claims its first major political casualty". *The Washington Post Blogs*, available at: [http://www.washingtonpost.com/blogs/plum-line/post/weiner-resigns-and-twitter-claims-its-first-major-political-casualty/2011/03/03/AGxzRNxH\\_blog.html](http://www.washingtonpost.com/blogs/plum-line/post/weiner-resigns-and-twitter-claims-its-first-major-political-casualty/2011/03/03/AGxzRNxH_blog.html). Published: June 16.
- Sargent, G. (2011b). "Please, no more media 'Twittergasms'". *The Washington Post Blogs*, available at: [http://www.washingtonpost.com/blogs/plum-line/post/please-no-more-media-twittergasms/2011/03/03/AGOUx3cH\\_blog.html](http://www.washingtonpost.com/blogs/plum-line/post/please-no-more-media-twittergasms/2011/03/03/AGOUx3cH_blog.html). Published: June 20.
- Solove, D.J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, New Haven and London.
- Strauss, J., and Rogerson K. S. (2002). "Policies for online privacy in the United States and the European Union". *Telematics and Informatics* 19 (2002) 173–192.
- The Guardian* (2011). "Man on trial over Twitter 'affair' claims says case has 'big legal implications'". *The Guardian*, available at: <http://www.guardian.co.uk/technology/2011/jun/15/twitter-affair-claims-legal-implications>. Published: June 15.
- The Independent* (2011). "'Shame' of affair boss outed online". *The Independent*, available at: <http://www.independent.co.uk/news/uk/crime/shame-of-affair-boss-outed-online-2297652.html>. Published: June 15.
- van Dijk, T. A. (1983). "Discourse Analysis: Its Development and Application to the Structure of News". *Journal of Communication* Spring 1983 Volume 33:2 20–43.
- von Schomberg, R. (2007). *From the ethics of technology towards an ethics of knowledge policy/knowledge assessment - Working Document*. Publication series of the Governance and Ethics unit of DG Research. Brussels, European Commission.
- Walther, J. B. (2011). *Introduction to Privacy Online*. *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*. S. Trepte and L. Reinecke. Heidelberg, Springer: 3-8.
- Westin, A. (1967). *Privacy and Freedom*. New York, Atheneum.

Andrew A. Adams, Kiyoshi Murata, Yohko Orito and Pat Parslow:

## Emerging Social Norms in the UK and Japan on Privacy and Revelation in SNS

### Abstract:

Semi-structured interviews with university students in the UK and Japan, undertaken in 2009 and 2010, are analysed with respect to the revealed attitudes to privacy, self-revelation and revelation by/of others on SNS.

### Agenda

Introduction	20
Privacy and Revelation: Theory and Practice	21
Who Are You? And Who's Your Friend?	22
Friends Don't Embarrass Friends Online	23
Conclusions	24

### Authors:

Prof Andrew A. Adams

- Centre for Business Information Ethics, Meiji University, 1-1 Kanda Surugadai, Chiyoda-Ku, Tokyo-To 101-8301, Japan
- [aaa@meiji.ac.jp](mailto:aaa@meiji.ac.jp) [www.a-cubed.info](http://www.a-cubed.info)
- Relevant publications:
  - Adams, A. A., Murata, K. and Orito, Y.: The Development of Japanese Data Protection. Policy and Internet 2(2) art. 5, pp. 95-126, 2010. [www.psocommons.org/policyandinternet/vol2/iss2/art5](http://www.psocommons.org/policyandinternet/vol2/iss2/art5)
  - Adams, A. A., Murata, K. and Orito, Y.: The Japanese Sense of Information Privacy. AI & Society 24(4), pp. 327-341, 2009. [opendepot.org/209](http://opendepot.org/209)
  - Brown, I. and Adams, A. A.: The ethical challenges of ubiquitous healthcare. International Review of Information Ethics 8, pp. 53-60, 2007. [www.i-r-i-e.net/inhalt/008/008\\_9.pdf](http://www.i-r-i-e.net/inhalt/008/008_9.pdf)

Prof Kiyoshi Murata

- Centre for Business Information Ethics, Meiji University, 1-1 Kanda Surugadai, Chiyoda-Ku, Tokyo-To 101-8301, Japan
- [kmurata@kisc.meiji.ac.jp](mailto:kmurata@kisc.meiji.ac.jp) + 81 3 3296 2165 [www.kisc.meiji.ac.jp/~ethicj](http://www.kisc.meiji.ac.jp/~ethicj)
- Relevant publications:
  - Murata, K. and Orito, Y.: The Right to Forget/Be Forgotten. Proceedings of CEPE 2011, pp. 192-201, 2011.
  - Murata, K. and Orito, Y.: Japanese Risk Society: Trying to Create Complete Security and Safety Using Information and Communication Technology. Computers and Society 40(3), pp. 38-49, 2010.
  - Murata, K. and Orito, Y.: Rethinking the Concept of the Right to Information Privacy: A Japanese Perspective. Journal of Information, Communication and Ethics in Society 6(3), pp. 233-245, 2008.

Dr Yohko Orito

- Faculty of Law and Letters, Ehime University, 3 Bunkyo-cho, Matsuyama, Ehime 790-8577, Japan
- [orito@ll.ehime-u.ac.jp](mailto:orito@ll.ehime-u.ac.jp)
- Relevant publications:
  - Orito, Y.: The Counter-Control Revolution: "Silent Control" of Individuals through Dataveillance Systems, Journal of Information, Communication and Ethics in Society 9(1), pp. 5-19,2010. <http://dx.doi.org/10.1108/14779961111123197>

Mr Pat Parslow

- School of Systems Engineering, University of Reading, Whiteknights, Reading RG6 6AY, UK
- [p.parslow@reading.ac.uk](mailto:p.parslow@reading.ac.uk) [brains.parslow.net](http://brains.parslow.net)
- Relevant publications:
  - Williams, S. A. Fleming, S. Lundqvist, K. and Parslow, P.: Understanding your digital identity, Learning Exchange 1 (1), 2010. [learn-ingexchange.westminster.ac.uk/index.php/lej/article/viewFile/17/14](http://learn-ingexchange.westminster.ac.uk/index.php/lej/article/viewFile/17/14)

## Introduction

Various figures in the media and technology worlds have claimed that the younger generation have no sense of privacy, or at least that they have got over the fact that they have no privacy anyway and embraced transparent life.<sup>1</sup> Others such as Livingstone,<sup>2</sup> Marwick et al.,<sup>3</sup> Marwick and boyd<sup>4</sup> dispute this, and point to a clear understanding of the trades that are being made by teenagers between general visibility (their 15 minutes of fame), connectability (amongst existing connections and occasionally to potential new electronic connections) and privacy. Much of the existing work in this area focusses on a single culture, most particularly the US, and focusses on groups where Facebook is almost the only social networking site in use. In order to provide elements of a broader picture, semi-structured interviews were carried out with students at the University of Reading in the UK and at Meiji and Ehime Universities in Japan, using suitably translated versions of the same questionnaire.<sup>5</sup> The result of the interviews were reviewed for similarities and differences in attitudes between the two sets of students.

The goal of the work was to understand the basic approach to using social networking sites amongst university-age students in the UK and Japan, with particular reference to:

- the identity of the target group for inclusion in their list of contacts;
- their attitudes towards identity, pseudonymity or anonymity on these sites;
- their attitudes towards self-revelation within a contact group and more broadly;
- their attitudes towards revelation by others of their information;
- their attitudes towards revelation by them of information about others;
- their attitudes towards revelation by third parties of information about that third party;
- their attitudes towards revelation by third parties of information about other third parties.

Even among this small group of interviewees (five from the UK and four from Japan) both some common factors and variations emerged. The different default settings of the systems used by subjects, including Mixi (the dominant Japanese SNS according to Alexa Internet Inc: [www.alexa.com/siteinfo/mixi.jp](http://www.alexa.com/siteinfo/mixi.jp)) and Bebo (a significant but not dominant player in the European market) as well as Facebook, were discussed with the interviewees. One subject who agreed to be interviewed in the UK was not registered with any social network site and in addition to the relevant remaining questions on attitudes to others' revelations online, their reasons for deliberately and positively refraining from joining such sites were investigated.

---

1 Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media and Society*, 10(3):393–411.  
eprints.lse.ac.uk/27072/1/Taking\_risky\_opportunities\_in\_youthful\_content\_creation\_(LSERO).pdf.(Newspaper articles referred to in Endnotes 5-7.)

2 *ibid.* (Main text.)

3 Marwick, A. E., Murgia Diaz, D., and Palfrey, J. (2010). Youth, Privacy and Reputation (Literature Review). Technical Report 5, Berkman Centre. [ssrn.com/abstract=1588163](http://ssrn.com/abstract=1588163).

4 Marwick, M. and boyd, d. (2011). Tweeting teens can handle public life. *The Guardian*.  
[www.guardian.co.uk/commentisfree/2011/feb/15/tweeting-teens-twitter-public-privacy](http://www.guardian.co.uk/commentisfree/2011/feb/15/tweeting-teens-twitter-public-privacy).

5 based on a questionnaire created by Trottier of Queens University in Canada for his PhD work

## Privacy and Revelation: Theory and Practice

The advent of the Internet and particularly so-called Web 2.0 has provided everyone who is online with a vast opportunity for destroying their own and other's reputations on a much broader scale than in the past. Even refraining oneself from being online may not be a hindrance to fame or infamy on the social web, as explained by Solove<sup>6</sup> in the cases of the Korean girl labelled *gae-ttong-nyue* (dog shit girl) after allowing her dog to defecate in a train carriage and refusing to clear it up, and of the Star Wars kid, whose childish imitation of a lightsaber routine went viral on the video sharing sites, much to his chagrin.

As Marx<sup>7</sup> explains there are complex interplays of law and social norms at work in disclosing information whereby some information is required to be kept private, other information is required to be public, and others are required to be submitted to certain bodies in certain circumstances. Into this mix SNS have allowed not only self-revelation but revelation by/of others. In some cases, this revelation may be mistaken, such as when a photo tag is misapplied and identifies the wrong user. Where the photo is of something embarrassing this can be significantly harmful as shown by the reported practices of a substantial number of US firms who use online searches, including of SNS, to filter out "unsuitable" candidates.<sup>8</sup> The practice is so prevalent and potentially harmful that the German federal government has introduced regulations banning employers from considering information posted on purely social network sites when considering job applications (professional-oriented sites such as LinkedIn sensibly remain fair sources).<sup>9</sup>

Surveillance by SNS and blog is not limited to potential employers, but includes school or university authorities, current employers, insurance companies and the police:

- Three baseball players at Kosei Gakuin High School in Aomori Prefecture in Japan, whose baseball team took the second place in the 2011 Koshien High School Baseball Tournament<sup>10</sup>, each separately posted on their mobile blogs about their underage drinking at Japanese-style pubs. One of them also posted salacious details of his dates with a female student who acted as an assistant manager to the team. Someone reported these posts to official at both the high school and the prefecture's high school federation. As a consequence, the players were suspended from school. All the local events to celebrate the vice championship were cancelled due to the scandals.<sup>10 11</sup>
- A University of Minnesota student in the US was suspended after making comments on her Facebook account which were considered threatening by staff at her school, when brought to their attention.<sup>12</sup> The case here is rather reminiscent of the more disturbing example of Jake Baker from 1994 who posted a violent rape-and-murder fantasy story to a usenet newsgroup using the name of

6 Solove, D. J. (2007). *The Future of Reputation*. Yale University Press, New Haven, CT.

7 Marx, G. T. (2011). *Turtles, Firewalls, Scarlet Letters and Vacuum Cleaners: Rules about Personal Information*. In Aspray, W. and Doty, P. (editors), *Privacy in America: Interdisciplinary Perspectives*. Scarecrow Press, Lanham, MD. Early draft available at [web.mit.edu/gtmarx/www/turtlesandfirewalls.html](http://web.mit.edu/gtmarx/www/turtlesandfirewalls.html).

8 Microsoft (2010). *Data Privacy: Perceptions Study*. [download.microsoft.com/download/E/0/9/E094917B-049C-4B00-AE65-E97F55585C08/DPD\\_%20Online%20Reputation%20Research.pptx](http://download.microsoft.com/download/E/0/9/E094917B-049C-4B00-AE65-E97F55585C08/DPD_%20Online%20Reputation%20Research.pptx). A survey whose results were widely reported in the press but for which no better presentation of the results is extant.

9 Out-Law.com (2010). *German law bans facebook research for hiring decisions*. [www.out-law.com/page-11336](http://www.out-law.com/page-11336).

10 Wall Street Journal (2011). *Booze of Summer: Scandal Hits Koshien Baseball*. [blogs.wsj.com/japanrealtime/2011/08/25/booze-of-summer-scandal-hits-koshien-baseball/](http://blogs.wsj.com/japanrealtime/2011/08/25/booze-of-summer-scandal-hits-koshien-baseball/). JapanRealTime Blog.

11 Matsuzawa, Y. (2011). *Kosei Gakuin: the fact that three baseball players drank was detected online and they were suspended from school*. Mainichi Shimbun. 22nd August. [mainichi.jp/select/today/archive/news/2011/08/22/20110823k0000m040055000c.html](http://mainichi.jp/select/today/archive/news/2011/08/22/20110823k0000m040055000c.html). In Japanese.

12 Wobbema, T. (2009). *U student suspended after threatening remarks on Facebook*. The Minnesota Daily. [www.mndaily.com/2009/12/16/u-student-suspended-after-threatening-remarks-facebook](http://www.mndaily.com/2009/12/16/u-student-suspended-after-threatening-remarks-facebook)

a classmate at the University of Michigan<sup>13</sup> showing that such issues pre-date social networking sites (Baker was prosecuted but cleared of any illegal act).

- CBC reported the case of a Canadian woman whose employer's insurance company stopped her disability benefits for depression after she posted holiday pictures of herself smiling on a beach.<sup>14</sup>
- There were claims that riots in the UK in the summer of 2011, initially sparked by a fatal shooting by police in London which spread to other areas of the capital and into other cities, were being coordinated using electronic messaging services, including SNS messages. Devon and Cornwall police, amongst other forces, have been investigating reports of messages inciting disorder and there have been a number of arrests made and verbal warnings against repeating such behaviour given.<sup>15</sup>

## Who Are You? And Who's Your Friend?

One of the differences between various SNS is the word used to describe the connections a user has. In addition the directionality of such connections is interesting to note. LiveJournal, one of the earliest SNS still running, uses the word *friend* to indicate connections, but unlike sites such as LinkedIn, Facebook and Mixi, LiveJournal allows a user to add any other user to their list of friends without an acceptance of that status by the new *friend*. The academic-oriented site academia.edu has *followers* instead of *friends* and is similarly unidirectional, whereas the general professional networking site LinkedIn uses the very neutral term *connections* and has only bidirectional connections. The Japanese site Mixi uses *mai-mikushi* as the name of the link to the page listing one's connections. In a standard Japanese linguistic approach, this is shortened to *mai-miku* by most users and used as the descriptive noun for the connections in their social circle by many Japanese, including the interviewees. This did not appear to indicate any difference in attitude to their UK counterparts towards those online connections.

The UK interviewees generally used their real name on their SNS accounts, although not necessarily as their main visible screen name. This was reversed for the Japanese users with none of them having their real name explicitly included on their accounts, and often other strongly deanonymising information such as university department and/or degree course also withheld. Indeed they regarded those who did so as acting dangerously. This may be part of the reason that Facebook, with its strong policy on visible real names, has had little success in Japan. The Japanese interviewees all felt that since their primary use of the system was to maintain contact with people with whom they already had strong real world relationships, that online pseudonymity provided some extra security with no downside. They used other contact forms to pass SNS identity information to potential connections.

The UK interview subjects all indicated that they distinguished in their minds between real friends and Facebook "Friends", although few of the UK or Japanese interviewees had many connections on their primary SNS whom they did not know in real life. Indeed, only one of the Japanese subjects stated that they were open to connections from people they had not met in real life and that was limited to seeking out people with a common interest in a specific type of music — the now-classic use of the interconnections possible online to find common travellers [which the subject referred to as 仲間 (*nakama* — friend, partner, companion)] with a shared minority interest.

13 Electronic Frontier Foundation (2003). EFF "Legal Cases - Jake Baker, the U. of Michigan, & the FBI" Archive. [w2.eff.org/legal/cases/Baker\\_UMich\\_case](http://w2.eff.org/legal/cases/Baker_UMich_case).

14 CBC (2009). Depressed woman loses benefits over Facebook photos. [www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html](http://www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html).

15 Halliday, J. (2011). Tory MP Louise Mensch backs social network blackouts during civil unrest. The Guardian, 12th August. [www.guardian.co.uk/uk/2011/aug/12/louise-mensch-social-network-blackouts](http://www.guardian.co.uk/uk/2011/aug/12/louise-mensch-social-network-blackouts).

*...members are my university friends or friends from high school only. I don't like to have a communication with unspecified people through the websites.*

*Japanese Student, Male, 21 (translated)*

*I want to track down my old school friends, from elementary school to high school, on the Mixi web site; I would like to find friends who have real relationships with me through using Mixi. I don't hold my breath to make a new personal relationship with those who share the same interest with me online.*

*Japanese Student, Male, 21 (translated)*

*I've got about 600 friends. They have to be someone I definitely know. I put up all the information about hobbies, music, what I'm doing in my degree, all my religious and political views, things like that.*

*UK Student, Female, Age not recorded*

*I wanted to find fellows [仲間 (nakama)] with whom I could enjoy talking over and exchanging information of heavy metal music and musicians. I didn't have any nakama to do such things before using Mixi; joining open communities of heavy metal music in Mixi provided me with the opportunities to get acquainted with those who had the similar taste of music and now enjoy good relationships with them not only in the cyberspace but in the real space.*

*Japanese Student, Male, 19 (translated)*

Both UK and Japanese interviewees felt pressure from their peer groups to be involved in the SNS, with both reporting that they used the sites to keep in touch with their pre-university social circle, as well as those they had met since starting university. Even those attending university in Tokyo who are from Tokyo, use the site to keep in touch with friends attending a different Tokyo-based institution, with whom they felt they might otherwise have lost touch.

## Friends Don't Embarrass Friends Online

Another common thread between the UK and Japanese interviewees was their attitudes to revelation of others' information on their SNS sites. Almost all of both groups felt that unrestricted revelation was not a proper way to act on such sites. It was felt by members of both groups that information with potentially negative consequences should either not be posted, or at least that the subject should be consulted before posting. Both Japanese and UK subjects were aware of the potential negative consequences of posting embarrassing photos online, even if the intent and initial audience is a tight circle of known individuals.

*I have been concerned that one of my university friends uploaded two photographs which show a girl (ed: not interviewee's partner) and me together. After that, I worried that her boyfriend may complain to me. In another case, while I don't disclose my department/course or name of my university, some user disclosed it without my agreement.*

*Japanese Student, Male, 21 (translated)*

Some of the Japanese interviewees regarded the subject of revelations as equally to blame as the person making the revelation, for any negative consequences arising. The UK interviewees regarded it as solely the responsibility of the revealer. This may well reflect broader Japanese attitudes to group assumption of blame and consequences, drilled into youngsters from their first days at kindergarten or school according to Hendry.<sup>16</sup> It also mirrors other elements of Japanese culture with regard to negative consequences of social interactions, for example the greater reluctance of Japanese junior high school students to report instances of bullying as shown by Kanetsuna et al.<sup>17</sup> Informal class discussions with a group of Japanese university students and two of the authors about online bullying also revealed the attitude that the victim is somehow jointly to blame with the victimiser.

*When Mixi stalking happens, this is a victims fault. Mixi users have to carefully determine what kinds of information can and cannot be published on Mixi. Information provision which evokes Mixi stalking can perfectly be deterred if users have enough knowledge about the Internet.*

*Japanese Student, Male, 19 (translated).*

## Conclusions

The sample size for these interviews is very small. Hence conclusions are only drawn about these particular interviewees. There are two intended tracks for following up on this work: developing and deploying a questionnaire about SNS usage targetted at confirming whether the interviewees were representative of their peer groups in their attitudes; comparison of the results of these interviews with the larger interview sample of Canadian residents (mostly Canadian citizens) undertaken by Trottier, on whose questions this work was based. Funding is being sought to perform these and related pieces of research.

Fear of isolation/peer pressure is the key to why the interviewees use SNS. Even where there is disquiet about the dangers of SNS usage, or the policies of a particular platform operator, almost all interviewees felt that they had to be online or be excluded from their social group. The one interviewee who had chosen not to be on SNS felt that they had to work harder to engage with the social group because of their lack of inclusion in the network, with other electronic communications tools such as email and SMS being their preferred modes of online contact.

The Japanese interviewees reported somewhat greater usage than the UK interviewees. This may be simply a reflection of the small sample size, but might also be reflective of the greater availability of featurephone-based SNS access in Japan at the time of the interviews (2009–10). The spread of smartphones in the UK may have reduced this difference by the time of writing (late 2011).

Most of the interviewees had some awareness of privacy boundaries, but it varies greatly and may be subject to large shifts from small causes. This gives hope for digital identity awareness training of the type promoted by the Williams et al.<sup>18</sup> in the This is Me project ([thisisme.rdg.ac.uk](http://thisisme.rdg.ac.uk)). All of the interviewees recognised there were dangers to their privacy in using SNS, with this awareness sometimes triggered by a specific instance of their own use and sometimes by things that happened to others (reported by word of mouth in the case of their friends or through the media for other people).

---

16 Hendry, J. (2003). Understanding Japanese Society. Routledge, Oxford.

17 Kanetsuna, T., Smith, P. K., and Morita, Y. (2006). Coping With Bullying at School: Children's Recommended Strategies and Attitudes to School-Based Interventions in England and Japan. *Aggressive Behavior*, 32(6):570–580.

18 Williams, S., Fleming, S., Lundqvist, K., and Parslow, P. (2011). Understanding Your Digital Identity. *Learning Exchange*, 1(1). [learningexchange.westminster.ac.uk/index.php/lej/article/viewFile/17/14](http://learningexchange.westminster.ac.uk/index.php/lej/article/viewFile/17/14).

*Recently, I have been very careful in writing a Facebook journal so that the writing will never cause any problem assuming that anyone can read the journal. I recognised this necessary (sic) through reading news reports about Facebook stalking by organisations.*

*UK Student, Male, 21.*

*I changed my profile picture, and I had about 15 people making a mess of my Facebook page all over the place, putting things on the wall. I looked at my wall and looked at my profile on there, and basically felt that it wasn't representative of what I wanted people to see, it was a representation of what other people wanted. And thinking about placements and trying to get a job this summer, I was thinking I wouldn't want people who might be working with me, or might be looking to employ me in the future, to see all this stuff. I wasn't really bothered about it until then. And then a switch flipped, and I thought I don't want people seeing this, or pictures tagged to me, and this, that and the other.*

*:*

*I spent an hour buried in the Facebook privacy things and the application settings, basically turning everything off....no one [else] can now do anything on Facebook which changes my profile.*

*UK student, Male, 20.*

*I used to put quite personal stuff on there, but recently I've not been doing that so much. I just began to realise how stuff I put online is going to stay there, and people can access it quite easily. You've really got to think about it whereas before I used to put quite random stuff on there. I began to use Live Journal rather than Facebook for publishing stuff. I put a few status updates, that kind of thing, but not very much.*

*UK Student, Male, Age not recorded.*

*My parents are online, so I monitor what I put up on Facebook. I mean you can't refuse a request from your parents to be your 'friends', but I remove things like pictures of me smoking, or lewd comments on my wall that I might not want them to see!*

*UK Student, Female, Age not recorded*

*I experienced the event where my father asked me to let him be my Facebook friend. If he hadn't sent me the message, I would not have realised he had access to my Facebook pages. Japanese Student, Male, 21 (translated)*

*I never upload my photograph, real name and something by which someone can identify me. It is OK for me to reveal the name of my university on Mixi.*

*Japanese Student, Male, 19 (translated)*

## References

- Aspray, W. and Doty, P., editors (2011). *Privacy in America: Interdisciplinary Perspectives*. Scarecrow Press, Lanham, MD.
- CBC (2009). Depressed woman loses benefits over Facebook photos. [www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html](http://www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html).
- Electronic Frontier Foundation (2003). EFF "Legal Cases - Jake Baker, the U. of Michigan, & the FBI" Archive. [w2.eff.org/legal/cases/Baker\\_UMich\\_case/](http://w2.eff.org/legal/cases/Baker_UMich_case/). Last Update.
- Halliday, J. (2011). Tory MP Louise Mensch backs social network blackouts during civil unrest. *The Guardian*. 12th August. [www.guardian.co.uk/uk/2011/aug/12/louise-mensch-social-network-blackouts](http://www.guardian.co.uk/uk/2011/aug/12/louise-mensch-social-network-blackouts).
- Hendry, J. (2003). *Understanding Japanese Society*. Routledge, Oxford.
- Kanetsuna, T., Smith, P. K., and Morita, Y. (2006). Coping With Bullying at School: Childrens Recommended Strategies and Attitudes to School-Based Interventions in England and Japan. *Aggressive Behavior*, 32(6):570–580.
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media and Society*, 10(3):393–411. [eprints.lse.ac.uk/27072/1/Taking\\_risky\\_opportunities\\_in\\_youthful\\_content\\_creation\\_\(LSERO\).pdf](http://eprints.lse.ac.uk/27072/1/Taking_risky_opportunities_in_youthful_content_creation_(LSERO).pdf).
- Marwick, A. E., Murgia Diaz, D., and Palfrey, J. (2010). Youth, Privacy and Reputation (Literature Review). Technical Report 5, Berkman Centre. [ssrn.com/abstract=1588163](http://ssrn.com/abstract=1588163).
- Marwick, M. and boyd, d. (2011). Tweeting teens can handle public life. *The Guardian*. [www.guardian.co.uk/commentisfree/2011/feb/15/tweeting-teens-twitter-public-privacy](http://www.guardian.co.uk/commentisfree/2011/feb/15/tweeting-teens-twitter-public-privacy).
- Marx, G. T. (2011). Turtles, Firewalls, Scarlet Letters and Vacuum Cleaners: Rules about Personal Information. In Aspray and Doty (2011). Early draft available at [web.mit.edu/gtmarx/www/turtlesandfirewalls.html](http://web.mit.edu/gtmarx/www/turtlesandfirewalls.html).
- Matsuzawa, Y. (2011). Kosei Gakuin: the fact that three baseball players drank was detected online and they were suspended from school. *Mainichi Shimbun*. 22nd August. [mainichi.jp/select/today/archive/news/2011/08/22/20110823k0000m040055000c.html](http://mainichi.jp/select/today/archive/news/2011/08/22/20110823k0000m040055000c.html). In Japanese.
- Microsoft (2010). Data Privacy: Perceptions Study. [download.microsoft.com/download/E/0/9/E094917B-049C-4B00-AE65-E97F55585C08/DPD\\_%20Online%20Reputation%20Research.pptx](http://download.microsoft.com/download/E/0/9/E094917B-049C-4B00-AE65-E97F55585C08/DPD_%20Online%20Reputation%20Research.pptx). A survey whose results were widely reported in the press but for which no better presentation of the results is extant.
- Out-Law.com (2010). German law bans facebook research for hiring decisions. [www.out-law.com/page-11336](http://www.out-law.com/page-11336).
- Solove, D. J. (2007). *The Future of Reputation*. Yale University Press, New Haven, CT.
- Wall Street Journal (2011). Booze of Summer: Scandal Hits Koshien Baseball. [blogs.wsj.com/japanrealtime/2011/08/25/booze-of-summer-scandal-hits-koshien-baseball/](http://blogs.wsj.com/japanrealtime/2011/08/25/booze-of-summer-scandal-hits-koshien-baseball/). Japan-RealTime Blog.
- Williams, S., Fleming, S., Lundqvist, K., and Parslow, P. (2011). Understanding Your Digital Identity. *Learning Exchange*, 1(1). [learningexchange.westminster.ac.uk/index.php/lej/article/viewFile/17/14](http://learningexchange.westminster.ac.uk/index.php/lej/article/viewFile/17/14).
- Wobbema, T. (2009). U student suspended after threatening remarks on Facebook. *The Minnesota Daily*. [www.mndaily.com/2009/12/16/u-student-suspended-after-threatening-remarks-facebook](http://www.mndaily.com/2009/12/16/u-student-suspended-after-threatening-remarks-facebook).

Daniel Skog:

## Ethical Aspects of Managing a Social Network Site: a Disclosive Analysis

### Abstract:

Managing an online social network site is not an easy task. First, the software environment must be designed with tools that promote social interaction. Second, the social environment must be nurtured and protected with thoughtful and balanced rules that allow for freedom within limits. This paper reports from an ethnographic study of a Swedish social network site, and focuses on how the site managers try to deal with undesirable use patterns and behaviors among members, at the same time struggling with the unexpected social outcome of a software redesign. Adopting a disclosive ethics approach, the paper highlights some of the ethical challenges embedded in the process of managing the site, and discusses their implications.

### Agenda:

Introduction	28
The case of LunarStorm	28
The Lajv feature	28
Redesigning Lajv - implementing an age division	29
Reasons why the technological intervention backfired	30
Disclosing ethical issues in a complex software environment	30
Concluding remarks	31

### Author:

Ass. Prof. Dr. Daniel Skog

- Department of Informatics, Umeå University, 901 87 Umeå, Sweden
- ☎ + 46 90 786 9575, ✉ [dskog@informatik.umu.se](mailto:dskog@informatik.umu.se), 🌐 [www.informatik.umu.se](http://www.informatik.umu.se)
- Relevant publications:
  - Software Environments for Community: A Study of Online Community, Technology and Culture. (Thesis.) Umeå: Department of Informatics, Umeå University, Sweden, 2010, 197 p. (In Swedish.)
  - Social interaction in virtual communities: the significance of technology. *International Journal of Web Based Communities*, 1(4), p. 464-474, 2005.

## Introduction

An online social network site (SNS) is defined as a web-based service that allows individuals to construct a public profile, and list connections with other users at the site (Boyd and Ellison, 2007). These sites flourish online, with Facebook as the most noticeable example hosting hundreds of millions of users. The enormous growth and popularity of these spaces is also illustrated in a recent report from the Pew Research Center (Madden and Zickuhr, 2011), stating that 50 % of all American adults use SNS.

Even though ethically charged questions regarding identity, friending, privacy and surveillance has surfaced in SNS research (see, for instance, Boyd, 2008; Frick and Oberprantacher, 2011; Hull, Lipford and Latulipe, 2011; Vallor 2011), Light and McGrath (2010) argues that ethical issues associated with these environments are somewhat neglected. Since SNS have become so popular, playing a vital role in many people's everyday life, their ethical implications deserve more attention. In this endeavor, Light and McGrath (2010) adopts a disclosive ethics approach (Brey, 2000a), with the aim of revealing ethically relevant features in the context of using an SNS.

Using a similar approach, this paper highlights ethically relevant mechanisms and situations within a Swedish SNS. When reviewing the events that followed a minor software redesign, using an ethical lens, critical issues emerge concerning SNS development and management.

## The case of LunarStorm

The empirical foundation of this paper originates from a recently finished long-term ethnographic study of LunarStorm (LS), a popular online social network site among young people in Sweden.

LS was one of the earliest SNS online, predating sites like Friendster, MySpace and Facebook (Boyd and Ellison, 2007). Many of the features now common at most SNS (i.e. user profiles, friends lists, guest books, etc.), thus appeared much earlier on LS. The site was launched at the millennium shift, January 1, 2000. However, it was actually a remake of StajlPlejs, a community site that had existed since the mid-nineties. For almost a decade, LS was the premier SNS in Scandinavia with more than 1 million active members. Even though a majority of the members were teenagers, the average age among members during this time period was about 18 years old. Losing ground to other SNS and facing a diminishing user base, LS recently remodeled again in August 2010, when it was transformed and reborn as L8.

This present study was initiated 2003. During five years empirical material was collected by the use of participant observations and semi-structured interviews with members and site administrators. In addition, a large number of text-based conversations with LS members concerning their social interactions, use of technology and experiences as SNS members, were carried out during fieldwork, generating a substantial amount of data. In total, the empirical material comprises field notes, screen images, transcripts from 37 interviews, about 1200 guest book entries, 750 e-mails, and 700 pages of forum discussions.

The ethnographic analysis can be described as iterative-inductive (O'Reilly, 2005), blending fieldwork, analysis, and theory elaboration in a joint process. For the purpose of this paper, the empirical material has been analyzed focusing on site members' interactions and experiences connected to a specific feature within the software environment. In the following sections quotes are sometimes used to illustrate a common attitude or viewpoint, and these quotes originate from different communication contexts at LS. The reader should observe that quotes from informants were documented in Swedish and have been translated by the author.

## The Lajv feature

LS can be described as a multifaceted environment, which offered its members a variety of communication modes. As a LS member you had access to a personal profile page including a guest book, a blog, a contact

list, a photo album and a file repository. In addition, the site comprised various discussion forums and several other communication tools.

One frequently used communication feature in LS was Lajv (corresponds to the English word Live), which allowed members to broadcast a text message to those online at the same time. The text messages that were put out appeared in a specific message box where new messages continuously showed and were visible for around 30 seconds. A typical Lajv message was sent out to draw attention to the member's home page and often included a request for guest book contributions or comments on the photo album. Lajv messages were also frequently oriented towards dating:

*Inf 1: You are cute if you could comment on my photo album (kiss)*

*Inf 2: Is there a sweet single girl who wants to add a lonely single guy on msn...*

*Inf 3: anyone up for CYBERSEX!?*

The Lajv feature was launched in 2002. It became very popular, and if you wanted to get attention there was no other feature as effective. People sent messages to get attention, to provoke, to ask questions, and to get in contact with other members.

### Redesigning Lajv - implementing an age division

It might not come as a surprise that a large social network such as LS also caught the interest of Internet predators. By using Lajv messages, unwelcome and typically adult male members could make contact with their targets, followed by communication via guest books and e-mails. When the LS administrators became aware of this they decided to intervene. With the primary aim of creating a safer environment, they modified the Lajv feature by implementing an age division (Eriksson, 2006). Lajv messages broadcasted by members older than 20 were not to be shown to members below 18, and vice versa. This modification would perhaps not stop Internet predators from making new contacts, but at least their primary tool for contacting minors was to some extent rendered harmless.

The Lajv feature continued to be a heavily used communication tool, and initially the age division seemed to work as intended by LS administrators. However, not all members were content with how the Lajv feature had been redesigned. Among the members of LS were many parents whose primary reason for being there was to monitor the environment where their children spent several hours per day. By applying an age partition on Lajv (and on some other features) the parents no longer could share their kids' online environment. Initially the age division was unknown to most members, but when discovering it, caring parents reacted with frustration:

*Inf 4: I think we are many who didn't know [about the age division]. For my part I feel totally deceived. So here you have one who will be sitting next to the children for some time now when they are logged in.*

*Inf 5: I didn't know that [the age division exists]. So there are two sides of Lunar in other words. How then should a parent be able to keep track? By checking on the kids' pages or what?*

*Inf 6: But this was the primary reason why I made a home page at Lunar, I wanted to know what the kids were doing. ... Is it that impossible in our society for all ages to spend time with each other in a shared forum without being separated by age, with or against your will?*

The maneuvering of Lajv probably made it somewhat more difficult for Internet predators trying to make new contacts, in that way contributing to the safekeeping of minors. However, considering how some parents tried to safeguard their kids by sharing their online environment, the age partition perhaps had the opposite effect on child safety. Parents being hindered from monitoring communication patterns involving their kids preferred having no age segments, instead being able to watch the full flow of messages. In their view the age partition of Lajv failed its purpose.

The frustration and anger among parents amplified by the news that another Swedish youth community online offered help with creating fake social security numbers (SSN). When you registered as a new member at LS you had to state your SSN, and since Swedish SSN are assigned according to a person's date of birth, the age of the person became known. But it was discovered that the fake SSN generator available online could be used to register a bogus membership at LS pretending to be a teenager. In that way people who did not want to adhere to the age segments could circumvent the partitions, being able to interact with teenagers without restrictions.

Since not that many sincere parents were attracted to the idea of creating fake personalities of their own, the age division maneuvered by LS administrators fell short in two ways. Not only did it prohibit caring parents from monitoring dubious Lajv messages, it also in some way offered protection to unscrupulous individuals who now could socialize using a fake identity as a disguise.

### **Reasons why the technological intervention backfired**

Reviewing the happenings connected to the modification of the Lajv feature, it can be argued that there were at least two major reasons to why the technological intervention to some extent backfired. First, the LS administrators failed to recognize how the Lajv feature was perceived and used for different purposes by different members. When it was created the intention was to offer a tool for members trying to catch the attention of the community. It was never meant to be a means for parents monitoring their kids, and this usage became evident only when it could no longer continue. Lajv was certainly not intended as a tool for Internet predators either. This apparent usage of Lajv messages was detected and the discovery was in part the reason for implementing age segments. However, dealing with this misuse both unveiled and hampered the unexpected usage of caring parents, without being powerful enough to put an end to the actual misuse being targeted.

Second, it was not anticipated by administrators that members would want to outmaneuver the imposed age segments. The modification of Lajv placed an obstacle in the way of Internet predators who were eager to find a way to outsmart it. Knowing first hand the flaws of the customary SSN control, LS administrators perhaps should have seen the loophole offered to these offenders, realizing that it could and would be exploited. But even if they did see it they perhaps still did not want to strengthen the control of SSN since doing so most certainly also would have had other undesired consequences for the community.

The story of the redesign of Lajv illustrates the intertwined relationship between technological factors and social interactions in online social networks. In addition, it also highlights some ethical issues in managing online social networks.

### **Disclosing ethical issues in a complex software environment**

As described by Brey (2000a), disclosive computer ethics is concerned with the moral deciphering of computer technology. The underlying assumption is that many computer-related practices are morally nontransparent:

*"Many design and uses of computer systems, I want to claim, have important moral properties, that remain hidden because the technology and its relation to the context of use are too complex or are insufficiently well-known." (Brey, 2000b: 126)*

This argument resonates well with the case study presented in this paper. At first, the redesign of Lajv (implementing an age division) might seem rational and straightforward. The result of the redesign might even be considered successful. But reviewing the social context of this specific feature, reveals a complex relationship between the software environment and the interactions among different user groups. With this complex relationship on display, ethical issues concerning SNS management also emerge.

If we once again review the events accompanying the Lajv feature, using an ethical lens, we should start from the very beginning, since not even the initial decision to launch Lajv can be seen as ethically neutral. Unlike many other SNS, the social interactions taking place at LS were not limited by members' friends lists. Anyone could see your profile page and write in your guest book. This fact created an environment that was dynamic and lively. The possibility of meeting new people seemed to be one of the main ideas with LS, having old friends blend with new acquaintances and strangers. The development of Lajv accentuated this idea, offering enhanced possibilities of contacting, and being contacted by, new people.

This strategy of creating an environment without clear boundaries, where everyone could make contact with you via Lajv or by using tools at your profile page, certainly communicates ethically flavored values and ideals. While many members seemed to cherish those ideals, enjoying their stay in a lively environment without thresholds and with almost unlimited possibilities of interacting with new interesting people, some of them also experienced the downside, having a hard time to be left alone, struggling with bullies or stalkers. As described by Skog (2005), some LS members consequently chose not to reveal much of themselves on their profile pages. They simply were not willing to take the risk of being teased, or having strangers contacting them offline.

Even before the advent of Lajv there had been a scribble board at LS where members could write messages for everyone to read. But with Lajv, the developers wanted to create a more effective scribble board, something that was in real-time and provided members with an even more powerful tool when trying to get attention (Eriksson, 2006). Using Lajv, someone could communicate a message with thousands of unknown members, currently being online. It is not hard to imagine that this possibility sometimes was exploited for the wrong reasons, and the site managers must have seen this coming and decided that it was an acceptable drawback to offering such a powerful communication tool. However, at some point in time, LS developers apparently decided that they had to modify Lajv in order to prohibit misuse of a certain kind. Targeting this specific misuse, by using age divisions, should also be considered as an ethically charged choice, communicating what the developers regarded to be good and bad behavior.

The modification of Lajv was perhaps not secret, but still not communicated to the site members. As if the LS developers preferred altering the software environment unnoticed, without having to discuss their incentives with the users. Perhaps not surprisingly, the developers also did not act on the complaints from caring parents who felt that the redesign of Lajv had failed its purpose. This reminds us that SNS are typically proprietary spaces. The site owners/developers not only build the site, and thereby design the social environment (Pargman, 2000). They also make decisions about membership guidelines and rules of conduct (Humphreys, 2008). However, when a site is being populated, the members develop social and behavioral norms of their own, within the broader set of regulations decided by the site administrators. Furthermore, the users start to explore and exploit the software in unexpected ways for different purposes. On the one hand, this is a natural process, vital for the growth and sustainability of the social network. On the other hand, site administrators might feel a need to control the process, or at least desire to influence it.

As Lessig (2006) points out, the code that builds the online social environments reflects choices and values of the coders. Likewise, many algorithms, e.g. the age division of Lajv, comprise value judgments (Kraemer, van Overveld and Peterson, 2011). One could argue that the developers should be morally responsible for the outcome of their designs. However, as the empirical case shows, it is almost impossible to predict the outcome of a software design. Even if LS developers would have made a thorough ethical analysis of Lajv, imagining different use patterns and possible scenarios, they could probably not have foreseen neither the range of initial use patterns emerging or the effects caused by the age division. Furthermore, recognizing that the meaning of technology ultimately is socially constructed by the users, the responsibility for its ethical implications must be shared by developers and users alike.

## Concluding remarks

This paper contributes to the endeavor of disclosing ethical aspects of SNS. By examining a single software feature in a Swedish SNS, this study highlights some ethically charged decisions embedded in the process of managing and developing a social online environment. However, it is important to emphasize that those

decisions cannot be removed. Developers cannot avoid them or be passive pretending they are not there. A SNS is like a garden that has to be nurtured, and managing it demands ongoing work trying to match technology with emerging social practices (Wenger, White and Smith, 2009). Still, developers can make an effort to show their value judgments and to make their ethical standpoints more transparent. Even more, users could be given more freedom of making their own choices, deciding for themselves how different software features should be set up.

Today, LS has been replaced by other more popular SNS. But ethical challenges similar to those highlighted in this paper still remains. There is clearly a need for continuous examination of online social spaces, aiming for a higher awareness of ethical issues among both users and developers.

## References

- Boyd, Danah: *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*. *Convergence: The International Journal of Research into New Media Technologies*, 14(1): 13-20, 2008.
- Boyd, Danah & Ellison, Nicole B.: *Social Network Sites: Definition, History, and Scholarship*. *Journal of Computer-Mediated Communication*, 13(1): 210-230, 2007.
- Brey, Philip: *Disclosive computer ethics*. *Computers and Society*, 30(4): 10-16, 2000a.
- Brey, Philip: *Method in computer ethics: Towards a multi-level interdisciplinary approach*. *Ethics and Information Technology*, 2(2): 125-129, 2000b.
- Eriksson, Rickard: *Interview with Rickard Eriksson, LunarStorm Brand Manager*. Conducted May 8, 2006.
- Frick, Marie-Luisa and Oberprantacher, Andreas: *Shared is not yet Sharing, Or: What Makes Social Networking Services Public?* *International Review of Information Ethics*, 15(9): 17-23, 2011.
- Hull, Gordon & Lipford, Heather & Latulipe, Celine: *Contextual gaps: privacy issues on Facebook*. *Ethics and Information Technology*, 13(4): 289-302, 2011.
- Humphreys, Sal: *Ruling the virtual world*. *European Journal of Cultural Studies* 11(2): 149-171, 2008.
- Kraemer, Felicitas & van Overveld, Kees & Peterson, Martin: *Is there an ethics of algorithms?* *Ethics and Information Technology*, 13(3): 251-260, 2011.
- Lessig, Lawrence: *Code: version 2.0*. New York: Basic Books, 2006.
- Light, Ben & McGrath, Kathy: *Ethics and social networking sites: a disclosive analysis of Facebook*. *Information Technology and People*, 23(4): 290-311, 2010.
- Madden, Mary & Zickuhr, Kathryn: *65% of online adults use social networking sites*. Washington: Pew Internet and American Life Project, 2011. Available 2011-10-27: <http://www.pewinternet.org/~media/Files/Reports/>
- O'Reilly, Karen, *Ethnographic Methods*. New York: Routledge, 2005.
- Pargman, Daniel: *Code begets community: on social and technical aspects of managing a virtual community*. Ph.D. thesis. Linköping: Department of Communication Studies, The Tema Institute, Linköping University, 2000.
- Skog, Daniel: *Social interaction in virtual communities: the significance of technology*. *Intl. Journal of Web Based Communities*, 1(4): 464-474, 2005.
- Vallor, Shannon: *Flourishing on Facebook: Virtue Friendship and New Social Media*. *Ethics and Information Technology*, 2011. Published online Jan 2011, print edition forthcoming. DOI: 10.1007/s10676-010-9262-2.
- Wenger, Etienne & White, Nancy & Smith, John D.: *Digital Habitats – Stewarding Technology for Communities*. Portland, OR: CPsquare, 2009.

Juan José Prieto Gutiérrez:

## Herramientas para el análisis y monitoreo en Redes Sociales

### Abstract:

Networks or partnerships are used by humans since the beginning of humanity and its analysis raises concerns from many different sectors of society.

In the era of the network of networks, Internet, networks are generated by virtual connections of the agents. Social Network Analysis (SNA) studies the relationship relation to each other, the social structure. It is an area that is emerging as essential in decision-making processes for its ability to analyze and intervene in the behaviour of structures.

We analyze three NSA tools that monitor conversations on the Organization "IFLA" keyword in order to measure the feeling of them, managing social efforts to relate the flows between the entities, groups, etc.

### Agenda:

Introducción.	34
Redes sociales	34
Medición en los medios sociales	35
Herramientas para el análisis de inteligencia en Redes Sociales.	36
Consideraciones finales	39

### Author:

Dr. Juan José Prieto Gutiérrez

- Law Faculty Library. Complutense University of Madrid. Ciudad Universitaria, 28040, Madrid, Spain.
- ☎ +34 91 394 56 16, ✉ [jjpg@buc.ucm.es](mailto:jjpg@buc.ucm.es)
- Relevant publications:
  - Instituciones culturales en un clic. Telos: Cuadernos de Comunicación e Innovación. Nº 89. Octubre 2011.
  - The community manager in libraries. World Library and Information Congress: 77th IFLA General Conference and Assembly 15 August 2011, San Juan, Puerto Rico.
  - Protección de material clasificado y sensible en las organizaciones. *Redseguridad*. Nº 52 - Junio 2011, Pág. 80-81
  - De occidente a oriente: un viaje a través de las colecciones. *Educación y Biblioteca: Revista Mensual de Documentación y Recursos Didácticos*, 2011 ENE-FEB; 23 (181)

## Introducción.

La creación de asociaciones, sociedades y comunidades es algo constitutivo del ser humano y compartir su conocimiento es una de los principales de los mismos<sup>1</sup>.

Internet, es la columna vertebral de la sociedad de la información, ofreciendo innegables posibilidades de intercambio de conocimiento. De hecho, las redes sociales se perfilan como el modelo de mayor crecimiento y más aun con la penetración de los smartphones<sup>2</sup>.

El conocimiento del entorno es algo esencial para percatarse de donde te encuentras, con quien te relacionas, las tendencias, las predicciones, etc.

El análisis de las redes sociales permite estudiar como los comportamientos y estructuras de ciertos colectivos (personas, grupos u organizaciones) afecta a sus conductas y actitudes. Por ello, este análisis en redes sociales (ARS) es una actividad que está brotando como imprescindible en los procesos de toma de decisiones de instituciones, empresas, colectivos, etc.

La aparición de la Web 2.0 ha abierto la posibilidad a redes sociales interactivas donde las personas o instituciones aportan y esperan recibir información útil de características o similitudes afines.

## Redes sociales

*"Las comunidades online se representan mediante las conexiones personales que los usuarios disponen los unos de los otros"*<sup>3</sup>.

La estructura de las redes sociales ha evolucionado a lo largo de la historia adquiriendo nuevos paradigmas y tipologías.

Una red social se define como una organización o estructura generada a través de las relaciones de diferentes actores (personas, instituciones, organizaciones, sociedades, etc.), debiendo poseer o estar vinculadas a ciertas particularidades o rasgos comunes con el fin de poder interactuar entre sí.

En la actualidad destacan las redes creadas al calor de las nuevas tecnologías, de Internet, de interacción social y que son en las que se centra la investigación. La primera red social, *classmates.com*, surgió en 1995 y fue ideada por Randy Conrads. A partir de ese momento emergen numerosas redes, principalmente para relacionar o conectar a amigos, compañeros o colegas.

Con la generación de la Web 2.0, aproximadamente en el año 2004, se produce una explosión en el campo de las redes sociales donde las temáticas y contenidos abarcan todas las áreas y donde se generan nuevas formas de constituir y conservar relaciones sociales.

Es importante destacar la gran cantidad de medios sociales ofrecidos en la red. Por ello, las clasificaciones se hacen necesarias con el fin de adecuarse para el desarrollo de análisis exhaustivos. Cabe destacar las redes sociales horizontales donde tiene cabida cualquier temática bien de ocio, laboral, deportes, etc. (Facebook, Twitter, Friendster, MySpace, YouTube, etc.) y las verticales que se especializan en temas

---

1 Barabasi, A. L. *Linked: The New Science of Networks*. Cambridge, MA: Perseus.

2 García Hervas, Jesús Galván. *Redes sociales en el móvil*. Telos: Cuadernos de comunicación e innovación. Año, n. 83. 8-12.

3 Ros-Martín, Marcos. *Evolución de los servicios de redes sociales en Internet*. *El Profesional de la Información*. V. 18, n. 5 / Septiembre - Octubre, 552 – 558

concretos (Check My Ride, Xing, BabyCenter, etc.), estas últimas, crecen a mayores porcentajes que los primeros<sup>4</sup>.

## Medición en los medios sociales

Con el desarrollo anterior se dice que el análisis de redes sociales es la cartografía y la medición de las relaciones y los flujos entre las personas, grupos, organizaciones o equipos<sup>5</sup> siendo necesarias en los procesos de toma de decisiones<sup>6</sup>.

Una vez evaluada o transformada la información y procesado el conocimiento extraído a partir del uso de determinadas herramientas, el objetivo será obtener el mayor nivel de inteligencia personal, en los centros de investigación o en empresas tecnológicas, con el fin de asesorar y dirigir políticas hacia las marcas privadas, personales y las Administraciones Públicas.

Las herramientas tecnológicas han fortalecido este desarrollo mediante la fusión de las ideas y opiniones ofrecidas en las redes sociales, aprovechando su gran potencial para obtener datos y realizar tareas de vigilancia. No cabe duda que para conocer lo que está pasando en el tejido social se necesita contar con instrumentos avanzados de tracking para realizar diagnósticos y monitorización de acciones en las redes sociales. La aproximación desde una metodología observacional es fundamental, puesto que se recoge lo que ocurre en el medio social interactivo.

Existen una gran variedad de proveedores de investigación que ofrecen herramientas que reflejan el entorno social y en común tienen el análisis de los contenidos generados por los usuarios o consumidores CGM (Consumer-Generated Media).

Pero, en la red se dispone de un gran número de herramientas gratuitas que realizan el seguimiento de los contenidos sociales en todos los campos de la red.

Por limitaciones de espacio, se analizarán varias herramientas de monitorización, con el fin de ajustar las cualidades de cada una de ellas a las demandas del usuario. Unas herramientas pueden monitorizar conversaciones a lo largo y ancho de la red sobre un tema específico, marca o persona y otras, centrarse en el análisis de determinadas aplicaciones de una forma simultánea. Ante esta situación se analizarán tres herramientas, la primera de ellas, **Socialmention** busca en variados espacios. La segunda opción reúne dos herramientas de Google, **Trends** e **Insights** y por último, tras la cada vez mayor demanda de Twitter, **Follow the Hashtag**.

Para facilitar la labor de análisis, se ha decidido realizar a modo de ejemplo una búsqueda concreta como es la "palabra clave" "IFLA" (International Federation of Library Associations and Institutions) debido a la popularidad de la misma en el área y a la amplitud del marco temporal a analizar.

Las herramientas elegidas poseen características afines: monitorean los medios sociales, son gratuitas, fáciles de usar, cuentan con una interfaz amigable y generan gráficos o sociogramas para representar actores y líneas para constituir lazos o relaciones. En el mercado existen otras muchas herramientas que se renuevan constantemente y que los técnicos de marketing analistas deben mantener al día, como Radian 6, Spiral 16, Alterian SM2, Hootsuitepro, etc.

---

4 Fumero, Antonio; García, Miguel. "Redes sociales: contextualización de un fenómeno "dos-punto-cero. Telos: Cuadernos de comunicación e innovación, n. 76, 56-68

5 Valdis E. Krebs. Mapping Networks of Terrorist Cells". CONNECTIONS 24, (3): 43-52

6 Wasserman, S. Faust, K. Social network analysis. Methods and Applications, Cambridge University Press, Cambridge.

## Herramientas para el análisis de inteligencia en Redes Sociales.

**Socialmention:** Es un motor de búsqueda totalmente gratuito, con contenido generado por el usuario en Blogs, Microblogs, foros, imágenes, videos, noticias, comentarios, eventos y con la posibilidad de realizar la búsqueda en todos a la vez.

Con fecha 1 de septiembre se ha testado el posicionamiento en la red de la palabra clave "IFLA".

Esta herramienta además cuantificar el número de entradas y el acceso a los comentarios realiza un análisis semántico de los contenidos, de modo que permite realizar una valoración más descriptiva del sentido de las menciones, destacando:

- **Strength:** 2%. Es la probabilidad con la que se está debatiendo en los medios de comunicación social sobre la IFLA. Para calcular el porcentaje se emplea un cálculo simple: frase mencionada en las últimas 24 horas, dividida por el total de posibles menciones.
- **Sentiment:** 13:1. El sentimiento es la proporción de menciones positivas sobre las que son negativas. Por lo que de cada diez menciones una es negativa.
- **Passion:** 37%. La pasión es una medida de la probabilidad de que los individuos que hablan de su marca, lo harán varias veces. Las menciones positivas sobre la IFLA, han sido realizadas por diferentes personas. El porcentaje se calcula mediante las palabras clave más utilizadas y el número de veces mencionadas, en definitiva es el número de menciones por sentimiento.
- **Reach:** 26%. Es una medida del radio de influencia. Es el número de autores únicos que referencian a la IFLA dividido por el número total de menciones.

Gráficamente obtenemos:

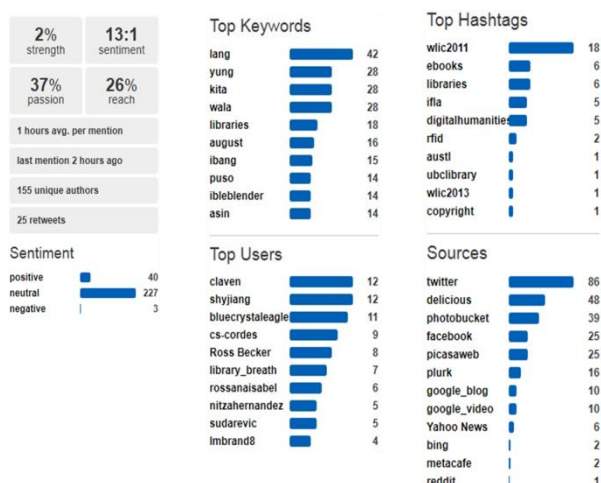


Figura 1: Gráficos de las búsquedas del termino "IFLA" el día 1/09/11. Fuente: Socialmention.

Se observa que el motor de búsqueda de Socialmention es muy completo, el cual trabaja con más de una centena de redes sociales, entre las cuales se encuentran Twitter, Facebook, LinkedIn, YouTube, StumbleUpon, Digg o Google, permitiendo la exportación a hojas de cálculo de la información obtenida. Como dato positivo cabe destacar la eliminación de búsqueda en los scraper sites.

Asimismo el resultado de búsqueda muestra las *Top Keywords* relacionadas con la cadena buscada, los *Top users* que las generaron, el *Top Hashtag* (en este caso *wlic2011*, que obviamente coincide con la reunión

anual de la IFLA, celebrada en el año 2011 en Puerto Rico) y las fuentes relacionadas, que encabezan por Twitter.

Por último, es posible suscribirse vía RSS a una búsqueda concreta. Interesante para no perder de vista qué se dice en Internet sobre un determinado concepto.

Destacar, que en pocos minutos es posible realizar un seguimiento y monitoreo y medir fácilmente, lo que la gente está señalando de uno mismo, de otro, de una empresa, un producto o cualquier otro tema a través de los medios Web de comunicación social.

A continuación se realiza una exploración de dos herramientas de Google, debido a que es el buscador más utilizado en Internet, alrededor del 60%, sus resultados suelen mostrar autenticidad, Google Insights y Google Trends. Con fecha 1 de septiembre se ha testado el posicionamiento en la red de la palabra clave "IFLA".

**Google Trends:** esta aplicación proporciona información sobre la relevancia que tienen los términos de búsqueda en la red, sin indicar concretamente el contenido social, permitiendo visualizar gráficamente la evolución de búsquedas en un determinado periodo de tiempo (desde el año 2004 hasta la actualidad) pudiendo analizar comportamientos sociales o posibles estacionalidades entre otra información.

En la parte superior del gráfico que se muestra aparecen las variables de búsqueda a lo largo del tiempo (eje abscisas) y en el gráfico inferior las noticias publicadas sobre la IFLA. En el eje vertical representa la frecuencia con la que se ha buscado el término globalmente.



Figura 2: Gráfico de la evolución del termino "IFLA" desde el año 2004. Fuente: Google

Acotando la muestra a ciclos anuales es posible percibir el despunte de la estacionalidad de los periodos en que se celebran los congresos anuales, generalmente en agosto. Otra de las características de la herramienta es la posibilidad de comparar hasta cinco términos simultáneamente y acceder al acotamiento geográfico regional, de ciudades y del lenguaje empleado a través de gráficos.

**Google Insights:** esta segunda herramienta del gigante Google, posee una gran similitud en cuanto a la idea y a la funcionalidad que Google Trends pero, ofrece más datos sobre las palabras clave y precisa la geolocalización de los rastreos.

Cabe la posibilidad de cotejar patrones de volumen de búsqueda en determinadas áreas geográficas, intervalos de tiempo, categorías y propiedades analizando que zona está más interesada en el término examinado. Gráficamente se accede al resultado acotado temporalmente desde el año 2004 hasta la actualidad y representando en el eje vertical la frecuencia con la que se ha buscado el término. En la tabla ofrecida se muestra un mapamundi con el índice de volumen de búsquedas representado por diferentes colores.

Intereses de búsqueda en la Web sobre IFLA: <http://www.google.com/insights/search/?cat=0-11&q=IFLA&cmpt=q#cat=0-11&q=IFLA&cmpt=q>



Figura 3: Evolución de las búsquedas del termino "IFLA" desde el año 2004. Fuente: Google Insights.

Interés regional:

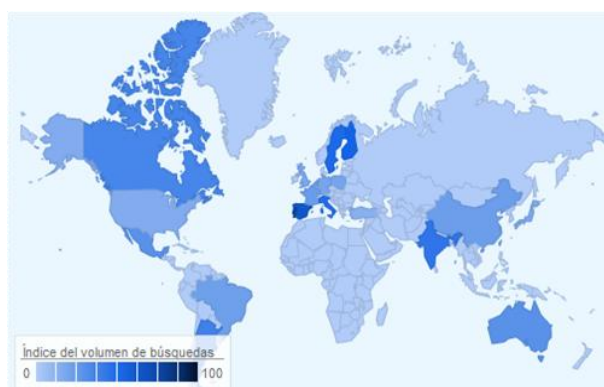


Figura 4: Distribución por países del volumen de las búsquedas del termino "IFLA". Fuente: Google Insights.

Los resultados demuestran que el número de búsquedas que se han realizado, sobre la IFLA, desde el 2004 es decreciente en relación con el número total de búsquedas que se han hecho en Google. Por otro lado es curioso destacar que el interés regional no coincide plenamente entre Google Trends y Google Insight.

Como observación comentar que las interfaces de Google son muy sencillas, manejables y fiables al pertenecer al laboratorio Google; aportando información muy provechosa, complementando a otras.

Existen infinidad de herramientas que trabajan sobre Twitter, bien para administrar la cuenta, para gestionar a tus seguidores, para saber de que se habla, el seguimiento de *hashtags*, para calcular la influencia, gestionar eventos, etc.: como por ejemplo klout, Twendz, Twitter Sentiment, TwitterCounter, etc. Habiéndose elegido **Follow the Hashtag** creada por DNOiSE la cual permite conocer, conversaciones en Twitter mediante gráficas útiles y coherentes.

Como en las anteriores herramientas se ha introducido el *hashtag* IFLA (#IFLA) durante la semana del 26 de agosto al 1 de septiembre de 2011 y como resultado se dispone de 169 tweets, con una frecuencia de 1.13 tweets por hora de 138 twitteros diferentes, siendo el más activo @ABESelSalvador con 6 tweets y, mediante el diagrama de puntos o de burbujas generado, es posible apreciar la jerarquía de importancia de los tweets.

La precisión y limitación de la herramienta depende actualmente de la API de búsqueda de Twitter. Una de las restricciones que impone es que "como mucho" se remontará a los últimos 1500 tweets o 30 días pasados por cada *keyword*.

En la zona de búsqueda y control permite introducir los parámetros deseados y contrastar hasta 4 *keywords* o *hashtag* al mismo tiempo, muy útil para realizar benchmarking. También es posible controlar la cantidad de búsquedas hechas y representadas, el lenguaje y la localización y mediante la función *random* es posible acceder a diferentes gráficos.

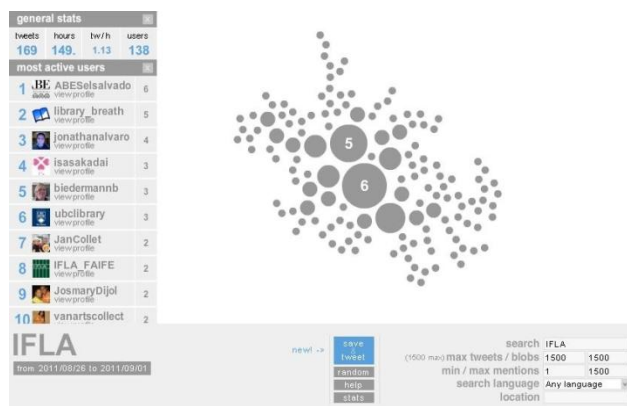


Figura 5: Diagrama de burbujas generado por la búsqueda del termino "IFLA" del 26/08/11 al 01/09/11. Fuente: Follow the Hashtag.

## Consideraciones finales

La propiedad más rica de una herramienta que analice y monitorice redes sociales es el hecho de que éstas son libres y virtuales, permitiendo que funcionen en los ámbitos más adversos con problemáticas de un sector geográfico o ideológico, conjugando el sistema de comunicación con la motivación social.

Los usuarios son dueños de los contenidos de las redes, por lo que el ARS se da cuenta y se apodera de ellos. Las redes sociales son más que un punto de encuentro, siendo necesario el empleo de diferentes aplicaciones virtuales capaces de coordinar y manifestar el comportamiento de las personas y las marcas transformándose los resultados en un componente inteligente.

En el estudio se examinan cuatro herramientas especializadas en el registro de la actividad en medios sociales, las cuales tienen un alto potencial para el ejercicio del seguimiento en el ámbito de las relaciones públicas y de la investigación tanto básica como aplicada. Hay un beneficio añadido de las herramientas que incluyen un analizador semántico que permite examinar los contenidos para su clasificación, creando indicadores de la actividad. Estos indicadores resultan especialmente adecuados para llevar a cabo comparativas temporales o de competencia.

La posibilidad de graficar las estructuras sociales y medir sus propiedades a partir de sofisticados programas de software, de muchas de estas herramientas, permiten de una manera comprensible y sucinta acceder a los resultados de la comunicación, colaboración, transacción, valoración, o cualquier otro tipo de relación que se desarrolle a través de medios presenciales o virtuales.

Se ha observado una gran actividad y participación en las redes destacando algunos líderes de opinión y es ahí donde el ARS selecciona y filtra la información con el fin de distinguir el conocimiento.

## References

- BARABASI, A. L. (2002) *"Linked: The New Science of Networks. Cambridge, MA: Perseus.*
- ESCORSA, P.; MASPON, R. (2001) *"De la vigilancia tecnológica a la inteligencia competitiva"* Madrid: Prentice Hall.
- FREIRE, Juan. (2008) *"Redes sociales: ¿modelos organizativos o servicios digitales?"*. *El profesional de la información*, noviembre-diciembre, v.17, n.6, pp. 585-588
- FUMERO, Antonio; GARCIA, Miguel. (2008) *"Redes sociales: contextualización de un fenómeno "dos-punto-cero". Telos: Cuadernos de comunicación e innovación*, n. 76, 56-68
- GARCIA HERVAS, Jesús Galván. (2010) *"Redes sociales en el móvil". Telos: Cuadernos de comunicación e innovación. Año, n. 83. 8-12.*
- LÉVY, Pierre. (2004) *"Inteligencia colectiva: por una antropología del ciberespacio"*, Washington DC. *La Découverte (Essais).*
- MIKA, P. (2005). *"Flink: Semantic web technology for the extraction and analysis of social networks"*, *Journal of Web Semantics*, 3(2).
- ROS-MARTÍN, Marcos. (2009) *"Evolución de los servicios de redes sociales en Internet". El Profesional de la Información. V. 18, n. 5 / Septiembre - Octubre, 552 – 558*
- VALDIS E. Krebs. (2002) *"Mapping Networks of Terrorist Cells". CONNECTIONS 24, (3): 43-52,*  
*<http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf>*
- WASSERMAN, S. FAUST, K. (1994) *"Social network analysis. Methods and Applications"*, Cambridge University Press, Cambridge.

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:

Introduction	42
Historical perspective	42
Privacy spotlight for social networks	43
Normative analysis	44
A Prescription for privacy protection	45
Conclusions	46

### 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](http://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 click-stream 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](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.

Sami Coll, Olivier Glassey and Claire Balleys:

## **Building social networks ethics beyond “privacy”: a sociological perspective**

### **Abstract:**

This article aims to widen the question of online social networks sites (SNS) ethics going beyond the questions of privacy and self-management of data, yet dominant in the public debates. The main theoretical framework developed in this paper, based both on recent contributions and classical sociology, is that SNS have to deal with the social dynamics of distinction and social classes like in any other spaces. From this perspective, focusing only on online privacy is too subjective and individualistic to provide a satisfying answer. Thus, we suggest that transparency should be considered as a social and collective fact rather than an individual characteristic. Boundaries between online and offline world are becoming increasingly porous and we argue, although acknowledging certain particular characteristics of SNS, that SNS ethics should be less about the specificities of online behaviors than on their articulation with the social world.

### **Agenda**

What is privacy?	48
Privacy in social network studies	48
Transparency and social networks	49
Is transparency a new social norm?	49
Transparency as a social fact	50
Conclusion	50

### **Authors:**

Dr. Sami Coll:

- Surveillance Studies Centre, Queen’s University, Kingston, Canada
- ✉ [sami@samicoll.com](mailto:sami@samicoll.com), 🌐 [www.samicoll.com](http://www.samicoll.com)

Dr. Olivier Glassey:

- Observatory Science, Policy and Society, University of Lausanne, Switzerland
- ✉ [olivier.glassey@unil.ch](mailto:olivier.glassey@unil.ch),  
🌐 <https://applicationspub.unil.ch/interpub/noauth/php/Un/UnPers.php?PerNum=881059>

Claire Balleys:

- Department of social sciences, University of Fribourg, Switzerland
- ✉ [claire.balleys@unifr.ch](mailto:claire.balleys@unifr.ch),  
🌐 <http://lettres.unifr.ch/fr/sciences-sociales/sciences-des-societes-des-cultures-et-des-religions/collaborateurs-esp/balleys.html>

Social network sites (SNS) and the way they affect society have rapidly become a main subject of discussion for social scientists and, more generally, for public actors. They are seen as playing an increasing role in the construction of individual and collective identities, in the creation of social links and in the way individuals involve themselves in the social and political life. In this context, most attention has been focused on issues such as trust, reputation and privacy. The latter is probably the biggest common and consensual concern.

In response to these legitimate concerns and beside the implementation of privacy and data protection laws, many advocates claimed that the users of these tools should be supervised and trained, in order to be able to face potential dangers and to keep control on their data. Usually, the problem is reduced to the idea of an inability of the users to understand that they put their privacy and reputation at stake, or in other terms, that they are not aware enough of the consequences of disclosing personal data. How to build trust and how to protect reputation and privacy has then become dominant in the public and political discourses, as the main key concepts for building ethics.

The aim of this paper is to establish the basis of a sociological analysis of online behaviours, with the purpose to diversify the dominant ethical discourses, expanding them beyond the question of the protection of privacy. Our approach is built upon the result of much recent research on SNS stating that social relations happening within social networks are not ontologically different from the ones which have existed before these platforms but that they rather increase the speed of exchanges, relationships, visibility and transparency. We suggest that SNS emphasize social effects which classical sociology knows already very well, rather than creating entirely new ones. Elaborating a framework of analysis built on classical sociology and applying it to the contemporary object of online social networks, we hope to enrich the debate differently and to offer fresh perspectives to think ethical issues in a new way.

## What is privacy?

The notion of "privacy" dominates the debate around ethics strongly (Bennett 2008), although it is a vague concept (Solove 2008; Stalder 2002). Still, it is dominant in policies and public discourses meant to protect people integrity. The main problem of the notion of privacy is its very individualistic nature. When speaking about privacy, it is usually about an individual facing government or private companies, and trying to find a balance between the advantage of enjoying services and partially renouncing to his/her privacy. But, privacy is also a very subjective notion. When asked, people give very distinct and personal definitions which most often do not fit the privacy advocates'. When observed as an everyday life experience, it becomes even more complicated to be conceptualized (Coll 2010).

Moreover, privacy should be seen not only as an individual good, but rather as a collective good (Westin 2003; Regan 2011). The main argument is that there is no equality in regard to privacy: "Privacy is frequently determined by the individual's power and social status. The rich can withdraw from society when they wish; the lower classes cannot. The affluent do not need to obtain subsidizing support from the government by revealing sensitive information to authorities, while those in economic or social need must disclose or go without" (Westin 2003, 432). Thus, although privacy is still somehow helpful from an individualistic perspective (Bennett 2011; Stalder 2011), we think that such approach cannot alone build a satisfying ethics for informational systems, including the case of social networks.

## Privacy in social network studies

Since the growing development of computers and Internet, early research focused on online disclosing of personal information (Turkle 1984). The specific ways users express themselves and adopt these new spaces of expression were also rapidly studied (Walther 1992; Turkle 1995). These studies, by exploring the anonymity of users and their multiple identities, dealt with the question of the building of transparencies/opacities (Wallace 1999).

However, these studies had to be updated since new platforms of exchange of information begun to appear (Allard 2007), even more with the raising of the Web 2.0 (Boyd and Ellison 2007). The fast adoption of such platforms which offer plenty of new forms of interactivity led to new studies focusing on the 'construction of the digital self' (Voirol 2010). The Web 2.0 and its technical devices oriented to information sharing can be seen as an opportunity to produce new and multiple forms of visibilities (Cardon 2008). At this stage, two levels have been addressed: first, the self-disclosure induced and controlled by technical devices (Lewis, Kaufman, and Christakis 2008; Fuchs 2011a); second, the strategies of presentation of the self produced by the social relationship between users (Fogel and Nehmad 2009). The first level is related to the ever-changing privacy settings of the platforms and raised for example research on how companies take advantage of disclosed data to do targeted advertisement (Wilkinson and Thelwall 2010). The second level has been empirically studied in the specific context of the culture of teenagers and their use of social networks (Boyd 2008).

Recent research also specialized themselves on particular types of tracks: profiles' pictures (Siibak 2009), body representations (Dobson 2008), claims for ethnical membership (Grasmuch, Martin, and Zhao 2009), display of gender (Geidner, Flook, and Bell 2007), or the appearance of persons which have been accepted as "friends" (Walther et al. 2008). These show how tracks circulate within social networks, as social but also symbolic markers. They shed light not only on why information is disclosed by users, but also why they are sometimes hidden on purpose.

The act of disclosing information is not only related to the presentation of the self, but also to the representation of the expectations of the audience (Evans, Gosling, and Carroll 2008; Ploderer et al. 2008). As a consequence, the analysis of a so-called "transparency" is not only about how information is disclosed, but also about how the same information is potentially used by others. Studies actually show that an important part of online activities consists in exploring tracks left by "friends" (Rau, Gao, and Ding 2008). They explore the criteria by which information is sorted in order to build an opinion and then a social judgment (Lampe, Ellison, and Steinfeld 2007). This consciousness of being watched and evaluated could lead to an internalization of social control (Back et al. 2010; Proulx and Kwok Choon 2011), inciting creation of strategies of reputation management (Madden and Smith 2010). This way, the so-called "transparency" can be seen as a co-product of both visible and invisible online interactions (Andrejevic 2005) or, in other terms, as an assemblage of contrasted attitudes toward the exposition of intimacy online, each one being balanced between modesty and exhibitionism (Aguiton et al. 2009).

In terms of ethics, the practices of self-disclosure on social network are most often reduced to the question of the protection of privacy. Yet, many sociological studies show that the boundaries between public and private are becoming ever more blurred (Boyd and Hargittai 2010; Cardon 2010; Christofides and Desmarais 2009).

## Transparency and social networks

### Is transparency a new social norm?

As seen above, in most studies on SNS, the notion of "transparency" has become increasingly recurrent. To the extent that it is sometimes considered by economical actors as a new social norm, replacing privacy<sup>1</sup>, or even a moral standard<sup>2</sup>. Indeed, when asked, many users claim that they have "nothing to hide" (Solove 2007).

This phenomenon is analyzed by some scholars as a "voluntary servitude" which informational capitalism is taking advantage of (Proulx and Kwok Choon 2011). Undoubtedly, one of the main salient characteristic of

<sup>1</sup> See Mark Zuckerberg's quotation: "Privacy no longer a social norm" (*The Guardian*, 11 January 2010).

<sup>2</sup> See Eric Smith's CNBC interview: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (3 December 2009).

SNS is the fact that users disclose data about themselves on a voluntary basis. It is also true that deep data-mining is made by companies to create efficient targeted marketing (Fuchs 2011b). However, as seductive the idea of a "voluntary servitude" can be, it is sociologically weak. The unclear notion of "transparency" needs to be theoretically deconstructed. We think that it suffers at the first place from the same problem as privacy does: to be seen from a very individualistic point of view.

### Transparency as a social fact

Some of classical sociology theories are able to shed light on the complex modalities of this so-called "voluntary transparency". From a macrosociological angle, SNS have to deal with the dynamics of social distinction and social classes like any other public space. From this perspective, classical sociology is important to reflect on visibility as an asset to build one's social identity and to claim one's membership to a certain social rank.

First, there is no absolute and generalized transparency. Not every individual makes oneself visible in the same way or at the same degree (Goffman 1959). Thus, the relationship between visibility and invisibility, disclosure or not disclosure, open transparency or limited transparency, is producing power (Simmel 1906). Visibility is as much an act of power when the purpose is to claim one's membership to a certain social rank, that a risk taken because it allows other to take control on one's self.

Second, this ambivalence led to a distinction: between transparency at the individual level, as perceived, experienced and practiced by users; and transparency as a social fact; that is as a key element – which was existing before the SNS – of social regulations in the large sense, involving judgements, positive or negative sanctions (Ogien 1990; Radcliffe-Brown 1965[1952]; Durkheim 1982[1895]), and social distinctions which maintain social hierarchy (Bourdieu 1987[1979]). This macrosociological approach allows going beyond the idea of a personal economy and control of personal data.

Our point is to emphasize the fact that the modalities of disclosure are more related to well-known sociological process rather than a personal economy of data. It is about fulfilling the social need to feel as a part of the society, to show one's social status, in other terms, to operate social distinction (Goblot 1967[1925]; Simmel 1957[1895]; Veblen 2008[1899]).

## Conclusion

By considering the transparency as a social fact rather than as an individual economy of data disclosure, too close to the individualistic concept of "privacy", we have pointed out the continuousness between the last research about social network and more classical sociological works.

The main conclusion we draw from these theoretical reviews of social visibilities, SNS related or not, is that the boundary between online and offline world is highly porous. Distinction and social judgments operate in these platforms as in the whole society and SNS cannot be considered any longer as separated microcosms where only geeks or teenagers were supposedly experiencing alternative social dynamics. SNS are a whole part of the information society, being combined with many other device or technology such as mobile phone, email, blogs, speeches, etc. and contributing to a continuum of intricate communication experiences which tend to form a seamless web (Hughes 1986) of social interactions.

This standpoint diminishes the requirement to develop an ontologically specific ethical framework for online activities and rather advocates for a broader perspective. In such perspective, online and offline activities should be symmetrically analysed, and the focus point of these investigations should be less about the specificities of online behaviours than on their articulations with the social world. We think that taking into account those convergences would set the foundation for a stronger hermeneutic approach in ethics. Such method would retain as its main object how social norms are translated from one world to the other and how those norms co-evolve notably through well known social processes.

The proposed reframing should however not be confused with a relativist stance negating the specificities of online social dynamics. Rather, in the context outlined in our paper, we think that these SNS related activities are less in the need of some epistemological differentiation than requiring an actual recognition as full-fledged social dynamics. By questioning some of the artificial theoretical fences built during the early steps of online social networks analysis, our ultimate goal is to let SNS studies contribute more directly and profoundly to the ethical debates around transparency for the whole society.

## References

- Aguiton, Christophe, Dominique Cardon, Aymeric Castelain, et al. 2009. *Does showing off help to make friends? Experimenting a sociological game on self-exhibition and social networks*, presented at the International Conference on Weblog and Social Media'09, San José, California, San Jose, CA.
- Allard, Laurence. 2007. « Emergence des cultures expressives, d'Internet au mobile ». *Mediamorphoses* 21: 19-25.
- Andrejevic, Mark. 2005. « The work of watching one another: Lateral surveillance, risk and governance ». *Surveillance & Society* 2 (4): 479-497.
- Back, Mitja D., Juliane M. Stopfer, Simine Vazire, et al. 2010. "Facebook profiles reflect actual personality, not self-idealization." *Psychological Science* 21: 372-374.
- Bennett, Colin J. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.
- . 2011. « In Defence of Privacy: The concept and the regime ». *Surveillance & Society* 8 (4): 485-496.
- Bourdieu, Pierre. 1987. *Distinction: A Social Critique of the Judgement of Taste*. Cambridge Mass.: Harvard University Press.
- Boyd, Danah. 2008. *Taken Out of Context: American Teen Sociality in Networked Publics*. Berkeley: University of California.
- Boyd, Danah, and Nicole Ellison. 2007. « Social network sites: Definition, history, and scholarship ». *Journal of Computer-Mediated Communication* 13 (1).
- Boyd, Danah, and Eszter Hargittai. 2010. « Facebook Privacy Settings: Who Cares? » *First Monday* 15 (8).
- Cardon, Dominique. 2008. « Le design de la visibilité. Un essai de cartographie du Web 2.0 ». *Réseaux* 152 (6): 93-137.
- . 2010. *Confiner le clair-obscur: réflexions sur la protection de la vie personnelle sur le web 2.0*. Dans *Web social. Mutation de la communication*, 315-328. Québec: Presses de l'Université du Québec.
- Christofides, Emily, and Serge Desmarais. 2009. « Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? » *CyberPsychology & Behavior* 12 (3): 341-345.
- Coll, Sami. 2010. *Consommation sous surveillance: L'exemple des cartes de fidélité*. PhD diss. Genève: Université de Genève, Faculté des sciences économiques et sociales.
- Dobson, Amy S. 2008. *The "grotesque body" in young women's self-presentation on MySpace*, presented at the Australian Sociological Association Conference: Re-Imagining Society, Melbourne.
- Durkheim, Emile. 1982. *Rules of Sociological Method*. New York: Free Press.
- Evans, David C., Samuel D. Gosling, and Anthony Caroll. 2008. *What Elements of an Online Social Networking Profile Predict Target-Rater Agreement in Personality Impressions?* Presented at the International Conference on Weblogs and Social Media.
- Fogel, Joshua, and Elham Nehmad. 2009. « Internet social network communities: Risk taking, trust, and privacy concerns ». *Computers in Human Behavior* 25 (1): 153-160.
- Fuchs, Christian. 2011a. « studiVZ: Social Networking Sites in the Surveillance Society ». *Ethics and Information Technology* 12 (2): 171-185.
- . 2011b. « Web 2.0, presumption, and surveillance ». *Surveillance & Society* 8 (3): 288-309.

- Geidner, Nicholas W., Christopher A. Flook, and Mark W. Bell. 2007. *Masculinity and online social networks: Male self-identification on Facebook.com*, presented at the Eastern Communication Association 98th: Annual Meeting, Providence, RI.
- Goblot, Edmond. 1967. *La barrière et le niveau*. Paris: PUF.
- Goffman, E. 1959. *The Presentation of Self in everyday Life*. New York: Anchor Books, Doubleday.
- Grasmuch, Sherri, Jason Martin, and Shanyang Zhao. 2009. « Ethno-Racial Identity Displays on Facebook ». *Journal of Computer-Mediated Communication* 15 (1).
- Hughes, Thomas P. 1986. « The Seamless Web: Technology, Science, Etcetera, Etcetera ». *Social Studies of Science* 16 (2): 281-292.
- Lampe, Cliff, Nicole Ellison, and Charles Steinfeld. 2007. *A Familiar Face(book): Profile Elements as Signals in an Online Social Network*. Dans *Proceedings of CHI 2007*.
- Lewis, Kevin, Jason Kaufman, and Nicholas Christakis. 2008. « The taste for privacy: An analysis of college student privacy settings in an online social network ». *Journal of Computer-Mediated Communication* 14 (1): 79-100.
- Madden, Mary, and Aaron Smith. 2010. *Reputation Management and Social Media How people monitor their identity and search for others online*. Pew Internet & American Life Project. <http://pewinternet.org/Reports/2010/Reputation-Management.aspx>.
- Ogien, Ruwen. 1990. « Sanctions diffuses: Sarcasmes, rires, mépris,... » *Revue Française de Sociologie* 31 (4): 591-607.
- Ploderer, Bernd, Steve Howard, Peter Thomas, and Wolfgang Reitberger. 2008. « Hey world, take a look at me! »: Appreciating the human body on social network sites. Dans *Proceedings of Persuasive 2008*, 245-248.
- Proulx, Serge, and Mary Jane Kwok Choon. 2011. « L'usage des réseaux socionumériques : Une intériorisation douce et progressive du contrôle social ». *Hermès* 59: 103-109.
- Radcliffe-Brown, A. R. 1965. *Social Sanctions*. Dans *Structure and Function in Primitive Society: Essays and Addresses*, 205-211. New York: Free Press.
- Rau, Pei-Luen P., Qin Gao, and Yinan Ding. 2008. « Relationship between the level of intimacy and lurking in online social network services ». *Computers in Human Behavior* 24 (6).
- Regan, Priscilla M. 2011. « Response to Bennett: Also in defence of privacy ». *Surveillance & Society* 8 (4): 497-499.
- Siibak, Andra. 2009. « Constructing the Self through the Photo Selection: The Importance of Photos on Social Networking Websites ». *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3 (1).
- Simmel, Georg. 1906. « The Sociology of Secrecy and of Secret Societies ». *American Journal of Sociology* 11 (4): 441-498.
- . 1957. « Fashion ». *American Journal of Sociology* 62 (6): 541-558.
- Solove, Daniel J. 2007. « "I've Got Nothing to Hide" and Other Misunderstandings of Privacy ». *San Diego Law Review* 44: 745-772.
- . 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.
- Stalder, Felix. 2002. « Opinion. Privacy is not the antidote to surveillance. » *Surveillance & Society* 1 (1): 120-124.
- . 2011. « Autonomy beyond privacy? A rejoinder to Bennett ». *Surveillance & Society* 8 (4): 508-512.
- Turkle, Sherry. 1984. *The Second Self: Computers and the Human Spirit*. New York: Simon & Schuster.
- . 1995. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon & Schuster.
- Veblen, Thorstein. 2008. *The Theory of the Leisure Class*. New York: Oxford University Press.
- Voirol, Olivier. 2010. « Digitales Selbst: Anerkennung und Entfremdung ». *WestEnd: Neue Zeitschrift für Sozialforschung* 7 (2): 106-120.
- Wallace, Patricia M. 1999. *The Psychology of the Internet*. Cambridge: Cambridge University Press.
- Walther, Joseph B. 1992. « Interpersonal effects in computer-mediated interaction: A relational perspective ». *Communication Research* 19: 52-90.

- Walther, Joseph B., Brandon Van Der Heide, Sang-Yeon Kim, et al. 2008. "The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep?" *Human Communication Research* 34: 28-49.
- Westin, Alan F. 2003. « Social and Political Dimensions of Privacy ». *Journal of Social Issues* 59 (2): 431-453.
- Wilkinson, David, and Mike Thelwall. 2010. « Social network site changes over time: The case of MySpace ». *Journal of the American Society for Information Science and Technology* 61 (11): 231-232.

Michelle Kilburn:

## **Why Individuals Choose to Post Incriminating Information on Social Networking Sites: Social Control and Social Disorganization Theories in Context**

### **Abstract:**

Facebook, Twitter, MySpace, and many more social networking sites are becoming mainstream in the lives of numerous individuals in the United States and around the globe. How these sites could potentially impact one's perception of community, as well as the ability to enhance (or impede) strong social bonding, is an area of concern for many sociologists and criminologists. Current literature is discussed and framed through the lenses of social disorganization and social control theories as they relate to an individual's propensity to commit crime/indiscretions and then post comments relating to those activities on social networking sites. The result is gained insight into the communal attributes of social networking and a contribution to the discussion of the relationship among the social components of the internet, criminal activity, and one's sense of community. Implications and areas of future research are also addressed.

### **Agenda**

Social Networking: Facebook at the Forefront	55
Social Control Theory	55
Social Disorganization Theory	56
Summation and Recommendations	57

### **Author:**

Asst.-Prof. Dr. Michelle Kilburn:

- Department of Criminal Justice and Sociology, Southeast Missouri State University, One University Plaza, Cape Girardeau, MO, USA
- ☎ 573-986-6414, ✉ [mkilburn@semo.edu](mailto:mkilburn@semo.edu)
- Relevant publications:
  - Kilburn, M. (2011). What are They Thinking? Why Individuals Might Choose to Post Incriminating Items on Social Networking Sites. Paper Presented at the Academy of Criminal Justice Sciences Annual Conference, Toronto, Ontario (Canada).
  - Kilburn, M. (2010). Social Networking: Exploring Social Disorganization and Social Control Theories. Paper Presented at the Midwestern Criminal Justice Association Conference, Chicago

## Social Networking: Facebook at the Forefront

A social networking site, in general terms, is defined as a website where users can create a profile and then connect to others in order to form a personal network (Pew Research, 2007). As of October 2011, Facebook was the most popular online social network in America and the world. Facebook started as a "virtual year-book" for college students but has quickly become a social phenomenon available to anyone who has access to the internet. In 2004, Facebook had 1 million users. Today, there are more than 800 million active users on Facebook. Approximately 1 person out of every 14 in the world is a Facebook user. On average, more than 250 million photos are uploaded per day and members interact with more than 900 million objects (groups, events and community pages). Users average 130 friends and spend more than 55 minutes per day on Facebook ("Facebook Statistics," 2011). The volume and type of information that is available to friends, family, and even the general public, can vary greatly.

In 2007, Peluchette & Karl conducted a study of college-age student profiles and found that 53% posted photos involving alcohol use; 50% used profanity; 42% made comments regarding alcohol; 25% posted photos containing semi-nude or sexually provocative photos, and 20% made comments regarding their sexual activities. In their study they suggested that students make a conscious effort to portray a particular image and those who post socially unacceptable information may do so to impress a particular audience – their peers.

Police officers routinely use social networking sites to investigate crimes and those who are suspect of committing those crimes (Masis, 2009). For decades, police have utilized confessions and admissions made by criminals to their friends, in an effort to secure enough evidence to prosecute perpetrators for their criminal actions. This same technique readily applies to social networking sites because criminals "cannot resist bragging about their handiwork" (Watkins, 2010).

"In the 20<sup>th</sup> century, police developed evidence from items such as fingerprints and DNA. In the 21<sup>st</sup> century, the computer and the Internet have become fertile fields for police to plow in the search for evidence" (Marsico, 2010, pg. 976). Police are using social networking sites to go "undercover" as friends on suspected offender profiles (Watkins, 2010).

Why would an individual choose to post information on social networking sites that could be used against them in a court of law? Why are young adults choosing to post activities that might be considered socially unacceptable behaviour? Utilizing the foundational frameworks of social control and social disorganization the author postulates the motivations behind, and purpose of, such activities in an online social medium such as Facebook. Analyzing such actions through these theoretical lenses provides insight into what makes a community and the relationship between communities and one's propensity to commit crimes.

## Social Control Theory

Social Control theorists seek to identify those features of personality and the environment that keep individuals from committing crimes. They believe it is the extent of a person's integration with positive social institutions and with significant others that influences resistance to criminal temptations. They tend to ask why people actually obey rules instead of breaking them (Schmallegger, 2009).

Facebook can be used by profile owners to engage with their friends and strengthen existing bonds and attachments (Young, 2011). It is certainly recognized that social networking sites can play a positive role:

*"By forming groups of people with similar interests (particularly if the interest or hobby is not mainstream), social networking sites can create a sense of unity and belonging in people who might have previously felt alienated in society because of an inability to relate to local people. Particularly in areas with smaller populations, the chance of discovering others with similar interests is infrequent; but, by*

*removing these location barriers through online communication, the chance of meeting people with the same interests is greatly increased" (Wheeldon, 2010, para 6).*

Travis Hirschi (2002), a major contributor to social control theory, contends that crime and delinquency occur when ties to the conventional and normative standards are weak or largely nonexistent. Many forms of traditional social controls include family, schools, communities, churches, youth athletic teams, civic groups, etc. and are often limited by geographical locations. Social networking sites make it very convenient for individuals to self-select their social groups or to weaken ties with groups who they may feel are too strict. Some of the social controls traditionally received from community, parents, civic, and religious groups may play a more muted role with individuals who rely heavily on social networking to form attachments. Technology affords the opportunity to evade social controls (Katz, 1998).

In a study conducted by Barker (2009), it was suggested that those who reported a disconnect from their peer group were more likely to turn to social networking sites. Older youth, who felt isolated and exhibited negative self-esteem, appear to turn to social networking for companionship. Barker suggested that individuals who feel a sense of negative social identity and self-esteem are more likely to distance themselves from their existing in-group and seek identification with other more favourably regarded groups. In summary, individuals looking for a social connection on Facebook, appear to be (1) looking for companionship, (2) desiring to identify with others (3) espousing a negative social identity and (4) male. Shy individuals are also more likely to have favourable attitudes toward Facebook (Orr, Sisic, Ross, Simmering, Arseneault, & Orr, 2009).

In the context of social control theory, individuals may choose to post socially unacceptable behaviour in an attempt to develop social bonds with a targeted group on Facebook. For example, negative messages about certain moral behaviours increased male profile owner's perceived physical attractiveness. "We might speculate that if greater attractiveness is perceived for males who misbehave, confirmatory and rewarding reactions by others might reinforce such behaviours or set observational learning dynamics into play encouraging others to behave in a similar manner" (Walther, Van Der Heide, Kim, Westerman, & Tong, 2008, pg. 45).

The internet provides a platform that makes it extremely easy to reach like-minded individuals located in various geographic locations, which removes one of the major barriers that limit group activity. Hate groups can exploit these and other online attributes to spread, legitimize and entrench hateful messages (Citron & Norton, 2011).

In a rather extreme example, social networking sites appear to also allow terrorists to disseminate propaganda to a young age group that could emphasize with their cause and could possibly agree to join. In the same way that marketing groups can view member's information to decide which products to push or target on a website, terrorist groups can view adolescent profiles in order to decide if they are going to target a particular individual and how they can effectively develop their message (Weimann, 2010).

Youths' patterns of peer relationship, friendship quality, and behaviour adjustments at ages 13-14 appear to be predicting similar qualities of interaction and problem behaviour on their social networking sites at ages 20-22 (Mikami, Szewdo, Allen, Evans, & Hare, 2010). Establishing strong and positive social controls both on and off-line at an early age is important and appears to have an impact on acceptable behaviour in adulthood.

### **Social Disorganization Theory**

Social disorganization is a condition that is said to exist when a group is faced with social change, uneven development of culture, maladaptiveness, disharmony, conflict, and lack of consensus. Social disorganization theories depict this social change, social conflict and the lack of social consensus as the root causes of crime and deviance. Shaw and McKay (1931) in their study of Chicago's Concentric Zones in the 1930's discovered that the first generation of immigrants tended to be law-abiding but it was the following generations in the transitional zones of the city/community that tended to become more criminal or reject social

norms. In general, social disorganization theory refers to the inability of a community's structure to realize common values of its residents and maintain effective social controls (Schmalleger, 2009).

A key theoretical proposition of social disorganization is that socially disorganized communities are less able to control the general behaviour of residents, thus affecting delinquent and criminal behaviour (Kornhauser, 1978; Shaw & McKay, 1931). Shaw and McKay (1942) theorized if a community is not self-policing some individuals will exercise unrestricted freedom to express their dispositions and desires.

Jones (1997) postulated that some online groups are virtual communities whereas others are "virtual settlements," which have fewer stable members, less frequent interaction, and fewer emotional connections. Others have suggested that greater online access and interactions can lead to networked individualism rather than community networks (Wellman, Quan-Haase, Boase, Chen & Hampton, 2003). This networked individualism allows people to "remain connected, but as individuals rather than being rooted in the home bases of a work unit and household. Individuals switch rapidly between their social networks" (Wellman, 2002, p. 15) opposed to remaining in a group or community. Although these sites may be often referred to as online communities, some research suggests that individual users support networked individualism rather than a sense of community (Reich, 2010).

In the context of social disorganization theory, individuals may choose to post socially unacceptable material on Facebook because the "community," to which they feel the strongest ties, is not really a community in the respect that social norms are reinforced and social consensus is strong and unified. Because online groups and communities are composed from members around the world, a lack of cultural development, maladaptiveness, and disharmony may be present. Also, the "norms" of online social networking media may not always mirror the social norms of a more geographically restrictive, face-to-face society.

For example, there is currently a wealth of media attention about how the current, younger generation is much less concerned about privacy than older generations (e.g., Dolliver, 2007; Robinson, 2006; St. John, 2006 as cited in Peluchette & Karl, 2010). Various details that older generations might find embarrassing are not uncommon on Facebook (Cole, 2006); and, when teens are seen getting a plethora of attention from posting outrageous and silly YouTube videos, it becomes apparent that keeping your life an open book can often be a ticket to fame (Funk, 2007). Stone & Brown (2006) purported that it appears that not all students want to hide information about their personal life. The Internet allows users to express themselves and to find similar-minded friends or communities. So while older generation Facebook users may see Facebook as a way to stay socially connected with old high school friends, younger generation Facebook users may feel it is simply a conduit to publish every aspect of their life to friends, family, networks and their online communities. Whether the information is incriminating or not, may not be a new generation of Facebook user's primary concern. Just as Shaw and McKay (1942) found that second generation immigrants lacked the social consensus and cultural transmission of their predecessors, the younger generation of Facebook users appear to be more accepting of behaviour that goes outside traditional social norms (Cole, 2006).

Another interesting feature of social networking sites is that overall impressions of a particular individual can be influenced by people other than the person who owns the profile. Postings by other people can not only reflect the character of the individuals who made the post, but it is also possible that observers' reactions of those posts may affect perceptions as well (Walther, et. al., 2008). For example, a user may choose not to disclose information regarding marijuana use at a party the night before; but, a "friend" might choose to post on the user's wall a comment that directly references the illegal activities.

## Summation and Recommendations

Relating to social control theories, Facebook users tend to develop bonds and connections with targeted groups. They have the ability to self-select social groups that mirror their current belief system or values and to evade traditional social controls such as parents, community, church, civic groups that might challenge those beliefs. Social networking provides the ability to find like-minded groups around the world and removes the geographical limitations of "real world" communities. Face-to-face controls (i.e., family,

schools, churches, civic groups) that have challenged socially unacceptable norms now have the potential of being muted or completely "tuned out."

In regards to social disorganization theories, social networking communities tend to have fewer stable members and may be more comparable to networked individualism rather than communities. Social norms, cultural transmission, or social consensus may not be present, or if they are present, may not be strong and/or unified. Research indicates that norms of online communities may not mirror socially acceptable norms found in face-to-face communities. For example, the new generation of Facebook users appear to be more accepting of behaviour that goes outside traditional norms (i.e., posting private, personal, or incriminating information). It also appears that wall posts from Facebook "friends" can influence or reinforce negative social activity that may or may not want to be directly disclosed by the user.

While social control and social disorganization theories can be used to suggest reasons why individuals choose to post incriminating evidence on their Facebook pages, there is still a real need to empirically study not only Facebook user's comments on their personal, community and group pages, but also to study user's "friend" wall posts/ comments. The author suggests further research on how social control and/or social disorganization theories might provide a theoretical foundation to help explain the desire to post criminal activities on Facebook.

Most of what we know about Facebook users and their attributes are based on studies from high school/college students. The author suggests studying criminals' motivations for posting criminal activities on Facebook. There is also a need to study criminal offenders' social networking profiles to see if online peers tend to encourage or discourage criminal behaviours.

## References

- Barker, V. (2009). *Older adolescents' motivations for social network site use: The influence of gender, group identity and collective self-esteem*. *CyberPsychology & Behavior*, 12 (2), pp. 209-213
- Citron, D. K., & Norton, H. (2011). *Intermediaries and hate speech: Fostering digital citizenship for our information age*. *Boston University Law Review*, 91(1435), pp. 1435-1484
- Cole, E.R. (2006). *Guess who else is reading those "Facebook" entries?* Retrieved October 21, 2011, from [http://www.black-collegian.com/news/bcwire/archives/facebook\\_employers\\_0306.htm](http://www.black-collegian.com/news/bcwire/archives/facebook_employers_0306.htm)
- Dolliver, M. (2007). *Despite appearances to the contrary, they're turning into normal adults*. *Adweek*, 48 (15), p. 40
- Facebook. (2011). *Facebook Statistics*. Retrieved October 21, 2011 from Facebook: <http://www.facebook.com/press/info.php?statistics>
- Funk, L. (2007). *Women on Facebook think provocative is empowering*. *USA Today*, p. A11
- Hirschi, T. (2002). *Causes of delinquency*. New Brunswick, NJ.: Transaction Publishers
- Jones, Q. (1997). *Virtual communities, virtual settlements and cyber-archaeology: A theoretical outline*. *Journal of Computer Mediated Communication*, 3 (3), p. 24
- Katz, J. (1998). *The social side of information networking*. *Society*, 35 (2), pp. 403-405
- Kornhauser, R. (1978). *Social sources of delinquency*. Chicago, IL. University of Chicago Press
- Masis, J. (2009). *Is this lawman your Facebook friend? Increasingly investigators use social networking websites for police work*, *Boston Globe*. Retrieved October 25, 2011, from [http://www.boston.com/news/local/articles/2009/01/11/is\\_this\\_lawman\\_your\\_facebook\\_friend/?page=full](http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend/?page=full)
- Marsico, E. M. (2010). *Social Networking websites: Are Myspace and Facebook the fingerprints of the 21st century?* *Widener Law Journal*, 19 (3), pp. 967-976
- Mikami, A. Y., Szwedo, D.E., Allen, J.P., Evans, M.A., & Hare, A.L. (2010). *Adolescent peer relationships and behavior problems predict your adults' communication on social networking websites*. *Developmental Psychology*, 46, pp. 46-56

- Orr, E., Sisic, M., Ross, C., Simmering, M., Arseneault, J. & Orr, R (2009). *The influence of shyness on the use of facebook in an undergraduate sample*. *CyberPsychology & Behavior*; 12 (3), pp. 337-340
- Peluchette, J. V. & Karl, K. A. (2007). *The prevalence of Facebook faux pas and students' "devil may care" attitudes*. Paper presented at the Midwest Academy of Management Meeting. Kansas City, MO, October 4-6, 2007
- Peluchette, J.V. & Karl, K.A. (2010): *Examining students' intended image on facebook: "What were they thinking?!"* *Journal of Education for Business*. 85, pp. 30-37.
- Pew Research (2007). *Social networking and teens*. Retrieved October 20, 2011, from <http://www.pewinternet.org/reports/2007/Social-Networking-Websites-and-Teens.aspx>
- Reich, S. M. (2010). *Adolescents' sense of community on Myspace and Facebook: A mixed-methods approach*. *Journal of Community Psychology*, 38 (6), pp. 688-705
- Robinson, T.G. (2006). *Not so private lives*. *CED*, 32 (9), pp. 45-46
- St. John, W. (2006, September 10). *When information becomes T.M.I.* *The New York Times*, 155(53698), Section 9.8
- Schmallegger, F. (2009) *Criminology Today: An Integrative Introduction*. 5th ed. Pearson Education: New Jersey
- Shaw, C.R. & McKay, H. D. (1931). *Social factors in juvenile delinquency: A study of the community, the family, and the gang in relation to delinquent behavior*. Prepared for the National Commission on Law Observance and Enforcement. U.S. Government Printing Office.
- Stone, B. & Brown, R. (2006). *Web of risks: Students adore social-networking sites like Facebook, but indiscreet postings can mean really big trouble*. *Newsweek*, 148(8/9), 76-77
- Weimann, G. (2010). *Terror on Facebook, Twitter and Youtube*. *Brown Journal of World Affairs*, 16 (2), pp. 45-54
- Walther, J., Van Der Heide, B., Kim, S., Westerman, D. & Tong, S. (2008). *The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep?* *Human Communication Research*, 31 (1), pp. 28-49
- Watkins, T. (2010) *Use of Twitter, Facebook Rising Among Group Members*, ABC News. Retrieved May 14, 2010, from <http://abcnews.go.com/print?id=9723899>
- Wheeldon, E. (2010). *A Social Society: The positive effects of communicating through social networking sites*. *Online Conference on Networks and Communities*, Retrieved October 27, 2011, from <http://networkconference.netstudies.org/2010/04/a-social-society-the-positive-effects-of-communicating-through-social-networking-sites/>
- Wellman, B. (2002). *Little boxes, glocalization and networked individualism? Digital cities II: Computational and sociological approaches*. Berlin: Springer, pp. 10-25
- Wellman, B., Quan-Haase, A., Boase, J., Chen, W., Hampton, K., Isla de Diaz, I., (2003). *The social affordances of the Internet for networked individualism*. *Journal of Computer Mediated Communications*, 8 (7)
- Young, K. (2011). *Social ties, social networks and the Facebook experience*. *International Journal of Emerging Technologies and Society*, 9 (1), pp. 20-34.

Eric Kyper and Roger Blake:

## Understanding the role of ethics in the intention to share files using P2P networks

### Abstract:

This research examines the role that ethics plays in an individual's intention to engage in peer-to-peer (P2P) file sharing. Previous studies have focused on P2P file sharing as primarily an act of piracy; and accordingly many, although not all, have found that ethical considerations do play a role in file sharing intentions. While piracy over P2P networks has continued and ethical predispositions clearly remain important issues, in the face of new business models and increased use of P2P file sharing for perfectly legitimate applications, the percentage of pirated files has decreased even as overall P2P network traffic has grown.

It is therefore important to understand a user's intentions to engage in P2P file sharing as a whole, without restricting that understanding to the single aspect of piracy. But because piracy is still a factor, it is critical to consider the role of ethics in those intentions. The objectives of this research are to propose and test a model of file sharing intentions based on the theory of planned behavior which considers ethical predisposition. Structural equation modeling is used to analyze our model. The results show that while ethical predisposition does not have a significant effect on intentions, other factors do. From this we draw several important conclusions regarding P2P file sharing. These are findings that have significance for network managers and internet service providers, both of who are greatly concerned about the impact of this mode of file sharing. This work is the first of its kind to provide a macro level understanding of the role ethics plays in file sharing in general, not restricted to illicit activities.

### Agenda:

Introduction	61
Background	61
The Theory of Planned Behavior	62
The Decomposed Theory of Planned Behavior	64
Hypotheses	64
Methodology	66
Analysis	66
Analysis	68
Discussion and Conclusions	69

### Authors:

Eric Kyper, Ph.D.

- School of Business and Economics, Lynchburg College
- ✉ [kyper@lynchburg.edu](mailto:kyper@lynchburg.edu)

Roger Blake, Ph.D.

- College of Management, University of Massachusetts Boston
- ✉ [roger.blake@umb.edu](mailto:roger.blake@umb.edu)

## Introduction

Research has investigated ethics with respect to an individual's intention to pirate copyrighted material using peer-to-peer (P2P) file sharing technology in prior work. However, to date few studies have investigated P2P file sharing outside of piracy (see Shen et al., 2010, Grodzinsky and Tavani, 2005). This has become more important as industry analysis has shown that legitimate file sharing has increased and the percentage of P2P files that are pirated has decreased (Multimedia Intelligence, 2008). The goal of this research is to explore the role of ethics in P2P file sharing (hereafter referred to simply as file sharing).

To do so we propose and test a model incorporating an index of ethical predisposition incorporated in the theory of planned behavior (TPB) (Ajzen, 1991); this theory has often been used in studies of user intentions with respect to technology (Venkatesh and Morris, 2003). The TPB guides our study by allowing us to measure behavioral intentions towards peer-to-peer file sharing while including both internal and external factors that can affect these intentions. The ethical index we use is one that has been previously validated in behavioral models of file sharing intentions (Gopal et al., 2004).

A study of the role ethics plays in an individual's file sharing is timely in light of the tremendous amount of Internet traffic now attributed to P2P file sharing and the keen concern of network managers on campuses and in corporations. Universities struggle with the potential legal liability associated with piracy, even if they passively allow it to take place on their networks (Gelpi, 2009).

In industry, beyond the obvious concerns of copyright holders such as the Recording Industry Association of America (RIAA), Internet service providers (ISPs) are greatly affected. For example, in 2008 the Federal Communications Commission issued an order against Comcast, one of the largest ISPs in the U.S. and directed this ISP to stop blocking or otherwise limiting the bandwidth of P2P traffic, in accordance with the FCC's Internet Policy Statement (FCC-08-183, 2008). Comcast first vigorously denied the allegations that they had been throttling P2P traffic, but later agreed to comply with the order while filing a suit to overturn it. In 2010 their suit was successful, and whether or not Comcast has resumed the practice against P2P traffic is unclear: in the same year of that ruling the company indicated it was not blocking P2P traffic but instead had a policy by which they would terminate accounts with "excessive use" (Comcast, 2010). In the meantime, a class action suit was filed against Comcast for blocking P2P traffic, a suit that settled with an award of \$16 for each of Comcast's customers (US-District.Court, 2010).

Clearly, P2P file sharing is an important issue today. A greater understanding of an individual's intention to file share is necessary before we create meaningful policies to encourage legitimate uses, curb illicit use, and design better network traffic management standards; the purpose of this paper is to contribute towards that understanding.

The remainder of this paper first discusses prior research of P2P file sharing intentions with a focus on ethical considerations, and then the theory of planned behavior. Next the hypotheses are presented followed by the methodology, analysis, and a discussion of the results. To clarify, for the purposes of this study file sharing is defined as the use of file sharing software for the purposes of either downloading or uploading content.

## Background

While their conclusions and methods have varied, researchers have generally found that ethical considerations have some effect on a user's intention to share files. For example, Chiou, Huang, and Lee (2005) included ethical decision-making within the construct termed "perceived social consensus" and focused on music piracy in Taiwan. These authors found that if the content holder, e.g. a record company or website such as Apple's iTunes, is perceived to be behaving fairly, then illegal downloading is not acceptable. But they also found that if an individual believes the content holder has behaved improperly then there is a justification for illegal downloading, calling into question the role of ethics in file sharing.

Gopal and Sanders (1998) determined that ethical predispositions had a significant relationship with software piracy in both the U.S. and India. Gopal, Sanders, Bhattacharjee, Agrawal, and Wagner (2004) applied a similar model focused on music piracy, and again found that the ethical predispositions index they studied was significantly related to piracy intentions. Their study concluded that more ethically inclined individuals were likely to download less. The study also found that other factors such as deterrence, legal actions, and education are not likely to be effective in reducing music piracy.

LaRose and Kim (2007) looked at moral justification as an antecedent to deficient self regulation and the intention to download music files, finding a significant relationship. They found that the belief structure of subjective norms, one of three such structures in the theory of planned behavior, was not related to intentions. Our research finds some contrasting results adding valuable contributions to the current literature.

In another study involving the role of ethics, Freestone and Mitchell (2004) found that when compared to a group of five activities downloading music or movies was viewed as the least wrong. Respondents may agree that illegal downloading is wrong, but that it is a lesser wrongdoing when compared to acts such as "using stolen credit cards" or "gaining unauthorized access to systems". In a similar vein, Altschuller and Benbunan-Fich (2009) used content analysis to conclude that half their respondents regard downloading as unacceptable, but that the majority of respondents condone others engaging in downloading.

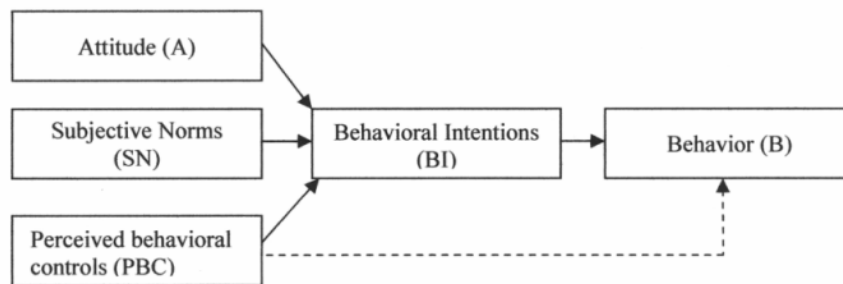
Finally, research has been inconclusive as to whether ethics are antecedents of either attitude or of behavioral intention, in studies related to file sharing more generally to P2P file sharing in particular. Lysonski & Durvasula (2008) found that ethical orientation was related to an awareness of the social costs and consequences of piracy, and found a general consensus that downloading is not morally wrong. However, they did not find a relationship between ethical orientation and attitude towards pirating MP3 files. They concluded that stressing the unethical aspects of downloading music illegally is unlikely to be an effective deterrent.

An important contribution of our study is that we are focusing on the possible role ethics has on an individual's intention to engage in file sharing regardless of the legality of the actions. The research reviewed shows the range of conclusions reached about ethics and the effects it has on file sharing intentions. However, in all of these studies ethics is only considered in legal situations. There is precedent to study file sharing at the macro level providing an understanding of individual intentions not bounded by legal specifics (see Blake and Kyper, 2011). Given the different results these studies have found for ethical considerations and the changing landscape of P2P file sharing more research needs to be done to clarify the role of ethics. Our study adopts the ethical predisposition index used by Gopal and Sanders in studies of both software and music piracy (Gopal et al., 2004, Gopal and Sanders, 1998), an index also used by d'Astous, Colbert, and Montpetit (2005) as an antecedent of attitude in the context of music piracy. Before discussing this index and how ethics was incorporated in that model, we discuss the theory of planned behavior next.

### **The Theory of Planned Behavior**

Our research model is based on Ajzen's theory of planned behavior (Ajzen, 1991, Ajzen, 1985). There are three belief structures with the direction of predictors posited by this theory shown in Figure 1.

Figure 1: The Theory of Planned Behavior (TPB)



The TPB states that a measurement of behavior (B) will be a weighted function of behavioral intention (BI) and perceived behavioral control (PBC) as:

$$B = w_1BI + w_2PBC$$

In turn, behavioral intention is a weighted function of the following monolithic belief structures: attitude (A), subjective norms (SN), and perceived behavioral control (PBC). If all individual internal and external factors are known, then this model is accurate within the limit of measurement error (Ajzen, 1991).

$$BI = w_3A + w_4SN + w_5PBC$$

Each monolithic belief structure is a predictor of behavioral intention; each of A, SN, and PBC has a separate formulation as shown in the following equation:

$$A = \sum(b_i)(e_i)$$

$$SN = \sum(nb_j)(mc_j)$$

$$PBC = \sum(cb_k)(pf_k)$$

Attitude (A) is the sum of the products of attitudinal belief ( $b_i$ ) and desirability of that outcome ( $e_i$ ). In this study we are measuring attitude towards using file-sharing software. This concept is represented by perceived usefulness and perceived ease of use as originally developed by Davis, Bagozzi, and Warshaw (1989). We include these constructs because they have been integral parts of every TAM study, and similar studies have found them significant in predicting behavioral intentions (Davis, 1993; Mathieson, 1991).

Subjective norms (SN) are the sum of the products of an individual's normative beliefs ( $nb_j$ ) regarding a particular referent, and the motivation to comply with that referent ( $mc_j$ ). Subjective norms are a function of both peer and superior influences. This allows us to measure the external pressure an individual feels to use file sharing software and the internal pressure to comply with those externalities.

The role of subjective norms in technology research is ambiguous. Initially Davis et al. (1989) did not find the concept significant. However, since that time other researchers have found subjective norms significant in theory of planned behavior models (Taylor and Todd, 1995). We include subjective norms because an individual could perceive their actions to have negative consequences.

Perceived behavioral control (PBC) is the sum of the products of control beliefs ( $cb_k$ ) and perceived facilitation ( $pf_k$ ) of the control belief. For example, if an individual may perceive a certain proficiency level is required to use a file sharing software package, and that proficiency is important in determining the usage behavior. We know from Ajzen (1991) that when an individual has complete control over behavioral performance, intentions alone should be a sufficient predictor. However, the fact that many individuals don't have

such complete control is readily apparent. For example, most users have no control over the speed of their network or the files that may be available to share at any particular point in time. ISPs have recently blocked or increased the response time of peer-to-peer networks (Andersen, 2008). In such cases an individual may have the intention to file share but lack access to the technology. Perceived behavioral control is an essential component of our study, and an important reason to choose the theory of planned behavior.

### The Decomposed Theory of Planned Behavior

In more recent years most studies have analyzed the decomposed version of the theory of planned behavior. In this version monolithic belief structures are decomposed into multi-dimensional belief constructs as shown in Figure 2. Several advantages are noted for this approach. First, Bagozzi (1981) and later Shimp and Kavas (1984) pointed out that it is unlikely that monolithic belief structures will consistently relate to the antecedents of intention. Decomposition allows the role of each structure to be more clearly understood. Second, decomposition overcomes some operationalization disadvantages pointed out by Mathieson (1991) and Berger (1993).

Our factors relating to attitude in our decomposed model are based on the technology acceptance model (TAM), first introduced by Davis et al. (1989) TAM is frequently used in studies of behavioral intentions, such as used in Yang, Hsu, and Tan's study of an individual's motivation to use YouTube (Yang et al., 2007). Decomposed models are also often used as factors in the constructs of subjective norms and perceived behavioral controls, such as in models of the intentions to use computer labs by Taylor and Todd (1995). and the intentions to download music over P2P networks by LaRose and Kim (2007). Decomposed models use specific factors for each of the TPB constructs, meaning the model translates readily to practice and is more managerially relevant. This last point is of particular interest to our research because we would ideally like to provide recommendations for deterrent and network management policies.

### Hypotheses

For the purposes of this study file sharing is defined as the use of file sharing software for the purposes of either downloading and/or uploading content.

Based on the above theoretical background we pose ten hypotheses to answer our research questions. The three main hypotheses represent the monolithic belief structures in the theory of planned behavior (attitude, subjective norms, and perceived behavior controls). *H1 – H3* each has related sub-hypotheses corresponding to the decomposed version of our model. Attitude is comprised of ethical intention, perceived ease of use, and perceived usefulness. Subjective norms are comprised of peer influences and superior influences. A perceived behavioral control is comprised of self-efficacy and technology facilitating conditions.

The theory of planned behavior states the more favorable an individual's assessment of a behavior, the greater peer pressure they feel, and the greater their perceived behavioral control over a behavior the greater should be their intention to perform the behavior. Of course we expect the relative importance of each determinant of intention to change depending on the specific behavior in question. Note that in figure 1 above perceived behavioral control influences both intention and behavior directly. According to the theory of planned behavior people's behavior is strongly influenced by their confidence in their ability to perform the behavior (perceived behavioral control). The reasons for this are as follows: first, assuming constant intention, effort expended to perform a behavior will increase with increases in perceived behavioral control. Second, perceived behavioral control can be used as a proxy for actual control (assuming the individual's perceptions of control are accurate).

Our hypotheses stated in the null are defined here and summarized in Figure 2:

*H1: An individual's attitude towards sharing files over peer-to-peer file-sharing has no impact on their intention to share files over peer-to-peer networks.*

*H1a: Ethical predisposition has no impact on an individual's attitude towards sharing files over peer-to-peer networks.*

*H1b: The perceived ease of use of peer-to-peer file-sharing has no impact on an individual's attitude towards sharing files over peer-to-peer networks.*

*H1c: The perceived usefulness of peer-to-peer file-sharing has no impact on an individual's attitude towards sharing files over peer-to-peer networks.*

*H2: An individual's subjective norms for peer-to-peer file-sharing have no impact on their intention to share files over peer-to-peer networks.*

*H2a: An individual's [social] peer influences on peer-to-peer file-sharing have no impact on their subjective norms for sharing files over peer-to-peer networks.*

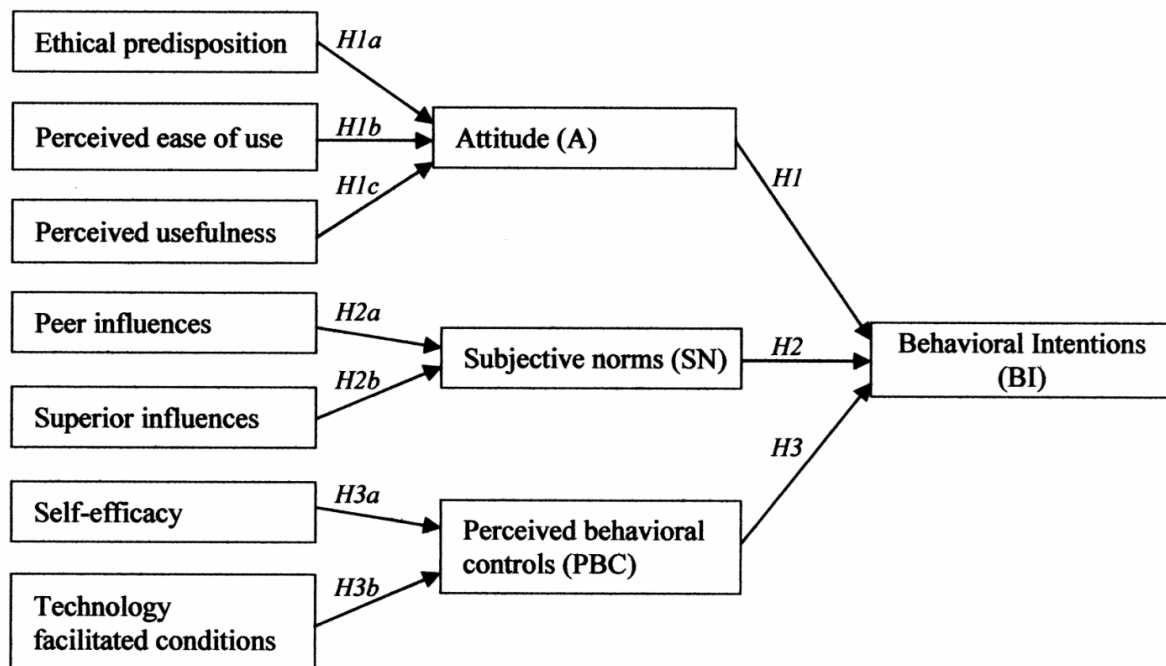
*H2b: An individual's superior influences on peer-to-peer file-sharing have no impact on their subjective norms for sharing files over peer-to-peer networks.*

*H3: An individual's perceived behavioral controls over peer-to-peer file-sharing have no impact on their intention to share files over peer-to-peer networks.*

*H3a: An individual's self-efficacy related to peer-to-peer file-sharing has no impact on their perceived behavioral control on sharing files over peer-to-peer networks.*

*H3b: The technology facilitated conditions for an individual to use peer-to-peer file-sharing have no impact on their perceived behavioral control on sharing files over peer-to-peer networks.*

Figure 2. Hypotheses from the decomposed TPB related to an individual's intention to share files



## Methodology

Our instrument measured the monolithic belief structures and the constructs separately. We asked questions about belief structures (e.g. subjective norms), which are each from the theory of planned behavior; these are classified as direct questions. We asked questions relating to each construct, considered indirect questions, because we are using the decomposed theory of planned behavior and each construct is related to a specific belief structure. Each measurement approach makes different assumptions regarding the underlying cognitive structures (Ajzen, 1991).

Based on the equations for the relationships in the theory of planned behavior, our survey instrument includes measures for the three monolithic belief structures and the constructs for each in the decomposed theory of planned behavior. We adapted existing scales for use in our study because they have been empirically validated in previous studies. Individual items were modified to reflect our specific technological context. Table 1 summarizes our measurement concepts which include monolithic belief structures and individual constructs comprising each structure, and the sources used for the items in our instrument.

Table 1. Measurement Constructs and Item Sources

Monolithic belief structure from the TPB	Construct	Source for items in instrument
Attitude	Ethical predisposition	Gopal et al. (2004)
	Perceived ease of use	Davis et al. (1989)
	Perceived usefulness	Davis et al. (1989)
Subjective norms	Peer influences	Taylor and Todd (1995)
	Superior influences	Taylor and Todd (1995)
	Efficacy	Taylor and Todd (1995)
Perceived behavioral control	Facilitating conditions – technology	Taylor and Todd (1995)

Our adaptations were doubled-checked using the procedures suggested by Ajzen (1991, 1985). With the exception of ethics related items, all survey items relate specifically to the peer-to-peer technology rather than computer usage in general or to alternate file-sharing technologies such as streaming media. This is in accordance with recommendations by Fishbein and Ajzen (1975).

There were 52 items in the instrument we used for a pilot study, each measured with a Likert scale having a range of one through seven. This study was conducted by collecting data from 20 students at two separate universities. While college students are a convenient sample, evidence supports the supposition that this group is among those most frequently sharing files over peer-to-peer networks; a 2005 NPD Group study reported this demographic are much more likely to be engaged in this activity d'Astous, Colbert, and Montpetit (2005).

Analysis of the pilot study indicated several redundant questions and several with inconsistent wording. These were either modified or removed, bringing the total number of items in our instrument to 46. This revised survey was administered to undergraduate and graduate students in business and economic programs at three universities in the Mid-West, Northeast, and Mid-Atlantic States, and analyzed as follows.

## Analysis

From a total of 246 solicitations for our revised survey we received 204 completed surveys, a response rate of 83%. As with our pilot study, all responses were anonymous and the completely voluntary nature of the survey was stressed; no incentive was offered to entice completed surveys. After removing surveys with one or more incomplete answers our sample size for analysis was 179. The reliability of each construct was measured by Cronbach's alpha and is summarized in Table 2. In the TPB manual for researchers Francis et al. recommend a cutoff of 0.6 as a rough guide for internal consistency scores (Francis et al., 2004).

Table 2. Chronbach's Alpha for Each Construct and Belief Structure

Construct	Chronbach's Alpha
Ethical predisposition	.71
Perceived ease of use	.85
Perceived usefulness	.78
Peer influences	.84
Superior influences	.92
Efficacy	.69
Facilitating conditions – technology	.81
Belief Structure	
Behavioral Intention (BI)	.81
Attitude – direct measure (A)	.87
Subjective Norms - direct measure (SN)	.82
Perceived Behavioral Control - direct measure (PBC)	.64

Once adequate reliability was established we determined the correlations between our direct measures for monolithic belief structures and our indirect measures for their associated constructs. Our instrument measured the monolithic belief structures and the constructs separately. First, we asked direct questions about a belief structure (e.g. subjective norms), because they address the structure directly they are considered as direct questions. Second, we asked questions relating to each construct, considered as indirect questions. Each measurement approach makes different assumptions regarding the underlying cognitive structures. A low correlation between the measurements of monolithic belief structures and the measurements for constructs would flag a problem that would need to be addressed before proceeding. Table 3 shows the correlations between our measures; all are significant at  $p < .05$  enabling us to proceed to further analysis.

Table 3. Correlations of direct and indirect measures; all significant ( $p < .05$ )

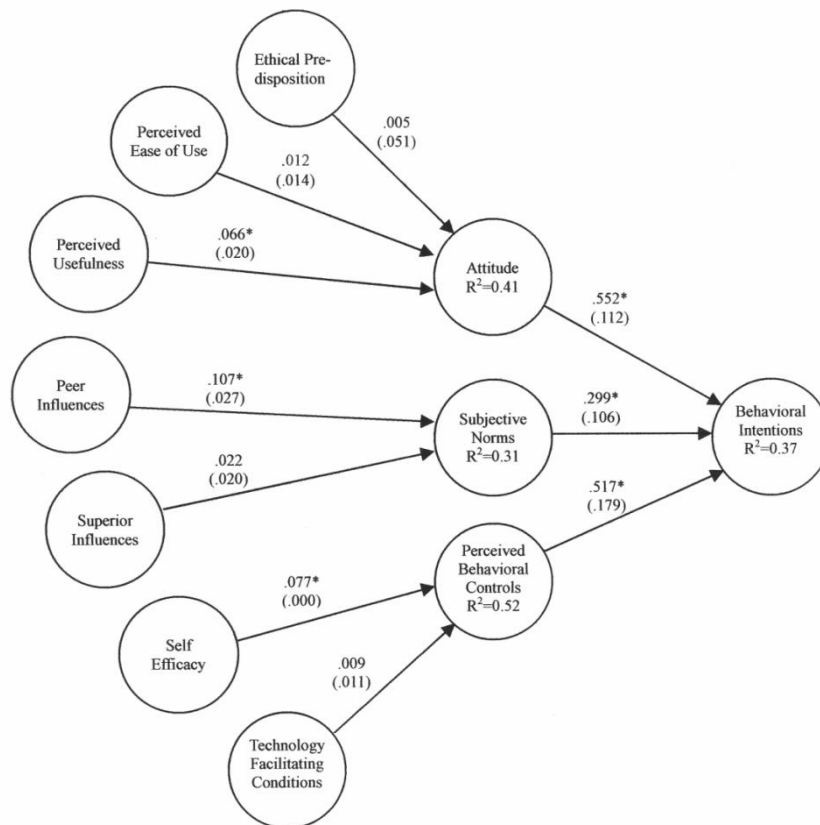
	A	SN	PBC	BI	A	SN	PBC	BI
A	1.00							
Indirect measures								
SN	0.35	1.00						
PBC	0.75	0.38	1.00					
BI	0.50	0.47	0.53	1.00				

	A	0.54	0.33	0.46	0.57	1.00			
Direct measures	SN	0.41	0.42	0.31	0.45	0.47	1.00		
	PBC	0.52	0.35	0.39	0.34	0.31	0.31	1.00	
	BI	0.38	0.43	0.40	0.62	0.37	0.24	0.26	1.00

## Analysis

We constructed a structural equation model using EQS 6.1 to test our decomposed theory of planned behavior modeled in figure 2 above. Figure 3 shows the path coefficients and standard errors for each construct (\* =  $p < .05$ ).

Figure 3. Path coefficients for the decomposed TPB model (standard errors) \* $p < .05$



The goodness of fit scores for the model are  $\chi^2 = 1594$ ,  $p < .0001$ ; CFI = .711; RMSEA = .100, with  $n = 179$ . The  $R^2$  value indicates that the decomposed theory of planned behavior model explains 41% of the variation in behavioral intentions. This is comparable to the  $R^2$  values from successful behavioral intention models in information systems research (Legris et al., 2003).

## Discussion and Conclusions

Our results show all three monolithic belief structures of the theory of planned behavior to be significant predictors of file-sharing intentions. However, these results indicate ethical predisposition is not a component of an individual's attitude towards file sharing. This is contrary to some previous research such as the findings made by Gopal et al. (2004). However, Gopal et al. were specifically studying intention to pirate music, while our study considers the activity of file sharing as a whole and is not focused solely on piracy. This is an important result for networks managers and ISPs grappling with how to manage P2P file sharing, and indicates that pointing to ethical considerations is likely to have no effect on users' intentions. ISPs are struggling to control P2P file sharing so that networks are not overwhelmed by relatively few users. Attempts to control this are likely going to have to be technological in nature and not attempt to rely on ethical values such as fairness.

Each monolithic belief structure is a significant predictor of behavioral intention. In addition, one construct was significant for each belief structure. Perceived usefulness, peer influences, and self-efficacy each are significant predictors of attitude, subjective norms, and perceived behavioral controls respectively. Our significant results mirror those of some previous studies described in the background section.

With regard to the constructs representing each belief structure, we conclude that perceived usefulness is a significant predictor of an individual's attitude towards file sharing, a result we expected. However, perceived ease of use was not. One possible explanation for the lack of significant results for perceived ease of use is that current users are comfortable with technology. This is supported by self-efficacy; those who feel confident in their ability are not concerned with the ease of learning file sharing software.

The finding that technology facilitating conditions do not affect intentions was counter to our expectations. We had expected the restrictions placed on this method of file sharing to have had some effects. One possible reason could be that our respondents are using networks with few if any limitations to file sharing. To assess this we sampled several colleges and universities. Each school had a policy for file sharing but had not taken any action to prevent it. Each school provided more than ample throughput to adequately support this technology, supporting the results we found for technology facilitating conditions.

Perhaps most interesting is what was found not to be significant. The results for the effects of superior influences suggest that parents, teachers, and authorities do not have much of an influence in determining an individual's intention to file share. This finding is consistent with previous research and the role of superior influences on music piracy through file sharing networks (LaRose and Kim, 2007). LaRose and Kim did not find subjective norms to be significant predictors of intention directly. However, they found this result puzzling and suggested that peer pressure may be the best way to convince people that their behavior is out of line with their peers.

Altschuller and Benbunan-Fich (2009) found that 67% of peers recommended downloading and file sharing. Indeed they found that a portion of their sample while they agree downloading is wrong, condone others engaging in music piracy and may participate themselves at some point. In our study Hypothesis H2a was supported for peer influences. Some previous research seems to support the idea that peer pressure may be a more effective means of influencing behavioral intention (and behavior) than superior influences. These results suggest that perhaps the best way to influence file sharing behavior is through changing the peer culture. Changing culture is notoriously difficult but we have at least anecdotal evidence of environments where the illicit use of file sharing is well below the norm for a U.S. college setting. For example Virginia Military Institute (VMI) has strict rules regarding file sharing, but students tend to enforce the rules among each other more than from the administration. Certainly the culture on that campus influences the students' sense of right and wrong.

There are limitations of this study. First, our sample is limited to undergraduate and graduate college students. While there is evidence that people in this age group are most likely to file share, they clearly don't constitute the population of file sharers. Extending future studies to a wider sample pool may increase the explanatory power of the model. Second, the resources file sharing networks are consuming world-wide are not bound to America, but affect the global on-line community. International versions of this study will play

an important role in understanding the cross-cultural differences in intention to file share. Finally, third, we measured a narrow definition of ethical predisposition. Expanding the measure of ethics to be more comprehensive may provide a better understanding of ethic's role in file sharing.

## References

- AJZEN, I. 1985. *From intentions to actions: A theory of planned behavior*. In: KUHL, J. & BECKMAN, J. (eds.) *Action control: From cognition to behavior*. New York: Springer Verlag.
- AJZEN, I. 1991. *The theory of planned behavior*. *Organizational Behavior and Human Decision Processes*, 50, 179-211.
- ALTSCHULLER, S. & BENBUNAN-FICH, R. 2009. *Is music downloading the new prohibition? What students reveal through an ethical dilemma*. *Ethics and Information Technology*, 11, 49-56.
- ANDERSEN, N. 2008. *Hammer Drops at Last: FCC Opposes Comcast P2P Throttling*. *ars technica* [Online]. Available: <http://arstechnica.com/old/content/2008/07/hammer-drops-at-last-fcc-opposes-comcast-p2p-throttling.ars> [Accessed].
- BAGOZZI, R. 1981. *Attitudes, Intentions, and Behavior: A Test of Some Key Hypotheses*. *Journal of Personality and Social Psychology*, 41, 607-627.
- BERGER, I. 1993. *A framework for Understanding the Relationship Between Environmental Attitudes and Consumer Behavior*. In: VARADARJAN, R. & JAWORSKI, B. (eds.) *Marketing Theory and Application*.
- BLAKE, R. & KYPER, E. 2011. *An investigation of the intention to share media files over P2P networks*. *Behaviour and Information Technology*, 30.
- CHIOU, J.-S., HUANG, C.-Y. & LEE, H.-H. 2005. *The antecedents of music piracy attitudes and intentions*. *Journal of Business Ethics*, 57, 161-174.
- COMCAST. 2010. *Frequently Asked Questions about Network Management* [Online]. Available: <http://customer.comcast.com/Pages/FAQViewer.aspx?Guid=24f9d063-b8ca-4c93-a528-cb62e1fd664b&fss=p2ppolicy#realworld> [Accessed].
- D'ASTOUS, A., COLBERT, F. & MONTPETIT, D. 2005. *Music piracy on the web-How effective are anti-piracy arguments? Evidence from the theory of planned behaviour*. *Journal of Consumer Policy*, 28, 289-310.
- DAVIS, F. D. 1993. *User acceptance of information technology: system characteristics, user perceptions and behavioral impacts*. *International Journal of Man-Machine Studies*, 38, 475-487.
- DAVIS, F. D., BAGOZZI, R. P. & WARSHAW, P. R. 1989. *User Acceptance of Computer Technology: A Comparison of Two Theoretical Models*. *Management Science*, 35, 982-1003.
- FCC-08-183. 2008. *Memorandum opinion and order, Formal complaint against the broadband industry practices of Comcast* [Online]. Available: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-08-183A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf) [Accessed].
- FISHBEIN, M. & AJZEN, I. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA, Addison-Wesley.
- FRANCIS, J. J., ECCLES, M. P., JOHNSTON, M., WALKER, A. E., GRIMSHAW, J. M., FOY, R., KANER, E. F. S., SMITH, L. & BONETTI, D. 2004. *Constructing questionnaires based on the theory of planned behaviour. A manual for health services researchers*. Newcastle upon Tyne, Centre of Health Services Research, University of Newcastle upon Tyne.
- FREESTONE, O. & MITCHELL, V. 2004. *Generation Y attitudes towards e-ethics and internet-related misbehaviours*. *Journal of Business Ethics*, 54, 121-128.
- GELPI, A. 2009. *Universities face new challenges in evolving file-sharing landscape*. *Campus Legal Advisor*, 9, 1-16.
- GOPAL, R. D. & SANDERS, G. L. 1998. *International software piracy: Analysis of key issues and impacts*. *Information Systems Research*, 9, 380-397.
- GOPAL, R. D., SANDERS, G. L., BHATTACHARJEE, S., AGRAWAL, M. & WAGNER, S. C. 2004. *A behavioral model of digital music piracy*. *Journal of Organizational Computing and Electronic Commerce*, 14, 89-105.

- GRODZINSKY, F. S. & TAVANI, H. T. 2005. P2P networks and the Verizon v. RIAA case: Implications for personal privacy and intellectual property. *Ethics and Information Technology*, 7, 243-250.
- LAROSE, R. & KIM, J. 2007. Share, steal, or buy? A social cognitive perspective of music downloading. *Cyberpsychology, Behavior, and Social Networking*, 10, 267-277.
- LEGRIS, P., INGHAM, J. & COLLERETTE, P. 2003. Why do people use information technology? A critical review of the technology acceptance model. *Information & Management*, 40, 191-204.
- LYSONSKI, S. & DURVASULA, S. 2008. Digital piracy of MP3s: Consumer and ethical predispositions. *Journal of Consumer Marketing*, 25, 167-178.
- MATHIESON, K. 1991. Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research*, 2, 173-191.
- MULTIMEDIA INTELLIGENCE, I. 2008. P2P: Content's "Bad Boy"; Tomorrow's Distribution Channel [Online]. Available: <http://multimediaintelligence.com> [Accessed October 23, 2008 2008].
- SHEN, X., YU, H., BUFORD, J. & AKON, M. (eds.) 2010. *Handbook of Peer-to-Peer Networking*: Springer.
- SHIMP, T. & KAVAS, K. 1984. The theory of reasoned action applied to coupon usage. *Journal of Consumer Research*, 11, 795-809.
- TAYLOR, S. & TODD, P. A. 1995. Understanding information technology usage: A test of competing models. *Information Systems Research*, 6, 144-176.
- US-DISTRICT.COURT. 2010. Hart v. Comcast. Case no. 2:08-MD-1992-LDD [Online]. Available: <http://p2pcongestionsettlement.com> [Accessed].
- VENKATESH, V. & MORRIS, M. 2003. User Acceptance of Information Technology: Toward a Unified View. *Management Information Systems Quarterly*, 27, 18.
- YANG, C., HSU, Y. & TAN, S. 2007. Predicting the Determinants of Users' Intentions for Using YouTube to Share Video: Moderating Gender Effects. *Cyberpsychology, Behavior, and Social Networking*, 13, 141-152.

#### Key of Item Abbreviations

E = Ethics  
 A = Attitude  
 SN = Subjective Norms  
 PBC = Perceived Behavioral Controls  
 BI = Behavioral Intention  
 PEAU = Perceived Ease of Use Attitudinal Component  
 PEAUD = Perceived Ease of Use Desirability of Outcome  
 PUA = Perceived Usefulness Attitudinal Component  
 PUD = Perceived Usefulness Desirability of Outcome  
 SNPIN = Subjective Norm – Peer Influences Normative Beliefs  
 SNPIM = Subjective Norm – Peer Influences Motivation to Comply  
 SNSIN = Subjective Norm – Superior Influences Normative Beliefs  
 SNSIM = Subjective Norm – Superior Influences Motivation to Comply  
 PBCECB = Perceived Behavioral Control – Efficacy Control Beliefs  
 PBCEFC = Perceived Behavioral Control – Efficacy Facilitating Conditions  
 PBCTCB = Perceived Behavioral Control – Technology Control Beliefs  
 PBCTFC = Perceived Behavioral Control – Technology Facilitating Conditions

**Appendix A: Survey Instrument (item key at bottom)**

Q#	Item	Question	Left Anchor	Right Anchor	Reverse Coded
1	E1	An executive earning \$150,000 a year pads his expense account by about \$5,000 a year.	always acceptable	never acceptable	Yes
2	E2	In order to increase profits a manager let a factory exceed the legal limits for environmental pollution.	always acceptable	never acceptable	Yes
3	E3	Because of pressure from company, a stock broker recommended a type of bond he didn't think was a good investment.	never acceptable	always acceptable	Yes
4	E4	A small business received quarter of its gross revenue in cash. The owner reported only half of that for income tax.	always acceptable	never acceptable	Yes
5	E5	An engineer discovered a possible design flaw he thought was a safety hazard. His company decided not to correct that flaw. The engineer decided to keep quiet instead of notifying anyone outside the company.	never acceptable	always acceptable	No
6	A1	Using file sharing software to share files is ...	a bad idea	a good idea	No
7	A2	Using file sharing software to share files is ...	worthless	worthwhile	No
8	A3	Using file sharing software to share files is ...	good for me	bad for me	Yes
9	A4	Using file sharing software to share files is ...	foolish	wise	No
10	SN1	People who influence my behavior would think that I should share files	definitely	definitely not	Yes
11	SN2	People who are important to me would think that I should share files	definitely	definitely not	Yes
12	PBC1	I would be able to share files using file sharing software	strongly agree	strongly disagree	Yes
13	PBC2	Being able to share files is entirely within my control	strongly agree	strongly disagree	Yes
14	PBC3	I have the resources and the knowledge and the ability to share files	strongly agree	strongly disagree	Yes
15	BI1	Thinking about past, how often have you shared files?	never	very often	No
16	BI2	Thinking about now, how often do you share files?	never	very often	No
17	BI3	I intend to share files in the future	definitely	definitely not	Yes
18	PEUA1	I could easily configure file sharing software to let me share files	likely	unlikely	Yes
19	PEUA2	I would find it easy to get file sharing software to do what I want it to do	likely	unlikely	Yes
20	PEUA3	My interaction with file sharing software would be straight forward	unlikely	likely	No
21	PEUA4	It would be easy to download file sharing software	unlikely	likely	No
22	PEUA5	It would be easy for me to become skillful at using file sharing software	likely	unlikely	Yes
23	PEUA6	I would find file sharing software easy to use	likely	unlikely	Yes
24	PEUD1	File sharing software that is easy to install/configure is:	desirable	undesirable	Yes
25	PEUD2	File sharing software that will do what I want is:	desirable	undesirable	Yes
26	PEUD3	File sharing software that is straight forward to use is:	undesirable	desirable	No
27	PEUD4	File sharing software that is easy to find and download is:	undesirable	desirable	No
28	PEUD5	Becoming skillful with file sharing software is:	undesirable	desirable	No
29	PEUD6	File sharing software that is easy to use is:	undesirable	desirable	No
30	PUA1	Using file sharing software would enable me to obtain content more quickly	likely	unlikely	Yes
31	PUA2	The files I want to have (software, music, video) are readily available through file sharing	likely	unlikely	Yes

32	PUA3	Compared to other options, file sharing software lets me obtain files faster	likely	unlikely	Yes
33	PUA4	I would find file sharing software useful	likely	unlikely	Yes
34	PUD1	Obtaining content more quickly is:	undesirable	desirable	No
35	PUD2	Readily available content through file sharing is:	undesirable	desirable	No
36	PUD3	Better options for obtaining content are:	undesirable	desirable	No
37	PUD4	Useful file sharing software is:	desirable	undesirable	Yes
38	SNPIN1	My friends would think that I should use file sharing software	strongly disagree	strongly agree	No
39	SNPIN2	My classmates would think that I should use file sharing software	strongly disagree	strongly agree	No
40	SNPIM1	Generally speaking, I want to do what my friends think I should do	strongly disagree	strongly agree	No
41	SNPIM2	Generally speaking, I want to do what my classmates think I should do	strongly agree	strongly disagree	Yes
42	SNSIN1	People that I respect use file sharing	strongly disagree	strongly agree	No
43	SNSIN2	People who are important to me engage in file sharing	strongly disagree	strongly agree	No
44	SNSIM1	Generally speaking I want to do what people I respect do	strongly disagree	strongly agree	No
45	SNSIM2	Generally speaking I want to do what people who are important to me do	strongly disagree	strongly agree	No
46	PBCECB1	I would feel comfortable file sharing	strongly agree	strongly disagree	Yes
47	PBCECB2	If I wanted to I could easily use file sharing software	strongly disagree	strongly agree	No
48	PBCECB3	I would be able to use file sharing software without having someone teach me	strongly disagree	strongly agree	No
49	PBCEFC1	Being comfortable using a technology is:	unimportant	important	No
50	PBCEFC2	Finding file sharing software easy to use is:	unimportant	important	No
51	PBCEFC3	Being able to use file sharing software without formal instruction is:	unimportant	important	No
52	PBCTCB1	I think file sharing is prohibited on the network I use	strongly disagree	strongly agree	No
53	PBCTCB2	File sharing is discouraged on the network I use	strongly disagree	strongly agree	No
54	PBCTCB3	The speed of my Internet connection is too slow for file sharing	strongly disagree	strongly agree	No
55	PBCTFC1	The ability to file share on my network is:	unimportant	important	No
56	PBCTFC2	Open access to file sharing on my network is:	unimportant	important	No
57	PBCTFC3	Approval of file sharing on my network is:	unimportant	important	No
58	PBCRCB1	The content I want is not available through file sharing	strongly disagree	strongly agree	No
59	PBCRCB2	The content I want is available in the file format I want	strongly disagree	strongly agree	No
60	PBCRFC1	Having content available is:	important	unimportant	Yes
61	PBCRFC2	Having content available when I want it is:	unimportant	important	No

Rafael Capurro:

## Never Enter Your Real Data<sup>1</sup>

### Abstract:

The present debate over privacy and security is on shaping freedom in the digital age. It seems unquestionable that ICT in general and social media in particular are changing the "web of relationships" (H. Arendt) that binds us. What makes this debate on ICT and social media unique is the fact that it takes place at a local and global level with different forms of synergy related to questions of friendship and fun no less than of oppression and justice. This paper addresses particularly the question about different forms of concealing and unconcealing ourselves in and through social media.

### Agenda:

Introduction	75
On Information Ethics and Information Moralities	75
On Privacy and Secrecy	76
Conclusion	76

### Author:

Prof. (em.) Dr. Rafael Capurro:

- Redtenbacherstrasse 9, 76133 Karlsruhe, Germany
- ☎ + 49 - 721 - 98 22 9 22 , ✉ rafael@capurro.de, 🌐 [www.capurro.de](http://www.capurro.de)
- Relevant publications:
  - Rafael Capurro - John Holgate (eds.). Messages and Messengers. Angeletics as an Approach to the Phenomenology of Communication. Munich: Fink 2011.
  - Intercultural Information Ethics. In: Kenneth Einar Himma and Herman T. Tavani (eds.): The Handbook of Information and Computer Ethics. New Jersey: Wiley 2008, p. 639-665.

---

<sup>1</sup> Contribution to the workshop "ICT Ethics and Public Policy", Europe House, EU Commission and European Parliament's UK Office, London, March 23, 2011.

## Introduction

During a conference on ethical issues of the information society in January 2011, a colleague told me about family problems dealing with privacy in social networks, and particularly on what his children do or do not with their personal data. Young people, he said, are fascinated by the opportunities offered by social networks, such as making friends, sharing personal issues or just having fun together. A young woman who was taking part at this conversation said: "I never enter my real data, that is to say, I try to avoid personal identification by giving, for instance, wrong data concerning my place of birth or age or whatever." I told her: "This looks like a Nietzschean imperative: 'Learn to lie if you want to survive in a digital environment!'" "Not bad for an ethicist," she said. Then she added: "But what happens if everybody follows this maxime?" This is a Kantian question, of course. The consequences would be very bad - not only for Mr Zuckerberg.

February 8, 2011 was "Safer Internet Day" organised by Insafe "to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people across the world" this year around the slogan "It's more than a game, it's your life." The present debate or, I should better say, the present obsession over privacy and security is on shaping freedom in the digital age. It is still unclear what is precisely the impact of ICT and particularly of social media such as Twitter or Facebook on recent social protests for instance in the Near East (Wikipedia 2011). But it seems unquestionable that ICT is changing the "web of relationships" or the "in-between" that binds us, to put it in Hannah Arendt's terms (Arendt 1998, 182). What makes this debate on ICT and social life unique is the fact that it takes place at a local and global level with different forms of synergy related to questions of friendship and fun no less than of oppression and justice. It is a debate about possible shapes of the "vita activa" (H. Arendt) in the digital age. It starts at a very young age when kids learn being online (Insafe 2011). Sherry Turkle has analyzed the paradoxes arising from what she calls being "alone together" (Turkle 2011). Maybe it is not so much the fear of being alone but of being lonely and isolated or even excluded from social relationships. We do not learn to be alone but we do learn new ways of being together (Capurro 1995). We look for new codes of being together. They arise from a broad social and academic debate where traditional norms and rules are challenged and 'good practices' are analyzed. These questions are at the core of the academic debate on information ethics (Himma and Tavani 2008).

## On Information Ethics and Information Moralities

The task of ethics as an academic discipline is to problematize a given morality. The alternative is a sclerotic social life in which a morality with its rules, taboos, values and bias of all kinds, is considered as obvious and unchangeable being mostly used as power instrument to legitimate hierarchies and privileges. Morality and ethics as its catalyst are essential for survival in a similar way as any living organism needs an immune system in order to deal with the environment.

Information ethics is the academic discipline dealing with the critical reflection on information moralities, particularly but not restricted to the impact of ICT on norms and values in human communication. In a broader sense, information ethics deals with comparative descriptive and normative studies of information moralities related to other media and as well as to different epochs and cultures. Eventually, information ethics might address today the impact of ICT on norms and values in all areas of human society including its interaction with nature and non-human living beings.

The difference between ethics (*philosophia ethiké*) or moral philosophy – that together with the reflection on politics (*philosophia politiké*) and on the administration of the house (*philosophia oikonomiké*) belong to what Aristotle calls practical philosophy (*philosophia praktiké*) – and morality (Greek: *ethos*, Latin: *mores*) is essential in order not to confuse a theory with its object. In everyday life, and sometimes also in academia, both terms, ethics and morality, are used as synonyms, thereby creating confusion. Ethics committees turn sometimes into moral ones. In today's understanding, ethics deals with the whole of human action in all its spheres (individual, group, society) within the limits of the *conditio humana*. The so-called applied ethics, such as bioethics, business ethics, ecological ethics etc., take a specific perspective on such spheres of human practices.

## On Privacy and Secrecy

In her book "Privacy in Context" media theorist Helen Nissenbaum rightly criticizes the public/privacy dichotomy as detached from specific contexts. Within such contexts, norms provide the framework for what she calls "contextual integrity." "Contexts," she writes, "are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)." (Nissenbaum 2010, 132). Niklas Luhmann's system theory calls such contexts "systems" (Luhmann 1996). This is a theoretical perspective that Nissenbaum also implicitly shares with hermeneutics according to which the process of understanding a text in what it says and what remains hidden is related to a framework of "pre-understanding" of both, the author and the reader, that can be made explicit through interpretation, leading to understanding and to a new pre-understanding. Philosophical hermeneutics, as developed by Hans-Georg Gadamer (1975) following Heidegger's existential hermeneutics, further developed this issue with regard to our own understanding as human beings. The encounter between existential hermeneutics and the theory of computerized information storage and retrieval in the 1980s (Capurro 1986, Winograd and Flores 1986) was a forerunner of Nissenbaum's contextual thinking. The success of the WWW is due not only to its globality but also to its locality. New mobile applications allowing to physically localize people as well as any kind of objects show clearly the relevance of contextuality.

Social life is about concealing and unconcealing what and who we are according to different forms of trust and security. We are neither a society of angels nor one of devils, neither a fully open society nor a secret one. This is the reason why the difference between public and private as well as between public and secret is so relevant for every human society (Capurro and Capurro 2007). The concepts of public and private do not refer to properties of data. They are not first-order concepts. Data and their properties play different roles related to what they conceal and unconceal in different contexts of social life. Public vs private no less than public vs secret are second-order concepts. In other words, their understanding with regard to the data depends on the specific social interplay. This contextual relativity should not be misunderstood at the normative level as a moral relativism but as a necessity to specify which norms and values are at stake in a specific context. Let us take for instance the proposal of my colleague 'never enter your real data' in, for instance, an online community like Facebook and in a scientific community. Am I morally obliged to unconceal my personal data in a context dealing with fun and friendship following, for instance, Facebook's "Statement of Rights and Responsibilities" (Facebook 2011)? Can I conceal my real identity, my name for instance, using a pseudonym? If such a norm is not specified by the community nothing seems to be against it. I am not lying in this case but just playing a social game although the creator of the software might expect the contrary and try to use my data for other purposes. My virtual friends may or may not expect that my data are correct or that I might conceal or change them. In case of the scientific community its *ethos* implies that I do not conceal my name except, for instance, with regard to exceptional political situations (Strauss 1988). This rule applies vice versa: I should not omit or conceal my sources, particularly in the case of quotations but also of giving credit to authors that are the immediate source of 'my' ideas. Plagiarism in science is no less morally and legally reprehensible than fakes in industry and the arts. The question as to whether my name, address, affiliation and so on are private or public, or if I may conceal or reveal them depends on the context in which they are embedded.

This takes us to the problem of "maintaining multiple personas online" as Michael Zimmer remarks with regard to his ambiguous experiences with Moli, a platform that makes it possible to separate, for instance, personal and professional lives, which is difficult to do with Facebook (Zimmer 2008; Naone 2008). The problem is, as Zimmer remarks, "[w]hile I can set the privacy levels for each profile, *Moli gets to see it all...* all linked to my single account with a common e-mail address, zip code, birthdate and gender." (ibid.) This case clearly shows the problems of data protection and data exchange between different contexts. In this case it is a matter of a commercial platform but what if this is done by political power?

## Conclusion

What lessons can we learn so far? We live in a digital era in which the *habeas corpus* mutates into *habeas data* (EGE 2005, 29): 'We shall not lay digital hand upon thee.' But the question is how this legal procedure

can be applied in a globalized world, or, who is this 'we' and what kind of 'hands' can be laid upon which (digital) bodies. In other words, the question of informed consent, a leading principle in medical ethics, should be a major technical, ethical, and legal issue with regard to all kinds of personal data in different contexts.

The pragmatic imperative: 'Learn to contextualize!' is an educational problem starting at a very early age. Where it is said: 'enter your name' you should enter your nickname. It is just for fun, after all. This is a kind of guerilla tactic in a complex digital environment that might help to make not so easy the connection between data coming from different contexts without the explicit consent of the person(s) or institutions involved. The design of platforms for children and young people can provide different ways of making this contextuality technically possible and understandable. But this needs a complement in moral and ethical education at home and in school. Guerrilla tactics is in some way a fight against digital giants. It needs a legal supplement making the case of data migration between contexts an issue for the legal protection of individual freedom. Data protection is about freedom not just about data. Allowing political, commercial and economic power unlimited access and transfer of data arising from different contexts with different moral and legal rules means nothing less than undermining "contextual integrity" and it can be a precursor of various kinds of digital totalitarianism. This is particularly the case when every human being can be digitally identified and this code becomes even a legal must for all kinds of digital transactions in whatever context and for whatever purpose.

## Acknowledgements

Thanks to Michael Eldred (Cologne) and Daniel Nagel (Stuttgart) for their corrections and suggestions.

## References

- Arendt, Hannah (1998): *The Human Condition*. Chicago: The University of Chicago Press.
- Capurro, Rafael (1995). *Leben im Informationszeitalter*. Berlin: Akademie Verlag.
- Capurro, Rafael (1986). *Hermeneutik der Fachinformation*. Freiburg/München: Alber.
- Capurro, Rafael and Capurro, Raquel (2007). *Secreto, lenguaje y memoria en la sociedad de la información*. <http://www.capurro.de/secreto.html>
- EGE (European Group on Ethics in Science and New Technologies) (2005). *Ethical Aspects of ICT Implants in the Human Body*. Opinion No. 20. [http://ec.europa.eu/bepa/european-group-ethics/publications/opinions/index\\_en.htm](http://ec.europa.eu/bepa/european-group-ethics/publications/opinions/index_en.htm)
- Facebook (2011). *Statement of Rights and Responsibilities* [http://www.facebook.com/note.php?note\\_id=183538190300](http://www.facebook.com/note.php?note_id=183538190300)
- Gadamer, Hans-Georg (1975). *Wahrheit und Methode. Grundzüge einer philosophische Hermeneutik*. Tübingen: Mohr.
- Himma, Kenneth E. und Tavani, Herman T. (eds.) (2008). *The Handbook of Information and Computer Ethics*. Hoboken, New Jersey: Wiley.
- Insafe (2011). *Play and Learn: Being online. New activity booklet for children aged 4-8 years*. <http://www.saferinternet.org/web/guest/activity-book>
- Luhmann, Niklas (1996). *Soziale Systeme*. Frankfurt am Main: Suhrkamp (6th ed.)
- MOLI <http://down.moli.com/>
- Naone, Erica (2008). *Maintaining Multiple Personas Online A new site lets users create profiles for the different sides of their personality*. In *Technology Review*, Feb 11, 2008. <http://www.technologyreview.com/Infotech/20183/page1/?a=f>
- Nissenbaum, Helen (2010). *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
- Safer Internet Day (2011) <http://www.saferinternet.org/web/guest/safer-internet-day>
- Strauss, Leo (1988). *Persecution and the Art of Writing*. The University of Chicago Press.

*Turkle, Sherry (2011). Alone Together: Why We expect More From Technology And Less From Each Other. New York: Basic Books.*

*Wikipedia (2011). Egyptian Revolution of 2011. [http://en.wikipedia.org/wiki/Egyptian\\_Revolution\\_of\\_2011](http://en.wikipedia.org/wiki/Egyptian_Revolution_of_2011)*

*Winograd, Terry and Flores Fernando (1986). Understanding Computers and Cognition: A New Foundation for Design. Norwood, New Jersey: Ablex.*

*Zimmer, Michael (2008): Moli: Maintaining Multiple Personas Online, Sharing More Personal Information. <http://michaelzimmer.org/2008/02/11/moli-maintaining-multiple-personas-online-sharing-more-personal-information/>*

Sara L. Puotinen (Opinion Paper):

## Twitter Cares? Using Twitter to Care About, Care for and Care With Women Who Have Had Abortions

### Abstract:

In this paper, I argue that Angie Jackson and her live-tweeting of her abortion and Steph Herold, and development of the #ihadanabortion hashtag, used twitter to practice empathy-as-care. Challenging the perception, fueled by newspaper reports, television news segments, popular accounts of scientific studies and academic articles, that twitter strips us of our empathy and makes us uncaring and apathetic, I explore how Angie Jackson's live-tweet and Steph Herold's hashtag enabled users to care about, care for and care with women who have had abortions. While the caring practices that these projects allowed for were tenuous, fleeting and not always successful, their presence on twitter indicates that social media like twitter have the potential to enable us to care and should be taken seriously as spaces with ethical value.

### Agenda

Introduction.....	80
Twitter's Many Critics .....	80
Caring For, Caring About, Caring With .....	81
Caring About.....	82
Caring For.....	82
Caring With.....	83
Conclusion.....	83

### Author(s):

Prof. Dr. Sara L. Puotinen:

- University of Minnesota, 425 Ford Hall, Minneapolis, MN 55455
- Email and personal homepage: ✉ [puot0002@umn.edu](mailto:puot0002@umn.edu), 💻 <http://trouble.room34.com>

## Introduction

In February 2010, after finding out she was in the very early stages of an unwanted and potentially dangerous pregnancy, Angie Jackson decided to have an abortion using RU-486 and live-tweet about it. Her intention, as she announced it on twitter, her blog and a YouTube video, was to “demystify” abortion. Over the course of several weeks, she tweeted frequent updates about the physical and emotional effects of RU-486 in real time.

In November 2010, Steph Herold created a twitter hashtag, #ihadanabortion, and encouraged people to use it in their tweets in order to make visible their abortion stories and to link those stories together. Within days, #ihadanabortion was a trending topic on twitter, with more than 2000 tweets using the hashtag, as people “came out” with their accounts of having abortions.

Overwhelmingly, the criticisms of these twitter projects focused on tweeting about abortion as either a political or moral issue. Critics discussed how Jackson’s and the #ihadanabortion tweets functioned and failed as political tools for the pro-choice movement, arguing that twitter could not be used to persuade people to rethink their stance on abortion and that pro-choice organizers, like Steph Herold, were doing more harm than good to the cause of abortion rights. Critics also discussed the impropriety of tweeting about such a private and controversial issue and claimed that tweeting about abortion, at best, displays “bad manners” and, at worst, demonstrates a shocking lack of moral beliefs and values.

What was missing from both political and moral critiques of tweeting about abortion was a discussion of ethics and ethical practices. What, if any, ethical practices did Angie Jackson and the twitter users who included Steph Herold’s #ihadanabortion hashtag in their tweets engage in on twitter? And what ethical practices did they encourage in others?

In this paper, I argue that Jackson, Herold, and the individuals who marked their tweets with the #ihadanabortion hashtag, used twitter to practice empathy-as-care. Challenging the perception, fueled by newspaper reports, television news segments, popular accounts of scientific studies and academic articles, that twitter strips us of our empathy and makes us uncaring and apathetic, I explore how Angie Jackson’s live-tweet and Steph Herold’s hashtag enabled users to care about, care for and care with women who have had abortions. While the caring practices that these projects allowed for were tenuous, fleeting and not always successful, their presence on twitter indicates that social media like twitter have the potential to enable us to care and should be taken seriously as spaces with ethical value.

## Twitter’s Many Critics

Reactions were mixed, but the popular reception to Angie Jackson’s live-tweet and Steph Herold’s #ihadanabortion hashtag was negative as critics branded these two uses of twitter as inappropriate and unproductive. Some critics claimed that tweeting personal stories about having an abortion trivializes the issue because twitter is not a space for users to have serious and meaningful reflections about their lives. Instead, it is a space for pointless babble, where users tweet about everything that they are doing, thinking, and eating right at the moment that it is happening and without any reflection on its value or whether or not they should share it with others. This “cult of immediacy,” generates information and stories that are ephemeral and function primarily as distractions that “go in one ear and out the other” (Keller 2010, 2).

Other critics suggested that in using twitter to share their stories, users offer up too much private information about themselves to the public. For these critics, tweeting about how abortion feels or when you had one goes beyond oversharing unimportant details about everyday life; it’s “inappropriate,” “crass,” “too blunt,” “distasteful,” and displays “bad manners” (Jezebel 2010). These critiques reflected a more general dislike of twitter as a space that encourages people to blur the line between private and public and to reveal too much information about their lives, too often and too quickly.

And, some critics argued that twitter was the wrong venue for developing meaningful connections between those who tweeted about their abortions and those who read and shared the tweets with others. Online message boards, website forums specifically for women who have had abortions, pamphlets, and books were all discussed as spaces that were more appropriate than twitter for publicly sharing stories. Using twitter to tweet about abortion, many claimed, could indicate to others that one either has too cavalier of an attitude about a serious issue or is deliberately attempting to provoke and outrage, as a publicity stunt, to make a political point, or just for the fun of shocking others. In either case, these critics argued that using twitter to spread awareness about women's abortion stories does not change any perspectives about the issue and does not enable people to listen to, reflect on or connect over stories about women's experiences with abortion.

While these criticisms tended to focus on the political and moral impact of tweeting about abortions, we can also link their charges against twitter as too trivial, too concerned with inappropriate oversharing and not meaningful enough, with some more general critiques of twitter and its (lack of) ethical value.

Many critics are skeptical of twitter's ethical potential. Peggy Orenstein worries that "when every thought is externalized" and "when we reflexively post each feeling," we lose insight, reflection and, possibly empathy (2010, 2). Bill Keller echoes Orenstein's concerns, writing that new technologies like twitter "may be eroding characteristics that are essentially human: our ability to reflect, our pursuit of meaning, a genuine empathy, a sense of community connected by something deeper than snark or political affinity" (Keller 2010, 2). Central to their concerns is the fate of empathy within the twitter age. Both believe that empathy is essential for being engaged, reflective and ethical citizens. And both caution that twitter is contributing to its erosion because it encourages people to be self-centered, superficial and apathetic to the experiences or wants and needs of others.

To support her case against twitter, Orenstein draws upon the findings of a recent study by the University of Michigan. In this study, researchers evaluated college students on seventy-two different campuses between 1979 and 2009 and determined that a sharp decline in empathy, particularly in terms of concern for others and the ability to take on others' perspectives, has occurred since 2000. In evaluating the causes of this decline, the authors propose that the students' increased time online, particularly in social media spaces like facebook or twitter, has possibly been a factor. As students spend more time online, the authors argue, their offline engagements and relationships have suffered; students are less able to effectively interact with others offline, they spend less time in offline activities, and they have less close friends offline with which to share their private feelings. Additionally, social media's overemphasis on self-expression and individual wants and needs coupled with its overabundance of personal accounts of pain and violence, could be fueling the narcissism of "Generation Me" and desensitizing them to the suffering of others (Konrath/O'Brian/Tsing 2011, 189).

## Caring For, Caring About, Caring With

Both Orenstein and Konrath/O'Brian/Tsing speculate that a decline in empathy is at least partly the result of social media. However, this conclusion, which is based only on anecdotal evidence, does not account for the ways in which using social media like twitter may actually allow for users to be more, as opposed to less, empathetic. In *Share This! How You Will Change the World with Social Networking*, Deanna Zandt argues that using social media to share information and find community provides opportunities for not only paying attention to others, but also sharing in their stories. In contrast to Orenstein and Konrath et al, Zandt claims that social media provides us with new ways in which to share our stories with each other, to build up trust and understanding, to individually and collectively become aware of other ways of living and thinking, and to expand our networks of connections. As a result, "we're becoming more connected, and thus have the capacity to be more empathetic." This empathy, she continues, "will lead us away from the isolation and resulting apathy that we've experienced as a culture" (Zandt 2010, 40).

Zandt's suggestion that social media could increase our capacity for empathy is evidenced in Jackson's and Herold's twitter projects. Both Jackson and Herold used twitter to spread awareness about women's experiences with abortion and to provide twitter users with access to stories to which they may not have previ-

ously been exposed. Angie Jackson aimed to demystify the physical process of having an abortion for others and to let them know that it is not nearly as scary as she had imagined. And Steph Herold wanted to destigmatize abortion and create a space where women could share their stories and make visible how abortion is not the “sin of a few bad woman,” but “a regular part of women’s lives” (Baker/Herold 2010).

In both cases, tweeting about abortion was about spreading awareness and making those experiences visible that have been rendered invisible by mainstream media. It was about initiating a conversation on a difficult and painful topic and enabling twitter users to have access to ideas, feelings, experiences and stories that they might not find in other online or offline spaces. It was about cultivating an awareness and a caring for these women and their experiences and providing a wide range of folks—those who have had abortions, those who haven’t, those who are opposed to abortion, those who only want to hear “certain” stories about having an abortion—a space to develop empathy and to share in the stories of women whose abortion experiences usually do not get heard and are devalued, dismissed and/or ignored. And, it was about providing a means for women who have had or were contemplating having an abortion to connect with, care for and provide support for each other. For all of these reasons, Jackson’s live-tweet and Herold’s #hashtag project made possible multiple expressions of empathy in caring about, caring for and caring with other twitter users.

### Caring About

According to Joan Tronto, caring about “involves noting the existence of a need and...assuming the position of another person or a group to recognize that need” (1994, 106). Both Jackson’s and Herold’s twitter projects encourage users to pay attention to the stories of women having abortions. The short, 140-character limit of tweets and the common practice on twitter of frequently sharing moments of everyday life, allowed Jackson to repeatedly share her ongoing and ever-changing experiences of the physical effects of RU-486. Through twitter, she was able to document what it physically and emotionally felt like to use RU-486 in real time and without filtering or shaping those feelings to fit into a polished or appropriate narrative that would make her story more palatable but less authentic and less reflective of the messy process of actually experiencing an abortion. And she was able to do so in a way that enabled those following her to read about her experiences as they were happening. While reading her live-tweets did not lead to expanded empathy and caring about her or other women having abortions for everyone, for some it provided a space for gaining awareness and bearing witness to a new perspective.

While Jackson used live-tweeting to honestly communicate and make people aware of her individual story, Step Herold used another key feature of twitter to spread awareness about the many different experiences of women having abortions; she created the #iahdanabortion hashtag. In marking their tweets with this hashtag, twitter users connected their stories together in one continuous, ever-expanding feed. When anyone using twitter clicked on the hashtag, they were able to read a wide range of stories and experiences, many of which were not usually visible to a broader audience, especially outside of the prochoice movement. Reaching a broader audience did lead to flame wars, with anti-choice users marking their critiques against abortion with the #ihadanabortion hashtag, but it also enabled more people to access these abortion stories and to not only gain a better understanding and awareness of women’s physical and emotional experiences with abortion, but to connect with the stories, either by recognizing similarities with their own experiences or the experiences of loved ones or by being moved by the powerfully and sometimes painfully and brutally honest accounts in the tweets.

### Caring For

Both Jackson’s and Herold’s twitter projects did not only encourage others to have empathy by becoming aware and learning to care about women and their stories of abortion, however. These twitter projects also enabled the creators and participants to engage in their own practices of caring for and caring with.

Caring for combines two key features of Tronto’s ethics of care framework: 1. Taking care of, or “assuming some responsibility for the identified need and determining how to respond to it” (1994, 106) and 2. Care-giving, or meeting the identified need through specific practices (1994, 107). In live-tweeting her abortion,

Angie Jackson cared for others. She wanted to demystify abortion for other women not only so people would pay attention to or care about women having abortions, but in order to let women know that using RU-486 was not as scary or painful as they might imagine and that there are non-surgical options available, if women want or need them. Through her detailed and frequent tweets about the process—the varying levels of pain she was experiencing, the physical effects of RU-486, her ongoing feelings of relief, discomfort, annoyance, and frustration—Jackson was able to educate women on how the process feels, providing them with information that they would not otherwise have access to, either because it wasn't available or because they felt uncomfortable asking medical professionals or friends and family about it.

Through this live-tweeting process, Jackson cared for others (both real and imagined); she identified a need—the need for women to have access to unbiased and non-judgmental information about non-surgical abortion procedures—and took responsibility for meeting that need by using twitter to provide that information in a straightforward and honest way. Using twitter was crucial in enabling her to provide this information. Because twitter is public and accessible in many different ways, her tweets reached more people. And, because tweets are short, frequent, unfiltered and often focused on everyday experiences, she was able to document the details of the process as it was happening and easily and effectively share them with others.

### Caring With

While Jackson used her twitter project to care for, Herold used the #ihadanabortion hashtag to allow others to care with. Caring with speaks to Tronto's broader definition of care as an ongoing collective process of reaching out to and working with others and to Zandt's understanding of empathy as sharing stories to build up trust and solidarity.

The participants in Steph Herold's #ihadanabortion project, cared with others. In tweeting about their stories of abortion and then marking those stories with the #ihadanabortion hashtag, these women helped to create a public, open space that while not entirely safe and free of risk was supportive and enabled a diverse group of people to come together and care about and care for each other. In reading and replying to each other's tweets, users created an environment that encouraged an ever-expanding amount of people to share their stories and to feel supported in their frequently painful and difficult decisions to have abortions. This space was not entirely depoliticized, but because the emphasis was on enabling women to "connect with one another," "hear each other's stories," and "understand one another," it became more of a place for caring with each other than fighting for a specific political agenda (Baker/Herold 2010).

Again, using twitter, particularly the hashtag feature, was crucial in allowing for this form of care. It enabled a wide range of users with very different stories about abortion to connect with each other and, in contrast to other online spaces where stories were private and open to a select few or made to conform to the specific policies of a site, it allowed women to share "all kinds of abortion stories" (Herold in the Nation), thereby creating a powerful and public timeline of people supporting all (not just a select few) or each other's reproductive choices.

### Conclusion

Critics of twitter frequently ignore and/or dismiss its ethical potential. While it is important to take these critiques seriously, it is also important to challenge them and to explore the various ways in which twitter users are engaging in ethical practices. Moreover, it is essential that we attend to the specific features of twitter, as opposed to other forms of social media, that might encourage us to be ethical, particularly in the form of expressing empathy-as-care. Angie Jackson's live-tweets during her abortion and Step Herold's #ihadanabortion hashtag, are two valuable examples of using the specific features of twitter to generate empathy and care for, about and with others. While these twitter projects were not entirely successful, they serve as important starting points for critical and meaningful discussions about ethical practices on twitter.

## References

- Baker, Aspen and Steph Herold. 'I Had An Abortion,' in 140 characters or Less: An Exchange With Steph Herold and Aspen Baker. Retrieved November 10, 2011 from <http://www.thenation.com/article/156420/i-had-abortion-140-characters-or-less-exchange-steph-herold-and-aspen-baker>.
- Boyd, Danah and Sarita Yardi. (2010). Dynamic Debates: An Analysis of Group Polarization Over Time on Twitter. *Bulletin of Science Technology & Society*, 30 (5): 316-327.
- Jackson, Angie. (2011) @Antitheistangie. Retrieved November 10, 2011 from <https://twitter.com/#!/antitheistangie>.
- Jezebel. (2010) Why Tweeting About Abortion Isn't 'Trivializing'. Retrieved November 10, 2010 from <http://jezebel.com/i-had-an-abortion>.
- Keller, Bill. (May 18, 2011). *The Twitter Trap*, New York Times.
- Konrath, Sara H., Edward H. O'Brian and Courtney Hsing. (2011). Changes in Dispositional Empathy in American College Students Over Time: A Meta-Analysis. *Personality and Social Psychology Review*, 15 (2), 180-198.
- Newman, Arnie. (2010) I had an Abortion 2.0. Retrieved November 11, 2011 from [http://www.rhrealitycheck.org/blog/2010/11/04/i-abortion-tweet-ing?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+rhrealitycheck+%28RHRealityCheck.org%29](http://www.rhrealitycheck.org/blog/2010/11/04/i-abortion-tweet-ing?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rhrealitycheck+%28RHRealityCheck.org%29).
- Orenstein, Peggy. (July 30, 2010). *I Tweet, Therefore I Am*. New York Times.
- Serena. (2010). Steph Herold: Tweeting to End Abortion Stigma. Retrieved November 10, 2011 from <http://feministsforchoice.com/steph-herold-tweeting-abortion-stigma.htm>.
- Stanek, Jill. (2010). Live Tweeting an abortion. Retrieved November 10, 2011 from <http://www.wnd.com/?pageId=126860>.
- Stevenson, Stacy Elizabeth and Lee Ann Peek. (2011). "I am Eating a Sandwich Now": Intent and Foresight in the Twitter Age. *Journal of Mass Media Ethics*, 26 (1): 56-65.
- Tronto, Joan. (1994) *Moral Boundaries: A Political Argument for an Ethic of Care*. New York: Routledge.
- Twitter. (2011). #i-had-an-abortion. Retrieved November 10, 2011 from <https://twitter.com/#!/search?q=%23i-had-an-abortion>.
- Wakeman, Jessica. (2010). "I'm Live-Tweeting My Abortion." Retrieved November 10, 2011 from <http://www.thefrisky.com/2010-02-24/im-live-tweeting-my-abortion-on-twitter>.
- Zandt, Deanna. (2010). *Share This! How You Will Change the World with Social Networking*. San Francisco: Berrett-Koehler Publishers.

William Bülow (Opinion Paper):

## Pluralism about the Value of Privacy

### Abstract:

This paper responds to two counterexamples to the view that privacy is valuable because of its connection to personal autonomy. It is argued that these counterexamples fail to establish that personal autonomy is not relevant for the value of privacy, but only the cautious claim that respect for personal autonomy alone is not the only reason for which privacy ought to be respected. Based on the response to the counterexamples a distinction between value-monistic and value-pluralistic accounts about the value of privacy is introduced and it is argued that there are reasons for accepting a value-pluralistic approach to privacy.

### Agenda

Introduction	86
Counterexamples to autonomy-based accounts of the value of privacy	86
Value-pluralism about privacy	87
Final remarks	88

### Author:

Mr. William Bülow (M.A)

- Division of Philosophy, KTH Royal Institute of Technology, Teknikringen 78 B, 100 44 Stockholm, Sweden
- ☎ + 46 73 333 63 17 , ✉ [william.bulow@abe.kth.se](mailto:william.bulow@abe.kth.se)

## Introduction

The current debate on the concept of privacy certainly indicates the complexity of this concept. While all classical theories of privacy have attractive characteristics they all face difficult problems. One might say that on each account something is missing and it does not provide the whole story. The same observation, it seems, holds for discussions on the value of privacy. Why, exactly, is privacy held to be valuable and why ought there to be a right to privacy? In order to account for this issue, different suggestions have been given, such as the respect for human dignity<sup>1</sup>, its connection to personal autonomy<sup>2</sup> or that privacy concerns is as an expression for the need of safety and security.<sup>3</sup>

In this paper focus will be on one proposal, namely that privacy is valuable because of its connection to personal autonomy. More specifically, this paper will focus on two counterexamples that aim at refuting the claim that privacy is important because of this supposed connection. While these arguments are presented against the view that privacy derives its value from the value of personal autonomy, it is not obvious that they are successful in doing this. Instead I will argue that if these counterexamples establish anything, this is only the more cautious claim that privacy is not valuable because of its connection to personal autonomy alone (Section 1). Based on this insight I will introduce a distinction between *value-monistic* accounts about the value of privacy and *value-pluralistic* accounts. According to value-monistic accounts privacy derives its value from one source and one source only. In contrast value-pluralism holds that privacy derives its value from a plural of sources and not from one alone. In this section I suggest that we do have reasons for embracing a value-pluralistic account (section 2). Finally, I will make some concluding remarks about the argument presented here (Section 3).

## Counterexamples to autonomy-based accounts of the value of privacy

In the philosophical literature on privacy several authors have suggested that the value of privacy derives its value from personal autonomy.<sup>4</sup> That is, the protection of privacy is a safeguard for the protection of undesirable access of others and is necessary for individuals in order to be able to control aspects of themselves in a self-determination way. This view is at least *prima facie* plausible. As he points out in his famous paper "Why privacy is Important", James Rachels suggests that privacy is important because of its social function, enabling us to control how we present ourselves to others which is crucial in order to uphold and create different sorts of relationships.<sup>5</sup> Also, as Rössler emphasizes that the loss in control over personal information may come to limit individuals' autonomy. She writes:

"If it can in principle no longer be taken for granted that one has control over one's informational self-determination or that one is not (constantly) being observed, and if, as a result, one must (constantly) present oneself as though one were being observed, the result is a loss of autonomy in terms of the authenticity of one's behaviour, which is turned into behaviour *as if*, that is alienated behaviour."<sup>6</sup>

Focusing on privacy and its connection to autonomy, authors have argued that there are counterexamples in which privacy is violated while there is no violation to peoples' personal autonomy. One proposed argument against autonomy-based conceptions of privacy is that when we encounter instances where a person is incapable of autonomous decisions, this person still has privacy claims. A person in a coma has privacy interests but is incapable of making autonomous decisions, which is held to imply that autonomy is not

<sup>1</sup> von Silva-Tarouca Larsen, Beatrice: Setting the Watch: Privacy and the Ethics of CCTV Surveillance

<sup>2</sup> Rössler, Beate: The Value of Privacy

<sup>3</sup> Moor, James: Towards a theory of privacy for the information age

<sup>4</sup> Johnson, Debora: Computer ethics; Palm, Elin: Securing privacy at work: the importance of contextualized consent; Rössler, Beate: The Value of Privacy

<sup>5</sup> Rachels, James: Why privacy is Important

<sup>6</sup> Rössler, Beate: The Value of Privacy pp. 128-9.

always an issue in connection with privacy claims. Von Silva-Tarouca Larsen suggests that this provides a reason for seeing respect for human dignity, rather than the respect for personal autonomy as the source of value for privacy.<sup>7</sup>

A different argument, put forth by James Moor, points out that it is possible to imagine a person, A, who secretly searches a person B's financial records, medical records and criminal records etc. Also, A knows about B's late mortgage payments, propensity to hemorrhoids, and that B once had a driving while intoxicated charge that B has long forgotten about. A is has also installed cameras in B's home which records B's every moment. However, B knows nothing about this. A really enjoys watching B's life and to him it is like a soap opera. According to Moor there is something disturbing about A's behavior. But A is not sharing any of the information, nor is he hurting B in any way. Moreover, Moor concludes, this does not violate B's autonomy. In contrast Moor suggests that privacy is valuable because it is an expression of a need for security and safety.<sup>8</sup>

While these arguments are presented as arguments against the view that privacy derives its value from the value of personal autonomy, it is not obvious that they are successful in doing this. In order to see this we must analyze what is actually at stake and what the premises of these arguments are. I suggest that both arguments share a similar structure which can be summarized as follows:

1. If an autonomy-based conception of the value of privacy is correct, every privacy violation can be explained in terms of violations to personal autonomy.
2. There are instances in which privacy is violated but personal autonomy is not.
3. Hence, autonomy-based accounts of the value of privacy are incorrect.

In response to this sort of arguments one might deny premise 2, a strategy that is defended elsewhere.<sup>9</sup> But despite whether any of these arguments are successful or whether any of the proposed counterexamples are convincing, there is yet another problem with the arguments posted by von Silva-Tarouca Larsen and Moor. What both Moor and Silva-Tarouca Larsen try to prove is that while privacy is valuable, this is not because of its connection to personal autonomy. But in order to do so, they must first assert that either privacy is valuable because of its connection to personal autonomy, or personal autonomy is irrelevant for the value of privacy. This, however, seems like a very hasty and queer assumption. Why, exactly, should we assume that if privacy is valuable, it gains its value from one source and one source only? There are no good reasons for accepting this assumption without argument. In fact, I believe that by making this assumption explicit, it becomes obvious what is strange about the argument and why the conclusions drawn are too hasty. Instead, if the arguments proposed by Moor and von Silva-Tarouca Larsen shows anything at all, it is that respect for personal autonomy alone is not the only reason for which privacy ought to be respected. It is not enough to establish the claim that privacy gains no value whatsoever from its connection to personal autonomy.

## Value-pluralism about privacy

So far, it has been argued that neither Moor's nor Silva-Tarouca Larsen's arguments are successful in refuting personal autonomy as a value-giving feature to privacy. Based on this insight it is beneficial for the discussion to introduce a basic distinction between theories about the value of privacy. First there are value-monistic accounts about the value of privacy, according to which privacy derives its value from one source and one source only. In contrast there are value-pluralistic accounts about the value of privacy, according to which privacy derives its value from a plural of sources and not from one alone. Taking this distinction into account it is clear that Moor and Silva-Tarouca Larsen are successful in refuting value-monistic versions of autonomy-based accounts about the value of privacy. But they are not successful in refuting value-pluralistic versions in which privacy derives its value partly from personal autonomy.

<sup>7</sup> von Silva-Tarouca Larsen, Beatrice: *Setting the Watch: Privacy and the Ethics of CCTV Surveillance*

<sup>8</sup> Moor, James: *Towards a theory of privacy for the information age*

<sup>9</sup> Bülow, William, Wester, Misse: *The Right to Privacy and the Protection of personal data in a Digital Era and the Age of Information*

What is important in this context is that not only do Moor's and Silva-Tarouca Larsen's fail to refute the claim that personal autonomy is a value-giving feature to privacy, but also their own proposals are not incompatible with this claim. That respect for privacy is important because of its connection to personal autonomy does not exclude neither Moor suggestion that privacy is important because it is an expression for safety nor von Silva-Tarouca Larsen that respect for privacy derives its value from the notion of human dignity. None of them is in a necessary conflict with the idea that respect for privacy often provide us with a reason for respecting privacy. Hence, one can (and perhaps should) embrace a value-pluralistic view on privacy including all of these proposals. In fact, is not hard to imagine a case where at least two or more of these reasons are involved: that is, they are all violated as a result of a privacy violation. The case of aggregating digital data, for instance, may both decrease safety as well as violate personal autonomy if it is being misused. Furthermore, adopting a value-pluralistic account fits well with how we reason about privacy issues and how we express concerns about possible privacy issues and how different reasons are often given in favour of privacy protection. Taking Moor's proposal that privacy concerns are an expression for the need of safety we don't want every information about ourselves available to everyone, since it makes us vulnerable. Reduced privacy enhances the risk for what informational-based harms such as stalking or perhaps identity theft. If we consider personal autonomy surveillance and the fact that we may be under surveillance affects and shapes our behavior and hence decrease our personal autonomy. Finally, if we consider the privacy concerns of a coma patient who is unlikely to recover we may say that it is against human dignity not to respect his privacy. In each case, the reasons given in favour of privacy protection or in the name of privacy make sense and cannot necessarily be generalized to other privacy issues. That privacy is important for several reasons, and hence derives its value and importance from plural sources does not come as a surprise. Despite this, further developing pluralism about the value of privacy could provide a good analytical framework for evaluating ethical problems involving privacy. For these reasons it is concluded that value-pluralism about the value of privacy is plausible and should be held to be an interesting approach towards solving the axiological problems of privacy.

## Final remarks

I have argued that there are reasons for adopting what I have called a value-pluralistic account of privacy. So far, however, I have not provided with a clear picture of its content, but merely given an account for its structure. Also, I have assumed without argument that the value of privacy is a derived value. Perhaps this is false and that privacy is a fundamental value in its own right. However, I haven't seen any arguments for this view and since the account I have proposed is both plausible and shows how we can solve certain problems within the discussion about privacy and its value I leave it to others to prove that this is actually the case.

## References

- Bülow, W., Wester, M. (Forthcoming). *The Right to Privacy and the Protection of personal data in a Digital Era and the Age of Information*, i Akrivopoulou, Ch. M., Garipidis, N. (red.) *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies*. Pennsylvania: IGI Global.
- Johnson, D.G. (2001). *Computer ethics*. (3. ed.) Upper Saddle River, N.J.: Prentice Hall.
- Moor J. (2004). *Towards a theory of privacy for the information age* in Bynum, T. W., Rogerson, S. (ed), *Computer ethics and professional responsibility*, (pp. 249-262). Malden, Mass. : Blackwell Publishing:
- Palm, E. (2009). "Securing privacy at work: the importance of contextualized consent", *Ethics and Information Technology* 11: 233-241
- Rachels, J. (1975), "Why Privacy is Important" *Philosophy and Public Affairs*
- Rössler, B. (2005). *The Value of Privacy*, Cambridge, Polity Press.
- Von Silva-Tarouca Larsen, B. (2011). *Setting the Watch: Privacy and the Ethics of CCTV Surveillance*. Oxford: Hart.