# Privacy and Social Networks: From Data Protection to Pervasive Computing

**Antoni Roig**[(1)]

(1) Institute of Law and Technology (IDT-UAB), Universitat Autònoma de Barcelona
Faculty of Law, Building B, Campus UAB, Bellaterra (08193), Spain
antoni.roig@uab.es

### Abstract

Technological threats to privacy are not limited to data protection. Social Network Applications (SNA) and ubiquitous computing or Ambient Intelligence face other privacy risks. The business model of SNA and the improvement of data mining allow social computation. SNA Regulation should then favor privacy-by design and Privacy Enhancing Technologies (PET). Default friendly-privacy policies should also be adopted. The data portability of the applications shifts SNA into a new field of ubiquitous computing. Therefore, the solutions of the Ambient Intelligence should be also analyzed in the context of SNA.

## Legal Framework

### Data protection regulation

Data protection regulations are considered by some authors a reference base for the development of methodologies tailored to design privacy-aware systems (Guarda, Zannone, 2009). The first step is to summarize the privacy principles:

(1) Fair and Lawful Processing
(2) Consent
(3) Purpose Specification
(4) Minimality: the collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose.
(5) Minimal Disclosure
(6) Information Quality
(7) Data Subject Control
(8) More protection to sensitive data
(9) Information Security (Guarda, Zannone, 2009)

### Data Protection Recommendations

A report from 2008 is perhaps up until today the most relevant legal framework on WBSN and privacy ("Rome Memorandum"). The Rome Memorandum recommendations to regulators are:
- Introducing the option of a right to pseudonymous use.
- Ensuring that service providers are honest and clear about what information is required for the basic service. Specific problems exist with consent of minors.
- Making data breach notification obligatory for social network services.
- Possibly attributing more responsibility to WBSN providers for personal data content on WBSN.
- Improving integration of privacy issues and tools into the educational system.

Another interesting document is the European Network and Information Security Agency Position Paper 1. Some of the recommendations are:
- WBSN should, where possible, use contextual information to educate people in 'real-time'.
- Awareness-raising campaigns should also be directed at software developers to encourage security conscious development practices and corporate policy.
- The regulatory framework governing WBSN should be reviewed and, where necessary, revised:
•What is the legal position on deletion of user generated content by service providers if it is classed as WBSN spam?
•What is the legal position on image-tagging by third parties?
•Who is responsible for security flaws resulting from user-generated markup or scripting?
•How should privacy policies of embedded third party widgets be communicated to users?
•What exactly constitutes personal data in a WBSN environment?
•What is the legal position on profile-squatting?
•Should the posting of certain classes of data by minors (location data) be made illegal?
- Users should be given accurate information on what is done with their data before and after account closure. WBSN should be used in a controlled and open way (i.e. not banned or discouraged), with coordinated campaigns to educate students, teachers and parents.

Recently, we can mention the Working Paper nº163 of the article 29 Group, dealing with online social communities, of June 12th, 2009. This study considers that the European Directive of data protection covers also the SNA scenario: the new aspects of this recommendation are perhaps the reference to security tools and "privacy-friendly" default settings. For the first time, a recommendation mentions Privacy Enhancing Technologies as a solution, even if limited, to the problem of the privacy of young users.

### Beyond data protection

But privacy cannot be limited to the data protection regulation. The German Constitutional Court published a decision in February 2008 that establishes a new "basic right to the confidentiality and integrity of information-technological systems" as part of the general personality and privacy rights in the German constitution. The ruling explains the relevance of using information-technological systems for the expression of personality. Weiss considers that this right could be easily applied to social network profile data (Weiss, 2009).

## Privacy preserving tools and procedures

The ISO has at least achieved consensus on four components of privacy, as follows (Wright *et al.*, 2009):

- Anonymity ensures that a subject may use a resource or service without disclosing user identity.
- Pseudonymity ensures that a user may use a resource or service without disclosing identity, but can still be accountable for that use.
- Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

However, SNA need new PETs focused on transparency, automatic compliance assurance functions and proactive communications techniques on risks (Weiss, S., 2009).

The complete transparency and control of the usage of the user's PII is only possible with privacy-by-design practices for designers and developers. PETs can't be simply an added tool, but have to be incorporated at the first stages of the design or the application development.

A recent study show that while there is now some use of privacy settings by SNA users, there is still a significant portion of SNA users who have not changed their permissive settings and allow unknown users to view private bits of information. SNA must clearly indicate the bare minimum of private information needed for a particular set of interactions (Krishnamurthy *et al.*, 2008). The default privacy settings should be the bare minimum.

The adoption of some type of proactive communication would be also useful. Indeed, there should be options for the user to easily report privacy invasions.

## New challenges: Data Portability

Data mining and screen scrapping applications automatically infer real-word connections, and discover communities and individuals. Indeed, identifying consumer preferences is a key challenge in customizing electronic commerce sites to individual users.

The problem comes also from the inside. PII data from SNA have more and more applications to run with, or "mash up" applications. That's the reason why Weiss proposes a privacy threat model for SNA portability (Weiss, 2009):

- Information privacy needs to be controlled on the data (PII) level.
- The user needs to be able to determine the sensitivity and context of the PII provided.
- Privacy-preserving data portability can only work if the user can earmark the PII provided with individual privacy preferences.

In order to respect individual privacy preferences, the user self-control and the ease of public accessibility, further research is announced on semantic technologies for tagging data for context and purpose, transparency-enhancing technologies and Digital Rights Management (Weiss, 2009).

## Future Trends: Privacy and pervasive computing

The deployment of pervasive computing casts doubt on the extent to which privacy is legally protected in public spaces (De Hert *et al.*, 2009). In case law, the European Court of Human Rights has introduced the notion of ''reasonable expectation of privacy''. But ubiquitous computing is turning the reasonable expectation of privacy into an expectation of being monitored. Furthermore, pervasive computing needs as many data as possible, and this clearly clashes with some of the main principles of data protection law, like the data minimization principle, collecting as little data as necessary, and the purpose specification principle, using the collected information only for the purpose defined at the moment of data collection (De Hert *et al.*, 2009).

With the emergence of Ambient Intelligence or pervasive computing, the definition of personal data needs to be reconsidered (Wright *et al.*, 2009). Furthermore, the distinction between personal and other data in a ubiquitous computing world is difficult to maintain. Perhaps it is time for data protection tout court. So instead of using identifiability as a criterion, privacy relevant data should rather be all those that can be used to affect our behavior and decisions (Wright *et al.*).

Another important issue is the transparency of the processing. What will become important in the context of SNA is the profiling knowledge, that is to say, the access to the profile. This information could make comprehensible why the environment takes some actions, and could even help to prove liability in case of damage (Wright *et al.*, 2009). PETs could provide important factual means of transparency. Transparency-enhancing technologies (TETs) could contribute to information exchange and management. An example of a TET is the so-called ''sticky policies'', that stick to or follow data as they are disseminated (Hildebrandt, Meints, 2006). Sticky policies would provide clear information and indicate to data processors and controllers which privacy policy applies to the data concerned (De Hert *et al.*, 2009).

Concretely, for mobile, ubiquitous social awareness applications, some useful principles are (Raento, Oulasvirta, 2008):

1. Support lightweight permissions
2. Assume reciprocity
3. Make it possible to appear differently to different people
4. Allow for commenting, modifying and framing automatic disclosure
5. Provide for feedback
6. Allow the user to lie
7. Do not take control away from the user
8. Allow opportunistic use
9. Do not try to do everything within the system

In any case, Ambient Intelligence, or ubiquitous computing, requires a shift to privacy-by-design and PETs (Wright *et al.*, 2009). Regulatory authorities and/or industry leaders could usefully encourage or formalize this option. Some research consortia, under the European Commission 6th Framework Programme, are good examples.

## Conclusion

No single measure will adequately respond to the challenges to privacy posed by SNA and the ubiquitous Information Society. Rather, some combination of measures will be needed (Wright *et al.*, 2009). Privacy Principles, like Fair Information principles (FIPs) or data protection principles are not enough. We are assisting to, perhaps, the very first stages of an important shift: the proportionality and transparency can widen the traditional data protection principles. But, if we want to face to new possibilities of data portability or pervasive computing, we have also to encourage the adoption of PETs and TETs. Furthermore, this has to be done with privacy-by-design practices, and not leaving these to a second moment of the implementation. We can go on indicating how these changes are transforming the privacy right, but perhaps it's time now to analyze and offer concrete solutions to concrete SNA. This will require an in depth study of the privacy policies of a concrete SNA, and lawyers and designers working together in future applications adopted with privacy-by-design practices.

## References

Buchegger, S., Schiöberg, D., Vu, L.-H and Datta, J., 2009. PeerSoN: P2P Social Networking. Early Experiences and Insights concepts of law, *SNS'09*, March 31, 2009, Nuremberg, Germany.

Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M. and Thuraisingham, B. 2009. A Semantic Web Based Framework for Social Network Access Control, *SACMAT'09,* June 3–5, 2009, Stresa, Italy.

De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., González Fuster G., 2009, Legal safeguards for privacy and data protection in ambient intelligence, *Pers Ubiquit Comput* , 13 (2009):435–444.

Felt, A., & Evans, D. (2007). *Privacy protection for social networking APIs*. http://www.cs.virginia.edu/felt/privacy/ retrieved 2009-08-25.

Fogel J. and Nehmad, E. 2009. Internet social network communities: Risk taking, trust, and privacy concerns, *Computers in Human Behavior*, 25 (2009): 153–160.

Guarda, P. and Zannone, N. 2009. Towards the development of privacy-aware systems, *Information and Software Technology,* 51 (2009): 337–350.

Guha, S., Tang, K. and Francis P. 2008. NOYB: Privacy in Online Social Networks, *WOSN'08*, August 18, 2008, Seattle, USA.

Hildebrandt M., and Meints M. eds. 2006. RFID, profiling, and AmI, *FIDIS*, Deliverable D7.7. of the Future of Identity in the Information Society project, available at http://www.fidis.net.

Kacimi, M., Ortolani, S. and Crispo, B. 2009. Anonymous Opinion Exchange over Untrusted Social Networks, *SNS'09*, March 31, 2009, Nuremberg, Germany.

Kalloniatis C., Kavakli E. and Gritzalis S. 2008. Addressing Privacy Requirements in System Design: the PriS Method, *Requirements Engineering*, 13 (2008): 241–255.

Korolova, A., Motwani, R., Nabar, S. U., Xu, Y. 2008. Link Privacy in Social Networks, *CIKM'08*, October 26–30, 2008.

Krishnamurthy, B. and Wills, C. E. 2008. Characterizing Privacy in Online Social Networks, *WOSN'08*, August 18, 2008, Seattle, USA.

Lucas, M., and Borisov, N. 2008. FlyByNight: Mitigating the Privacy Risks of Social Networking, *WPES'08*, October 27, 2008, Alexandria, Virginia, USA.

McDonald, A.M.. Reeder, R.W., Kelley, P.G. and Cranor, L.F. 2009. A Comparative Study of Online Privacy Policies and Formats, In Goldberg and M. Atallah (Eds.): PETS 2009, *LNCS* 5672 (2009): 37–55.

Raento, M. and Oulasvirta, A. 2008. Designing for privacy and self-presentation in social awareness, *Pers Ubiquit Comput,* 12 (2008):527–542.

Ravichandran, R., Benisch, M., Kelley P.G. and Sadeh, N.M. (2009), Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden? In Goldberg and M. Atallah (Eds.): PETS 2009, *LNCS* 5672 (2009): 1–18.

Weiss, S. (2009), Privacy threat model for data portability in social network applications, *International Journal of Information Management* 29 (2009):249–254.

Wright, D., Gutwirth, S., Friedewald, M., De Hertb, P., Langheinrich, M and Moscibroda (2009), A., Privacy, trust and policy-making: Challenges and responses, *Computer Law & Security Review,* 25 (2009): 69–83.