Privacy issues in social networking: the European perspective

By Avv. Felix Hofer

1. Reports and statistics inform us periodically about the booming impact of social forums, -platforms or -networks on Netizens all over the World. Europe clearly doesn’t go exempt from the effects of such phenomenon: according to survey results published in Spring 2009 Facebook ranks as the number one social network in Europe with an incredible share of 4.9% of the time spent on-line by Internet users⁴. While in a country like the United Kingdom, the popular social network had been able to achieve in 2008 the remarkable target of about 22 million of unique visitors per month, even in geographic regions with significantly lower Internet use Facebook’s popularity simply exploded: in Italy, a country behind most of all other EU member states in Internet usage, the social network had approximately 2 million registered users in 2008, but 6.5 million twelve months later⁵. During the same period the number of unique monthly visitors has increased from 382,000 up to over 10 million! In a recent statement a Facebook manager has claimed that the network “…has surpassed 100 million active mobile users worldwide”.

2. Given these figures it’s definitely no surprise that companies from various industry sectors are keen on trying to develop potential business applications with a specific focus on social network users. Who wouldn’t like to reach out to and touch base with such an audience (and basin of potential customers)? We’ve therefore been noticing increased efforts for communicating with the people present on social networks, for monitoring their habits and views, for influencing their opinions and for directing their spending power. Companies targeting ‘social net-workers’ have started thinking about how to measure the effectiveness of their marketing efforts towards the new business environment. In parallel, they have also learned – sometimes in very unpleasant ways - to fear the terrific rampant impact, which their brands can easily suffer from negative comments posted on social networks both, by upset, unsatisfied or disappointed customers as well as by ranting individuals.

3. Again, no surprise that the booming phenomenon of social networks has also attracted the attention of lawmakers, authorities, watchdogs and groups advocating specific interests.

Increasing concern has arisen about aspects⁶ such as:
- data safety (frequently visitors got hit by identity theft and frauds),

---

¹ This paper was prepared as a handout to the audience attending the session “SOCIAL MEDIA AND ITS COLLISION WITH GLOBAL PRIVACY AND DATA PROTECTION” at the Advertising Law & Public Policy Conference 2010 organized by the Association of National Advertisers - ANA in Washington DC, on March 17th & 18th, 2010.
² Felix Hofer is a naming and founding partner of the Italian law firm Studio Legale Associato Hofer Lösch Torricelli, in Firenze (50132), via Giambologna 2/rosso; he may be reached through the following contact details: Phone +39.055.5535166, Fax +39.055.578230 – e-mail: fhofer@hltlaw.it (personal) or info@hltlaw.it (firm e-mail).
³ In February 2009; according to a Comscore report published on April 15th, 2009 just a year earlier the share figure was down to 1.1%.
⁴ Which basically means that more than 10% of the entire Italian population nowadays has a Facebook account. The figures appears quite impressive, but actually not that much if we consider that 83% of Filipino (and 80% of Korean) Internet users have created a social networking profile.
⁵ Which makes it a plus 2.617%; according to a recent study, currently the figure of unique monthly visitors is quickly approaching the 20 million figure.
⁶ A recent study released – in February 2010 under the title “Online as soon as it happens” - by the European Network and Information Security Agency – ENISA contains interesting details on the risks involved by on-line presence.
access related problems for certain categories of visitors (e.g. minors uploading or becoming exposed to improper content\textsuperscript{7} or female, young or elderly visitors establishing dangerous contacts or entering into risky relations),

unforeseen side effects deriving from on-line posts (an (in the author’s opinion) innocent and funny picture taken at the office’s Christmas party and uploaded to a social platform could encounter the employer's interest and disciplinary action; the same goes for an employee supposedly on illness leave, but actually blogging about the good time he’s enjoying on his surfboard in an exotic location)\textsuperscript{8},

additional risks both technology related as well as affecting individuals' social relations, the fact that not only ‘diamonds’, but also content posted on-line ‘are forever’ (it’s becoming obvious that personal information posted to social networks is no longer under individual's control and may stay and resist on-line forever).

4. Among such risks those referring to improper use of private information posted by users on social networks have quickly gained a prevailing position.

During their 30th International Conference\textsuperscript{9} the Data Protection Commissioners of the States members to the European Union, while expressly acknowledging the immense potential and the importance of social networks as a communication tool, did also voice their strong concern about subscribers’ interaction “based on self-generated personal profiles, which support an unprecedented level of disclosure of personal information about the individuals concerned (and others)”. The Commissioners therefore addressed both, users of social networks as well as service providers by recommending them some ‘golden rules’ for on-line activities.

Users were therefore invited to:

(i) carefully select which personal data (if any) to be posted on a social network,
(ii) bear in mind other individuals’ expectation to privacy when publishing information about them,

while providers were reminded to:

(i) comply with privacy standards in place, as set by country’s Information Commissioner,
(ii) inform users adequately about use of posted data, possible consequences of their publishing and security risks,
(iii) favour to a maximum extent users’ control on their data and profiles,
(iv) offer users privacy-friendly default settings,
(v) constantly improve systems’ security in order to prevent fraudulent access,
(vi) granting users’ right to access, control and correct their personal data,

\textsuperscript{7} In February 2010 during the Safer Internet Day (an annual event promoted and sponsored by the European Commission) two Italian consumer protection organizations – Adiconsum and Safe The Children – released a study, conducted on 453 subjects between January 21\textsuperscript{st} and 27\textsuperscript{th}, 2010 and performed by using Computer Assisted Web Interviewing. The research revealed that four kids out of hundred aged from 12 to 14 (8 from those aged between 15 and 17) have posted on-line pictures of themselves – partially or entirely – nude or in sexually provocative attitude; the report also shows that it’s a common trend to: upload posts with sexual references (43%), submit personal information to on-line ‘friends’ (43%), watch sexually explicit content (41%), hand over cell phone numbers to someone met on the Internet (40%) and have ‘intimate relations’ with a person found on-line (22%).

\textsuperscript{8} According to a survey released for EU Data Protection Day 2010, almost 50% of human resources professionals active in Europe perform on-line checks on candidates and 25% of all job applications are rejected based on the results of searches performed on candidates’ on-line reputation and profiles, where dismissal is usually grounded on ‘inappropriate comments’ or ‘unsuitable photos or videos’ found on the Internet. Interestingly the same survey shows that on the other side consumers continue to significantly underestimate the risks deriving from their on-line profiles: in the UK only 9% (in France 10% and in Germany 13%) of job seekers held that personal information available about them on the Internet would exercise influence on the outcome of their applications.

\textsuperscript{9} Held in Strasbourg (France) on October 17\textsuperscript{th}, 2008.

\textsuperscript{10} So the ‘Resolution on Privacy Protection in Social Network Services’ issued during the 2008 Conference.
(vii) offer suitable means for deleting personal profiles and information once membership is terminated,
(viii) enable the creation and encourage the use of pseudonyms,
(ix) prevent uncontrolled third party access and practices such as spidering and bulk harvesting,
(x) allow external crawling only on users’ informed, specific and in-advance consent.

These ‘golden rules’ basically reflect concerns and consider the risk indication previously flagged in the so-called ‘Rome Memorandum’ of the International Working Group on Data Protection in Telecommunications.

5. The premises were therefore laid for the European Union’s official bodies dedicating increased attention to social networking.

Early in 2009 EU Information Society Commissioner Vivianne Reding performed significant efforts in encouraging all major social networking sites to draft and adapt self-regulatory practices, meant to crack down on cyber bullying and to improve the safety level for young Net users. Ms. Reding succeeded in convincing eighteen social network service providers\(^\text{12}\) to join\(^\text{13}\) in a pan-European Agreement, the ‘Safer Social Networking Principles for the EU’, through which the adhering parties accept to abide by basic self-regulatory principles. In detail, these guidelines are intended to: (i) raise awareness of safety education messages and acceptable use policies, (ii) ensure that services are age-appropriate for the intended audience, (iii) empower users through tools and technology, (iv) provide easy-to-use mechanisms to report illicit conduct or improper content, (v) promptly respond to notifications of illegal content or conduct, (vi) enable and encourage users to employ a safe approach to personal information and privacy, (vii) assess the means for reviewing illegal or prohibited content/conduct.

More or less at the same time the problem was addressed by the Italian Information Commissioner (Autorità Garante per la protezione dei dati personali). In a keynote speech delivered in Rome during the 2009 European Data Protection Day the Commissioner highlighted the need of achieving a balanced coexistence on virtual platforms between individuals’ expectation to freedom of expression and their right to privacy. He therefore specifically acknowledged the general interest of maintaining the Web ‘open and freely accessible’, but also called for increased sensitiveness towards additional rights of individual Net citizens and felt that efficient protection of ‘on-line rights’ would necessarily imply adequate user consciousness about the many and serious risks present on the Internet.

To the purpose the Commissioner called for:

- adequate educational initiatives aimed at raising the level of awareness about potential misuses of personal data made available on the Internet,
- efficient means of self-regulation, favouring Web users’ ‘responsible behaviour’ and ‘accurate selection’ with respect to personal (in particular, sensitive) data uploaded to the on-line platforms,
- increased involvement of Providers, who were invited to focus on more intensive user information/education and on offering technical means allowing to prevent unconditional access to data by search engines or to restrict – at least partially – profiles’ visibility.

A few months later (in June 2009) the Article 29 Working Party\(^\text{14}\) felt necessary to delve into the

\(^{11}\) The ‘Report and Guidance on Privacy in Social Network Services’ – doc. no. 675.36.5 - prepared and released by the Working Group on March 4\(^\text{th}\), 2008 during the 43rd meeting, 3–4 March 2008, Rome (Italy).

\(^{12}\) Two further signatories were achieved in June 2009.

\(^{13}\) At the Safer Internet Day flagship event, which took place in Luxembourg on February 10, 2009.

\(^{14}\) An independent EU Advisory Body (set up by Directive 95/46/EC) for providing expert opinion from member state level to the EU Commission on questions of data protection, promoting harmonized application of the general principles.
privacy risks involved by social networking and dedicated a specific Opinion to the topic\(^{15}\).

The Working Party’s guidelines:

- offer indications about how and to which extent social networks are affected by the key principles laid down in the Data Protection Directives\(^{16}\) (with a focus also on ‘territoriality’ issues\(^{17}\)),
- provide a set of specific requirements and obligations, which social networks are held to comply with (such as: indications about providers’ identity, information about purposes and ways of data uses, warnings about privacy risks related to data posting, availability of privacy-friendly default settings, copyright and minors’ protection, respect of other data subjects’ rights, handling of abandoned accounts),
- establish users’ rights, equal to those generally granted by the Data Protection Directives (inclusive an easy-to-use complaint handling procedure and user’s possibility of adopting pseudonyms).

A specific section of the WP’s opinion is dedicated to direct marketing\(^{18}\), recognized as “an essential part of the SNS business model”, but also required to “comply with relevant provisions of both Data Protection and ePrivacy Directive”\(^{19}\).

On February 9\(^{20}\) (on the occasion of the Safer Internet Day 2010 in Strasbourg) Vivianne Reding, Commissioner for Information Society and Media, announced that a verification on the effective implementation of the ‘Safer Social Networking Principles for the EU’ (which all major European social network service providers had previously – in 2009 - agreed to comply with) had been performed and presented a summary of a report on the result of such verification.

The report\(^{20}\) was conducted on 25 social networking sites and found that some progress could be acknowledged with respect to the adoption of protecting measures (such as setting options for blocking profile access to other users, content selection and display of on-line status) and of specific policies informing user aged under eighteen about the risks of their on-line activities.

Nevertheless, the overall results could not be considered as satisfying.

---


\(^{17}\) The WP takes the position (see section 3) that “the provisions of the Data Protection Directive apply to SNS providers in most cases, even if their headquarters are located outside of the EEA” and on the point recalls its earlier opinion (no. 1 WP 148 – of April 4, 2008) on search engines “for further guidance on the issues of establishment and use of equipment as determinants for the applicability of the Data Protection Directive and the rules subsequently triggered by the processing of IP addresses and the use of cookies”.


\(^{19}\) “ePrivacy Directive” is Directive no. 58 of 2002 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (the latter to be implemented by the States members to the EU by May 25\(^{th}\), 2011); currently there it’s intensely debated whether the new wording of article 5/3 of the amended Directive no. 58 of 2002 implies a strict in-advance consent requirement for any kind of cookies placed on users’ equipment and therefore results in an imperative obligation for providers to follow a absolute opt-in approach.

\(^{20}\) The findings may be found at the following URL: http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementat_princip/index_en.htm
In fact, half of the sites put under scrutiny had failed in preventing search engines from catching minors’ profiles. Only nine sites had an efficient system in place for collecting users’ complaints and for timely response both, to collected reports as well as to assistance requests. Only fourteen sites had phrased their policies in terms easy to understand for minors and had placed them in a way to allow users immediate and easy access.

During the ‘Safer Internet Day 2010’ an additional initiative - "Think B4 U Post" – was therefore presented by Commissioner Reding and launched with the goal of increasing young people’s awareness about “the risks of sharing personal information online and of encouraging them to control their online identity by thinking carefully about the consequences”.

6. In the light of allowing Conference attendees also a more general idea about the current approaches to the topic at stake – and on a level broader than that of the European Union's official bodies - a short survey was performed during the last week.

The results are summarized in a Chart included in the session's handouts available to the audience and intend to offer an overview on how privacy issues are perceived and addressed in different jurisdictions.

The survey was intended to find out:
- whether the addressed countries had or not privacy provisions, established by Statute Law, specifically concerning social networks,
- whether such area was eventually covered by Self-Regulation,
- which key principles were inspiring these provisions,
- whether upcoming legislation or Self-Regulation guidelines were likely to deal with the topic in the near future,
- whether the national Information Commissioner (or equivalent Data Protection Authority) was paying attention to privacy issues relating to Social Networks,
- whether the Authority's focus was on general issues, sector specific problems or on marketing,
- finally, which key principles and requirements the Authority's guidelines had set with respect to general issues, sector specific problems and marketing.

Credits for the various country contributions are owed – together with my personal thankfulness for contributing – to the members of the Global Advertising Lawyers’ Alliance, who have kindly provided the material exposed in the summarizing Chart.

Without repeating what’s already apparent from the comparative Chart’s content and limiting the analysis to some summarizing comments, from the survey it appears that:

21 This year the 'Safer Internet Day' was celebrated through 500 events in 50 countries worldwide. In Russia all leading Internet providers signed on that day a charter on counteracting child pornography, under which signatory companies undertook to protect Internet users from contacts with child pornography by all legally acceptable means, including banning production and storage of such materials and access lockout. In Italy all interested stakeholders - 19 in total - dealing with Internet and new media, supported the 'Think B4 U Post' initiative and its specific focus on protection of minors; the State Departments both, for Equal Opportunities as well as for Economic Development, the International Telecommunication Union (ITU), the National Information Commissioner, the National Center for fighting child pornography on the Internet at the Postal and Communication Police Unit, the Center for the contrast of pedophilia and child pornography, Save the Children, Adiconsum, Italian Association of Internet Providers (IIIP), Italian Association of video game software’s Editors (AESVI), Telecom Italy, Vodafone, Facebook, MySpace, Netlog, Virgilio, Google/YouTube, Microsoft Windows Live, Skuola.net, TV station La7 were among those adhering to the initiative. Earlier this year – in January – the international press repeatedly reported about a special social network (“Shidonni”) founded in Israel, specifically dedicated to children aged under 12 and counting already 200.000 registered users.

22 For detailed information on the GALA network refer to the following URL: http://www.gala-marketlaw.com.
(a) Except the US almost no other country has in place Statute Law provisions or Self-Regulation guidelines specifically dealing with privacy issues on social networks (a number of countries do have Ethic Codes – usually adopted by providers of Internet related communication services – with a focus on such issues, particularly from a perspective of preventing – or blocking – the presence of illegal conduct or content and undue access by minors).

(b) In most cases, general provisions and requirements in place for processing of personal data will apply to social networks.

(c) In some jurisdictions (inclusive of several non-European ones in North and South American as well as in Asia and Oceania) dedicated rules are in preparation and likely to come into force in a near future.

(d) In a significant number of countries (primarily, but not exclusively, in Europe and North America) Data Protection Authorities have started to scrutinize both, the business models of social networks as well as the practices performed on such platforms, where such attention usually is reserved to general privacy issues (such as: identity theft, on-line frauds, data security) or to sector specific data protection problems (such as: financial transactions, e-commerce, electronic communication, children's protection), but not yet to marketing performed on such platforms (exceptions – with provisions specifically governing commercial communication on social networks – are a number of countries, members to the European Union).

No doubt that in the European Union the effects of the harmonizing efforts performed by various EU Institutions (e.g. the Article 29 Working Party, the European Data Protection Supervisor, ENISA, etc.) together with the provisions laid down in EU Directive no. 136 of 2009 (amending the previous Electronic Communication Directive no. 58 of 2002, etc.) will significantly impact the marketing industry.

Therefore privacy issues will result as the key problem both, for all those participating in activities on social networks (be it or for private or for business purposes) as well as for companies running such platforms.

On February 20th, 2010 the German Data Protection Commissioner was kind enough to inform Facebook about the fact that, since the company recently opened a branch office in Hamburg, it now was subject to German law and jurisdiction and was therefore required to comply with German provisions set for processing of personal data.

Companies will therefore need to assign adequate attention to their practices and policies of data handling. This will happen increasingly more as in most European jurisdictions (and specifically in EU member countries) non-compliance with certain legal requirements established for processing personal information results in a criminal offence.

(as per February 24th, 2010)