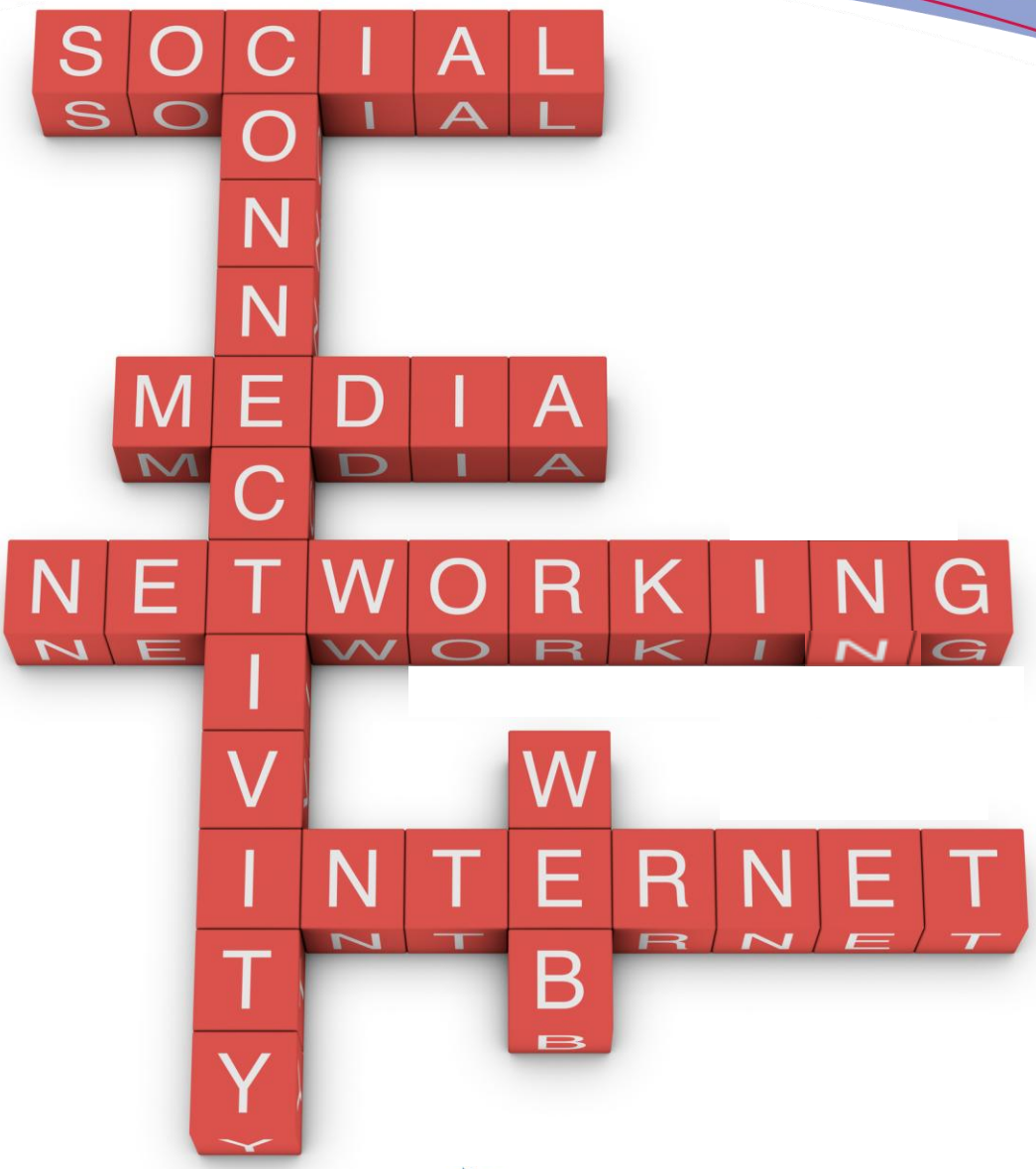


enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU Agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on Member State awareness programmes, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu
Internet: http://www.enisa.europa.eu

Online as soon as it happens

February 2010

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways. ENISA wishes to acknowledge the efforts of the members of the AR Community and their organisations, Ms. Sonia Valerio of AR Enterprise S.r.l., Mr. Diego Vazquez of ISDEFE, Ms. Zeina Zakhour of Atos Origin, Mr. Arjen de Landgraaf of E-Secure–IT, INTECO, Ms. Sissel Thomassen of InfoSecure, Mr. Mathieu Gorge of VigiTrust, Mr. Nicola Fabiano of Studio Legale Fabiano, Mr. Hans Pongratz of Technical University of Munich, Mr. Brian Honan of BH Consulting, Mr. Johannes Wiele of Defense AG, Mr. Corradino Corradi of Vodafone, Ms. Meltini Christodoulaki of Forth-ICS, Ms. Tara Taubman and Mr. Raoul Chiesa of @ Mediaservice.net S.r.l. who provided valuable inputs, material and prompt support for the compilation of the paper.

Finally we would also like to acknowledge and to thank Mr. Edward Kershaw of The Nielsen Company and Ms. Roberta Ruzzi of Vodafone, who contributed to this document with informal reviews, valuable insights, observations, suggestions. The content would be incomplete and incorrect without their help.

Contents

Executive summary

Experiencing online social networking sites (SNSs) has become one of the most popular activities carried out on the Internet. The modern way of staying in touch with business and personal contacts is to be present on social networking sites and to communicate using e-mail and other digital tools. The social networking phenomenon has registered an exceptional growth trend and there has been a widening in terms of users' profiles involved in such activity ([1]), affecting and changing consequently the way people get in contact, meet, communicate and share opinion, information and ideas. This phenomenon is rapidly evolving not only in relation to the audience, changing its demographics, but also in relation to the way the audience itself can experience social networks. Besides traditional computer-based access, users are now able to access social networks through their mobile phones.

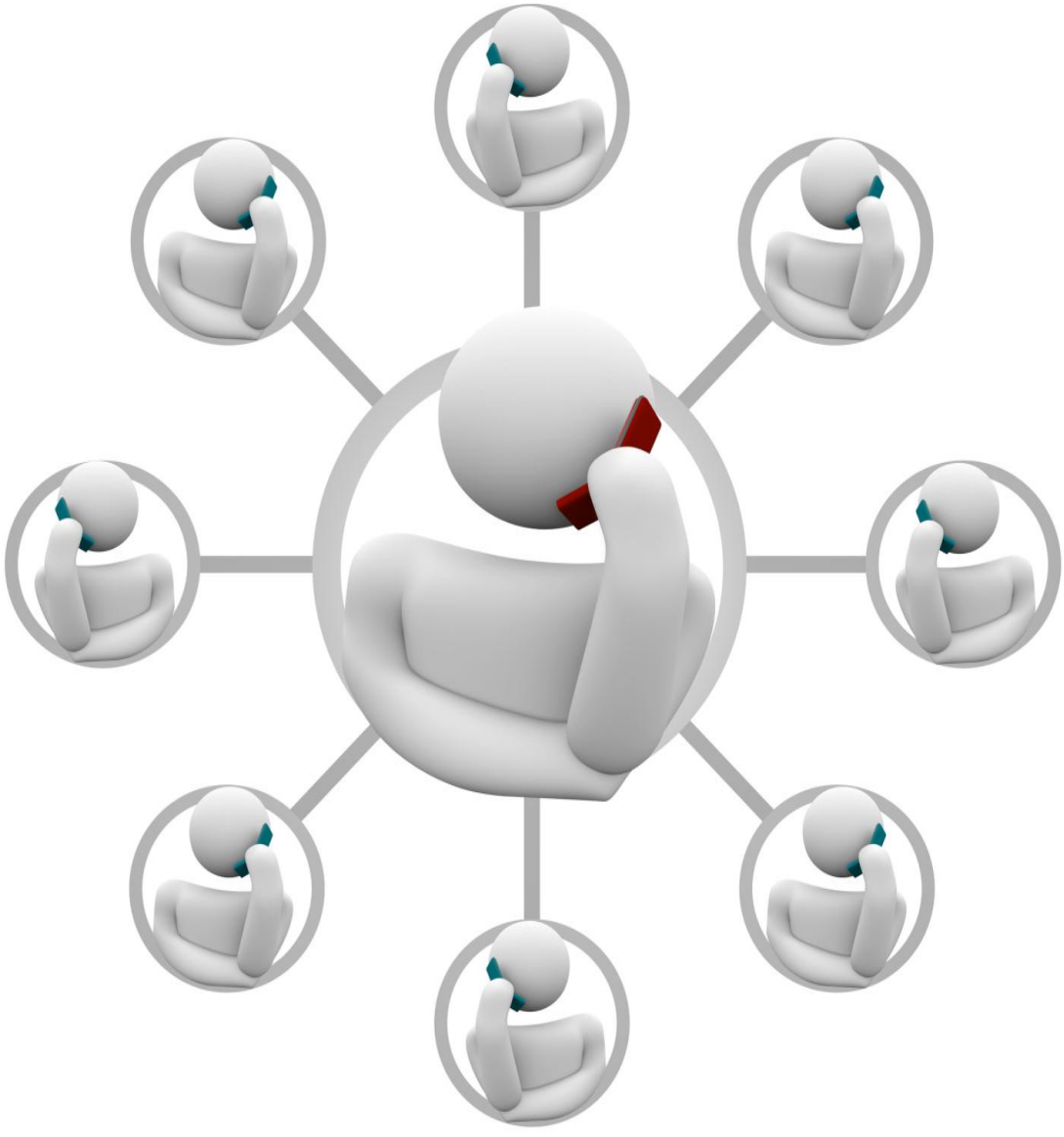
Mobile social network (MSN or social mobile) is a means of communication using a combination of voice and data devices over networks including cellular technology and private and public IP infrastructure ([2]). Subscribers access social networks on their mobile phone by browsing over the mobile internet, through downloaded applications and by text –messaging ([3]). In this paper we will refer and take into particular consideration the 'on deck' services ([4]), coming pre-packaged with the purchase of a mobile phone. Nevertheless the overall data and figures provided in this document include all modes of access to social networking.
Nowadays many mobile users use their phone as a backup device for business and personal data, contacts and pictures also keeping a record of their personal details and access codes. As a consequence, a lost or stolen mobile phone can cause serious damage considering that all information and data, about the user and the contacts, entrusted on SNSs and linked to the mobile phone could be used in an illegitimate way. Case studies from different European countries show that a considerable number of users are unaware of their exposure to security risks and privacy issues. While many of the privacy issues originating from the web-based access to SNSs also apply to MSNs, there are also a number of unique risks and threats against MSNs.

ENISA believes that users' awareness is the first line of defence regarding their privacy and security of their data. This white paper aims to provide a set of recommendations for raising the awareness of SNSs users and in particular of social mobile users of the risks and the possible consequences related to their improper use.

This document does not cover the access of SNSs through mobile phone by minors ([5]) and consequently any matters related to this aspect. Finally, it should not be seen as either a comprehensive source of all risks associated to the usage of social networks or as a technical guideline or specification to secure standards or solutions.

([1]) This shift has primarily been driven by Facebook, which started as a service for university students; now almost one third of its global audience is aged 35–49 years and almost one quarter is over 50 years old. Source: The Nielsen Company, *Global faces and networked places*, March 2009, available at http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/ (last visited on 5 October 2009).
([2]) Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (last visited on 18 November 2009).
([3]) Users can register a phone that allows them to send text message post directly to their user profile.
([4]) 'On deck' refers to applications that operate through a partnership between social network companies and wireless phone carriers whereby programs and application are distributed via the wireless carrier.
([5]) Nevertheless the data provided for the description of the social networking scenario in Europe include the access of social networks also by users aged 15 and older.

PART 1- SOCIAL NETWORKING GOES MOBILE



Introduction

According to recent statistics there are more than 65 million active users currently accessing Facebook through their mobile devices and the ones that do so are almost 50% more active than non-mobile users ([6]).

Today mobile devices are not only used for voice communication or simple peer-to-peer connections between people who know each other, but also for data connection to the Internet. Moreover, with their sophisticated and user friendly features, mobile devices are not only consuming content but are also capable of producing and storing content. The rapid development of information and communication technologies, especially the Internet and the mobile phone, has transformed the way people interact with each other and connect with the environment around them. Over the last few years, a plethora of new applications have sprung up, enabling a whole new dimension of social interaction. Portability, high capacity memories and 'always on' technology are pushing the use of mobile devices for an increasing number of services in the everyday life and are bringing the networking environment definitely closer to users. The MSN services that come pre-packaged with the purchase of a mobile phone, to which we refer in this paper, support social networks through their ubiquitous usability and easy sharing of location, information and experiences and allow access to SNSs anytime and anywhere with just a click ([7]).

Users need guidance and education on how simple lack of attention or voluntary misconduct when accessing and using social networks through a mobile phone can have unexpected consequences which can be avoided by following some good practices that each user should be aware of. Several stories highlight that many users are unaware of the risks and threats related to the misuse of the information they entrust to an SNS and of the proper way to protect their privacy ([8]). Severe reputational and personal damage can be caused not only by the users themselves but also by other users and third parties, using the social networking tools in an improper way. For example, in the UK, a teacher has been suspended for complaining on Facebook about her class ([9]) and in Italy, the forgery of a Professor's identity has been discovered on Facebook, while friends and colleagues of the victim were chatting and sharing information with someone that was not who he claimed to be ([10]).

ENISA believes that increasing awareness of the risks and the possible consequences related to social networks' improper use is the first line of defence. This paper is designed to provide comprehensive information about the MSN services and the risks and threats connected to their use. It will also analyse the social networking world under the lens of the European directive on data protection.

([6]) Facebook press room, statistics available at http://www.facebook.com/press/info.php?statistics (last visited on 5 October 2009).

([7])This paper does not include the description of the 'off deck' services referring to those applications that do not come pre-packaged with the purchase of a mobile phone but have to be downloaded from the Internet or from a wireless provider after the time of purchase.

([8]) According to a recent survey conducted by AVG and CMO Council 'less than one third of social networkers are taking actions to protect themselves online', *Bringing social security to the online community,* 26 August 2009, available at www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf (last visited on 19 November 2009).

([9]) MailOnline, *Teacher is suspended for jibe on Facebook about her class*, 1 August 2009, available at http://www.dailymail.co.uk/news/article-1202210/Teacher-suspended-jibe-Facebook-class.html (last visited on 26 November 20009).

([10]) LaStampa.it, *Facebook, rubata l'identita' a un Professore di Trento*, 5 January 2009, available at http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5580&ID_sezione=38&sezione=News (last visited on 26 November 2009).

Social network: a definition

A social network is an online community that allows people, through a built-up profile, to meet, communicate, keep in touch, share pictures and videos with other community members with whom a connection is shared.

The social network's structure includes having a profile (which contains personal information about the user), friends (trusted community members that can post comments on the user's profile and send private messages) and groups (people with the same interests meet online and discuss a variety of topics). Some social networks also allow users to personalise their profile using widgets or to create their own blog entries.

From a functional point of view ([11]), social networks can be classified in two main categories: 'general purpose' and 'niche' social networks. 'General purpose' social networks have as a primary scope communication and interaction among users and anybody is free to join the online community since they do not cater to any specific theme or interest but they gather a variety of interests. Among others, Facebook, Myspace, Badoo and Netlog belong to this category. On the other side, 'niche' social networks allow users to perform a specific activity ([12]). Business-oriented social networks such as LinkedIn or reunion sites such as Classmates.com are in fact sites focused on a specific interest such as professional contacts or the search for old school friends.

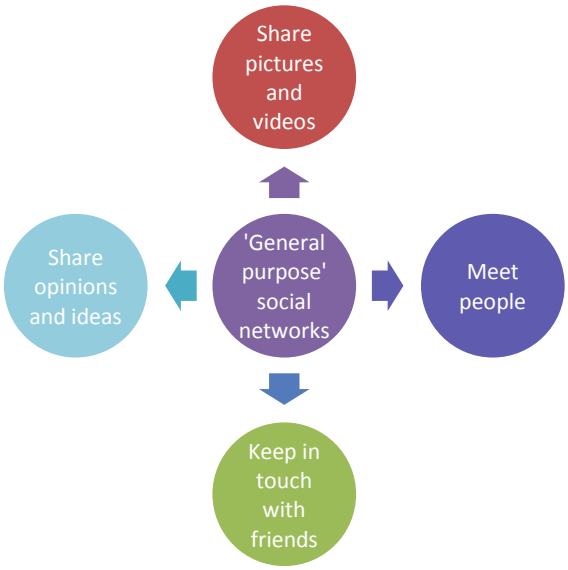


Figure 1: Different types of interests spread out from 'general purpose' social networks.

([11]) For a deeper analysis see Alexander Richter, Michael Koch, *Functions of social networking services,* in: Proceedings of the 8th International Conference on the Design of Cooperative Systems, Carry-le-rouet, France, Institut d'Etudes Politiques d'Aix-en-Provence, 2008, available at http://www.kooperationssysteme.de/docs/pubs/RichterKoch2008-coop-sns.pdf (last visited on 5 November 2009).

([12]) Joseph Bonneau, Sören Preibusch, *The privacy jungle: On the market for data protection in social networks*, Eighth Workshop on the Economics of Information Security (WEIS 2009), 24–25 June 2009, available at http://weis09.infosecon.net/files/156/index.html (last visited on 5 November 2009).

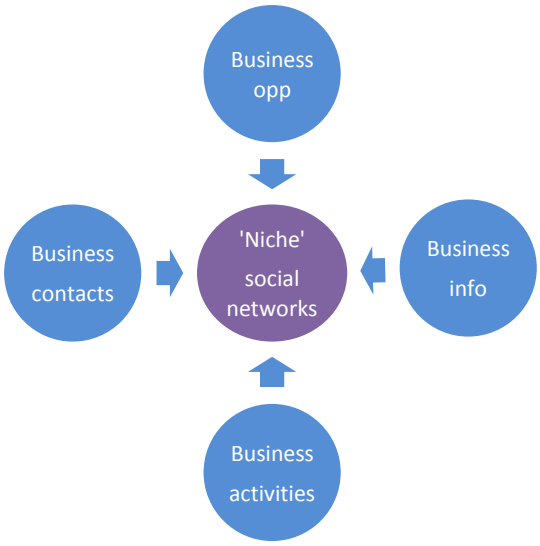


Figure 2: A 'niche' social network such as LinkedIn attracts the same sort of interest (i.e. professional/business).

Mobile social network: a definition

A first generation of social networking on mobile networks began in 1999/2000 as chat services launched in some European and non European countries ([13]). The phenomenon spread rapidly and evolved through the years to the current environment and services offered. According to Facebook ([14]), there are more than 180 mobile operators in 60 countries working to deploy and promote Facebook mobile products.

Mobile social networking is a means of communication using a combination of voice and data devices over networks including cellular technology and private and public IP infrastructure ([15]). Generally speaking MSNs can be divided into two categories: 'on deck' and 'off deck'. 'On deck' refers to services that operate through a partnership between social network companies and wireless phone carriers. This category of services programs and applications which enable the social networking experience are distributed via the wireless carrier and are pre-packaged with the purchase of a mobile phone. 'Off deck' refers instead to services whose applications do not come pre-packaged and the user has to download the application from the Internet or from a wireless provider after the time of purchase.

Many SNSs, like MySpace and Facebook, offer phone versions of their services, allowing users to interact with their friends. This enables the users to experience the social networks on their handset

([13]) For a complete description of the history of mobile social networking see Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (last visited on 18 November 2009).
([14]) Facebook press room, statistics available at http://www.facebook.com/press/info.php?statistics (last visited on 5 October 2009).
([15]) Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (last visited on 18 November 2009).

and to gain advantages from getting immediate alerts and notification of changes in their communities (immediacy), to personalize and reflect personal preferences and conditions (intimacy) and to spot the presence of others in the local area (discovery of others in proximity) ([16]).

A European overview

Social networking reach in European countries

Of the around 283 million European users, 211 million of them, aged 15 and older who accessed Internet via a home or work computer, visited a social networking site. The largest public is represented by the UK with 29 million visitors, reaching 80% of the country's total Internet audience ([17]). Among all social networking sites, Facebook has gained a top position throughout the majority of European countries. A research conducted by comScore ([18]) stated that, of the 17 European countries included in the study, Facebook played a leading role in the social networking category in 11 of them in terms of unique visitors. The site's largest audience is in the UK with about 23 million visitors followed by France with about 14 million visitors. The only countries in which Facebook does not hold the No 1 or No 2 position are Germany (No 4), Portugal (No 3) and Russia (No 7).

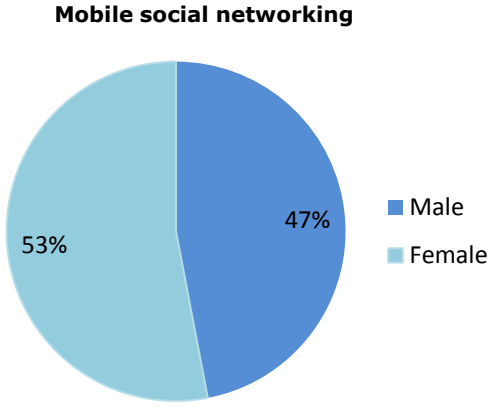


Figure 3: Mobile social networking
UK, Q4 2009, *Source:* The Nielsen Company.

Mobile social networking reach in European countries

The growing popularity of social networks has determined an increasing demand to access them via mobile phone. The mobile social networking scenario described by the data and figures below include all kind of access to social networking (such as mobile internet, apps). Social networking attracts three quarters of European Internet users and, in the UK, it is one of the few mobile Internet activities more popular with females than males (Figure 3) in respect of general mobile internet browsing (Figure 4).

([16]) Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (last visited on 18 November 2009).
([17]) comScore press release, 17 February 2009, available at http://www.mediametrix.com/Press_Events/Press_Releases/2009/2/Social_Networking_France (last visited on 5 November 2009).
([18]) comScore press release, 15 April 2009, available at http://www.comscore.com/layout/set/popup/Press_Events/Press_Releases/2009/4/Facebook_Top_Social_Network_in_Spain (last visited on 5 November 2009).

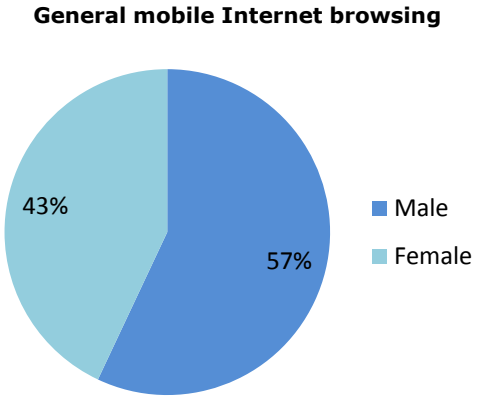


Figure 4: General mobile Internet browsing
UK, Q4 2009, *Source:* The Nielsen Company.

In the UK, in the fourth quarter of 2008, 2 million people visited a social network through their handset, corresponding to an increase in 2008 of 249% ([19]). The number of social mobile users grew rapidly. In the fourth quarter of 2009 figures for the UK show that 3.9 million people accessed a social network through their handset with an increase of almost 200% on Q4, 2008 ([20]).

The most popular social networking sites accessed via personal computer are also the leading ones being used over mobile phones. Facebook represents the vast majority of social networking's active reach on mobile phones and it has been the most visited site in at least four European countries: the UK, Italy, Spain and France ([21]).

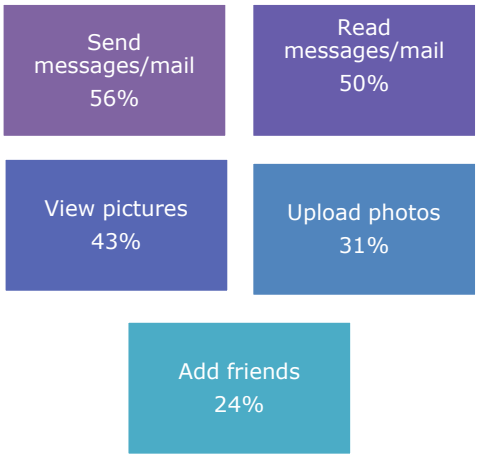


Figure 5 shows the top five social networking activities conducted on a mobile phone at a pan- European level ([22]). Other activities are also carried out on a mobile phone, such as: receive text alert (23%), view profiles (15%), create or update profile (13%), upload videos (10%), participate in chat rooms (8%) and post blogs (7%).

Figure 5: Top five mobile social networking activities
Source: The Nielsen Company.

([19]) The Nielsen Company, *Global faces and networked places*, March 2009, available at http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/ (last visited on 5 November 2009).
([20]) ENISA has been provided with this data by The Nielsen Company.
([21]) ENISA has been provided with this data by The Nielsen Company. It refers to Q2, 2009 and to Q1, 2009 (France).
([22]) The Nielsen Company, *Mobile media nei mercati emergenti e in Italia*, IAB Seminar, 16 July 2008, available at http://www.iabseminar.it/video.aspx?IDSessione=12 (last visited on 5 November 2009).

A marketing channel

Social networks are communication channels with features largely comparable to newspaper, radio and television. Companies with a product or service should consider it as another vehicle to target the audience and to communicate with consumers ([23]).

Social networks provide significant competition for publishers in terms of consumer attention but also give them the opportunity to create a tailored content, reflecting the public's desires and tastes and to optimize campaign reach. The time spent on social networks, by chatting with friends, posting content and so on, increase the size and value of the network, making the social network more attractive as an engaging advertising medium ([24]). Mobile advertising provides the opportunity for operators to earn revenues from greater data usage as users click through to, and browse, advertiser sites, or else respond to advertisement by SMS ([25]). In this regard, mobile social networks will play a leading role in term of revenues ([26]).

The exploitation and monetization of social networks include the following economical variables:

- ✓ Advertising (based on users' preferences and main source of income).
- ✓ Premium (in order to obtain a more advanced profile or use more applications users need to subscribe to options, subject to charges).
- ✓ Donations (users make donations for the maintenance of the platform).
- ✓ Payment for use (users need to pay for the access and usage of certain tools) ([27]).

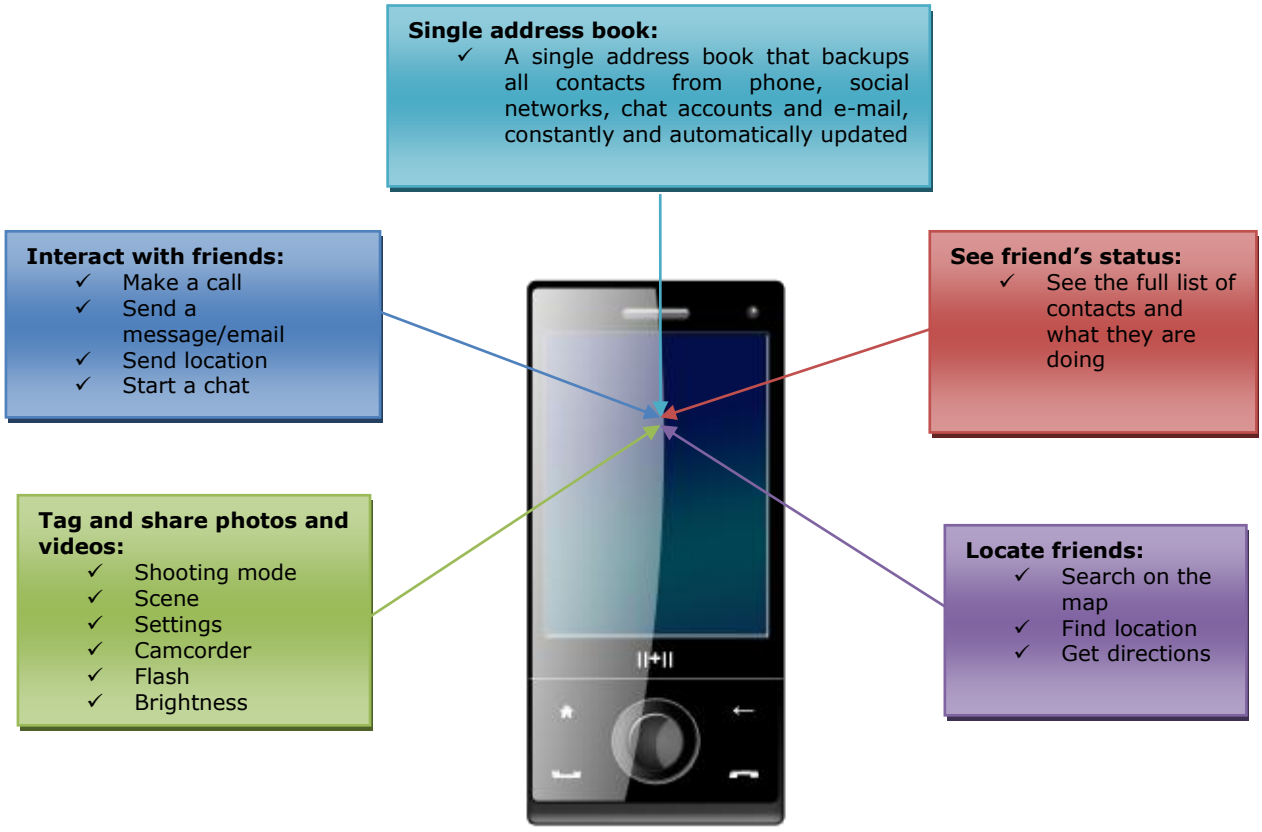
([23]) The Nielsen Company, *Global faces and networked places*, March 2009, available at http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/ (last visited on 5 November 2009).
([24]) Mashable, The social media guide, *Exploring best practices for building and monetizing mobile social networks,* 3 October 2008, available at http://mashable.com/2008/10/03/mobile-social-networking/ (last visited on 30 November 2009).
([25]) Juniper Research, *Mobile advertising, because I'm worth it*, extract from Mobile advertising delivery channels, strategies & forecasts 2008-2013, 2008, available at http://www.c2mweb.eu//files/Whitepaper_Mobile_Advertising.pdf (last visited on 30 November 2009).
([26]) *Advertising to Fuel Mobile Social Networking Growth as User Generated Content Revenues Reach $7.3bn by 2013*, available at http://arabcrunch.com/2008/09/advertising-to-fuel-mobile-social-networking-growth-as-user-generated-content-revenues-reach-73bn-by-2013.html (last visited on 25 January 2010).
([27]) INTECO, *Study on the privacy of personal data and on the security of information in social networks*, February 2009, available at http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en (last visited on 24 November 2009).

PART 2- THE SOCIAL MOBILE EXPERIENCE

Main features

The world of social networking and the new ways of communicating are no longer confined to the user's desk. The online social network experience has been extended into everyday life without the need for a PC screen thanks to the integration between mobile phones and social networks. The launch of this technology has brought the networking environment closer to the user, empowering and enhancing opportunities for interaction and communication. MSNs offer almost the same services of web-based social networks but which a much greater interaction with everyday life. 'Online as soon as it happens' better summarizes and describes the social mobile experience, allowing users to test a new kind of interaction and communication where every moment and thought can appear online as soon as soon it is experienced.

In particular, the MSN's services coming pre-packaged with the purchase of a mobile phone offer the chance to combine web-based and phone–based information in order to gather in one place all user contacts, communities, entertainment and personal favourites. One of the results of this interaction is the '*social phonebook*' which provides one place to store contacts available on a SNS and the ones already stored in a mobile phone, keeping them constantly synchronized. The user can rotate through all of the contacts displayed in the mobile's screen, pick up a friend and choose how to communicate, either by message, chat or e-mail. After synchronizing the social networks contacts and the chat accounts, users can see what their friends are doing in that very specific moment and where they are thanks to the map function that can locate them in real time. The quick and easy way to communicate can be found in another new feature provided by MSNs which is the possibility to take a picture, to save it and tag it on the mobile phone and share it online, as soon as it happens, with friends and peers.



Why social mobile?

It has been estimated that in 2011 the number of mobile social network users worldwide will be 554 million, corresponding to 13.3% of mobile phone subscribers, with a growing trend for 2012: 803 million users, corresponding to 18.8% of mobile phone subscribers ([28]). In Europe, in 2012, the number of users will be 134 million meaning that one out of five mobile phone subscribers will use the mobile device to access a social network ([29]).

The increasing demand to access social networks on the move is a natural consequence for social networks, as consumers are used to communicating with friends via mobile calls and text. Using a mobile phone to access social networks does not require much of a change in consumer habits ([30]). On the contrary, it lets the user explore new ways of communicating. Since a mobile phone is always with the user, it is possible to be constantly in touch with friends and peers and communicate what they are up to and where they are, anytime and anywhere, without the limitation of traditional web-based access. It is no longer, in fact, only a question of what the user is doing but also where he is located, since the new map function provided by mobile phones allows users to find and locate their friends and also to get directions. The quick and easy access to social networks can also be considered as a pre-eminent reason for this phenomenon. It is now possible to enter the user's personal profile with just a click and to upload a picture as soon as it has been taken with a mobile phone.

In this regard, it should be noted that the information posted and published, such as pictures, videos and comments, via the mobile phone services are the user's responsibility. This means that the user needs to take care of all the content he publishes about himself or his friends in order to protect his own and other people's privacy, personal and professional life.

([28]) eMarketer, April 2008, available at http://www.emarketer.com/Report.aspx?code=emarketer_2000489 (last visited on 2 November 2009).
([29]) Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at *http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf* (last visited on 2 November 2009), The daily bit, *Un fenomeno chiamato mobile social networking*, September 2008, available at http://www.thedailybit.net/index.php?method=section&action=zoom&id=2489 (last visited on 18 November 2009) and Lastampa.it, *In Europa il social network piace sul cellulare*, August 2008, available at http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5054&ID_sezione=38&sezione=News (last visited on 18 November 2009).
([30]) The Nielsen Company, *Global faces and networked places*, March 2009, available at http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/ (last visited on 5 October 2009).

PART 3- PRIVACY AND SECURITY ISSUES

Privacy issues

Every SNS user should be aware of the risks and threats related to the use of social networks. Besides the services and opportunities offered, social networks are not exempt from risks affecting users' privacy, personal and professional life. In this regard, it should be noted that general social networks are exposed to a higher level of risk than, for example, professional social networks since users, in general social networks, not only publish information related to their work experience or their studies but also information and data related to their tastes, ideology or experiences, thus making available much more information about themselves than in professional social networks ([31]). Privacy issues can arise from three different types of attackers ([32]):

- ✓ third parties.
- ✓ other users.
- ✓ platform providers.

Third parties

Third parties may gain fraudulent access to personal data published on a user profile or by stealing or finding a lost mobile. Information and data collected in such a manner can cause severe privacy issues. Access by a third party can also occur without violating any technical rules and is due basically to the privacy profile level which is not set properly by the user (who hasn't paid enough attention to the privacy settings). On some sites, users that change their default settings from private to public receive a security message about the risks they could face by making their profile public ([33]).

Other users

Other users also have the same potential as third parties to cause privacy issues. It is possible in fact to leave comments on the personal profile of other community members or to tag a picture portraying the user without his consent in an awkward situation. Many privacy issues can be traced back to the out-of–context use of personal data, with a greater impact when this involves trusted contacts who normally have legitimate access to a high level of information ([34]). This is why it is also important to agree with friends and peers on the rules to be followed when using and accessing social networks in order to ensure secure personal data processing.

([31]) INTECO, *Study on the privacy of personal data and on the security of information in social networks,* February 2009, available at http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en (last visited on 24 November 2009).
([32]) Martin Pekárek, Stefanie Pötzsch, *A comparison of privacy issues in collaborative workspaces and social networks*, published online 28 July 2009, available at http://www.springerlink.com/content/g54qk93430581554/?p=dae26d8123004ccf88e5004aa1aba269&pi=0 (last visited on 5 November 2009); Martin Pekárek, Ronald Leenes, *Privacy and Social Network Sites: Follow the Money!* January 15-16, 2009, available at www.w3.org/2008/09/msnws/papers/tilt.pdf (last visited on 24 November 2009).
([33]) *Privacy setting for social networks*, available at http://blog.safetyclicks.com/2008/09/03/social-networks-and-privacy-settings/ (last visited on 5 November 2009).
([34]) Martin Pekárek, Stepanie Pötzsch, *A comparison of privacy issues in collaborative workspaces and social networks,* published online 28 July 2009, available at http://www.springerlink.com/content/g54qk93430581554/?p=dae26d8123004ccf88e5004aa1aba269&pi=0 (last visited on 5 November 2009).

Platform providers

The user can regulate, through the privacy settings, who has access to the information that decides to provide. Nevertheless, in some cases, the platform provider has full access to user data, collecting for example the user's IP address and browser type and the information provided is available in search results across the network and to third-party search engines.

Major risks and threats related to MSNs

Social networks have drastically modified the traditional use of the Internet, turning it into an increasingly communicative medium and attracting millions of users that access SNSs through a PC screen or a mobile phone. The growing popularity of the social mobile phenomenon creates significant opportunities for business and personal purposes but also exposes its users to security risks and threats.

Identity theft

Identity theft in mobile social networks is one of the most important threats as its consequences may affect the reputation and privacy of the user. Identity theft can be easily carried out by a malicious attacker in a mobile environment because it can be performed by stealing, permanently or temporarily, security credentials (i.e. 'Man in the Middle' attack), or by stealing the device ([35]). Once the attacker takes control of the phone or has intercepted user credentials, he will be able to take full control of the user's account by publishing comments in the name of the legitimate user, by changing the current password and e-mail address to permanently take control of the account or by using the compromised account to spread malicious software — or 'malware' — through social engineering. The 'forgery' of a user's identity can have a very serious impact on his personal life and reputation at work.

Italy – Professor's fake profile on Facebook

A fake profile of a University professor in Turin was created on Facebook. The professor wanted to create his own Facebook page but he found out that someone else had already registered him, creating a profile with very offensive features, affecting his reputation. The episode was immediately reported to the public prosecutor in Turin for the necessary investigation and measures to be taken.

Spain – Multiple identity theft aimed at celebrities

During 2009 there have been multiple identity theft cases in Spain, aimed at celebrities and well-known people. A Spanish writer and a politician found out that fake profiles of them were circulating on a social network, with comments and opinions published in their names, affecting their reputation and privacy.

([35]) ENISA, *Security issues in the context of authentication using mobile devices (Mobile eID),* 2008, available at http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security issues mobile devices.

Malware

As social networking sites allow their users to interconnect, they constitute an ideal platform for the distribution of malware. Although there is not yet any known mobile malware propagation through mobile social networks, this kind of social network can send especially crafted malware directly to mobile phones, using also Bluetooth and Wifi features in mobile phones to propagate. Malware could steal information stored in the mobile social network, or infect the mobile phone itself in order to access the information stored; it could even use the device as a proxy to propagate the malware infection through SMS to the phone's contacts and through the Internet connection to the contacts in the mobile social network. Twitter, Facebook, Myspace and other social networking platforms have been used to distribute malware. The widespread takes place when a link to a website, rigged with malicious software, is posted by an infected computer on a social networking site. Users click on the link, trusting the friends who posted the links, not knowing that their friends have been hacked ([36]). One of the methods encouraging social networking users to click on infected links is the technique of sending out spoofed e-mail. Hackers create an e-mail message, appearing to be sent from a social networking site inducing the user to update the personal account or open an attachment containing the new password ([37]).

Corporate data leakage and reputation risk

Users discuss and share their experiences, including work ones, on social networking sites. In addition, users have been linking their numerous accounts available on different social networking sites, thus syndicating and federating the posts among the linked profiles. This interconnection especially between professional and personal social networking sites distributes data cross-boundaries and makes it extremely difficult to contain and remove indiscretions. Consequently, users posting professional information on their business profile could have these posts distributed to their Facebook or Twitter accounts leading to the accidental disclosure of corporate sensitive data.

UK- Data leakage for airlines companies

In 2008, Virgin Atlantic airlines investigated allegations that its staff posted rude comments on Facebook criticised the cleanliness of the company's fleet and of its passengers. The 13 members of the Virgin Atlantic staff have been dismissed for their behaviour. Later, a similar episode involved the British airlines check-in staff based in Gatwick who posted on Facebook messaging saying that travellers are 'smelly' and that operation's at Heathrow's Terminal 5 are 'shambolic'. An investigation was launched after the episode.

Mobile social network services can contribute, intentionally or unintentionally, to the information leakage. The real-time spread through social mobile of corporate data can cause serious damage to organisations. Users can also be affected by this threat as a result of unauthorised posts or photographs in real time which can affect their privacy and reputation at work.

([36]) InfoWorld, *Hackers put social networks such as Twitter in crosshairs,* 17 August 2009, available at http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-crosshairs-832?source=IFWNLE_nlt_sec_2009-08-17 (last visited on 19 November 2009).

([37]) Due to the newer techniques used by hackers, identifying malicious links has become harder. One of newer methods consists of hijacking Twitter's trending topics by creating Twitter new accounts and posting messages related to the most trending topic discussed on Twitter at that time. This would allow the post to be aggregated in Twitter search results where unsuspecting users would click on the included link. The text accompanying the link would be intriguing to those interested in the subject, tempting them to click through.

Italy – Critics of her company on Facebook: fired

An Italian woman working for a company based in Milan was fired because of comments posted on her Facebook profile about the company. The employee created a group online, aiming to gather all her colleagues in other cities working for the same company, in order to complain about being an employee at the company.

France – Video spreading on Facebook: breach of investigation secrecy

The leak of a night bus video surveillance tape, revealing the violent assault of a passenger, provoked outrage in France in mid-April 2009. The footage was posted by a French policeman on his Facebook profile and showed a violent attack inside a Parisian night bus where a passenger was robbed and brutally assaulted by a gang. It would have been just another urban violent robbery had the policeman not posted the footage on his Facebook profile. In fact, once the video was available online, it spread all over the Internet on various social networking sites and raised uproar in the country. The posting of the video was considered a direct violation of the victims' rights as they were clearly identifiable in the footage. The repercussions of this leak led the main victim to file a lawsuit denouncing a breach of investigation secrecy. Ironically the policeman was bewildered by the video spreading like wildfire as he believed it was only destined for his friends to see. He immediately deleted the video and his Facebook account hoping to contain the incident but it had already circulated on all possible networks.

Stolen or lost mobile phone

A lost or stolen mobile phone can cause serious damage. Nowadays the mobile phone has become a database, with all kind of information kept in it, and used as a backup device for important data, access codes, contacts, pictures and with the record of users' personal and corporate details. Many mobile users use their mobile phone for corporate e-mail with copies of them held on the phone. If the mobile phone gets lost or stolen, it is necessary to change the passwords of the SNSs, e-mail and any other sites that have been linked to the mobile in order to protect the user's personal information and the privacy of friends, company and clients whose contacts on the SNS have been synchronized with the mobile phone.

User's position tracking

Mobile service providers and some mobile phones are equipped with the necessary technology to track the devices, which implies that the users themselves are being tracked. Companies are launching new applications and widgets which implement this capability into mobile social networks. The map function gives users the chance to see, in real time, where their friends are located and to choose who can see where they are. The related threat is the possibility of knowing the geographical position of the user and to perform an attack directly aimed at his account or through the accounts of his contacts. Once this information is available, malicious activities such as blackmail, hijacking etc. could be carried out, affecting the user's personal security.

Data misuse

The access to personal information gained either through a lost, stolen or hacked mobile phone, or just because too many details have been provided on a SNS's profile can head to the possible misuse of such personal data, jeopardizing personal and professional life. The spreading of incorrect and private information becomes a relevant issue especially when it affects not only private life but also the working environment.

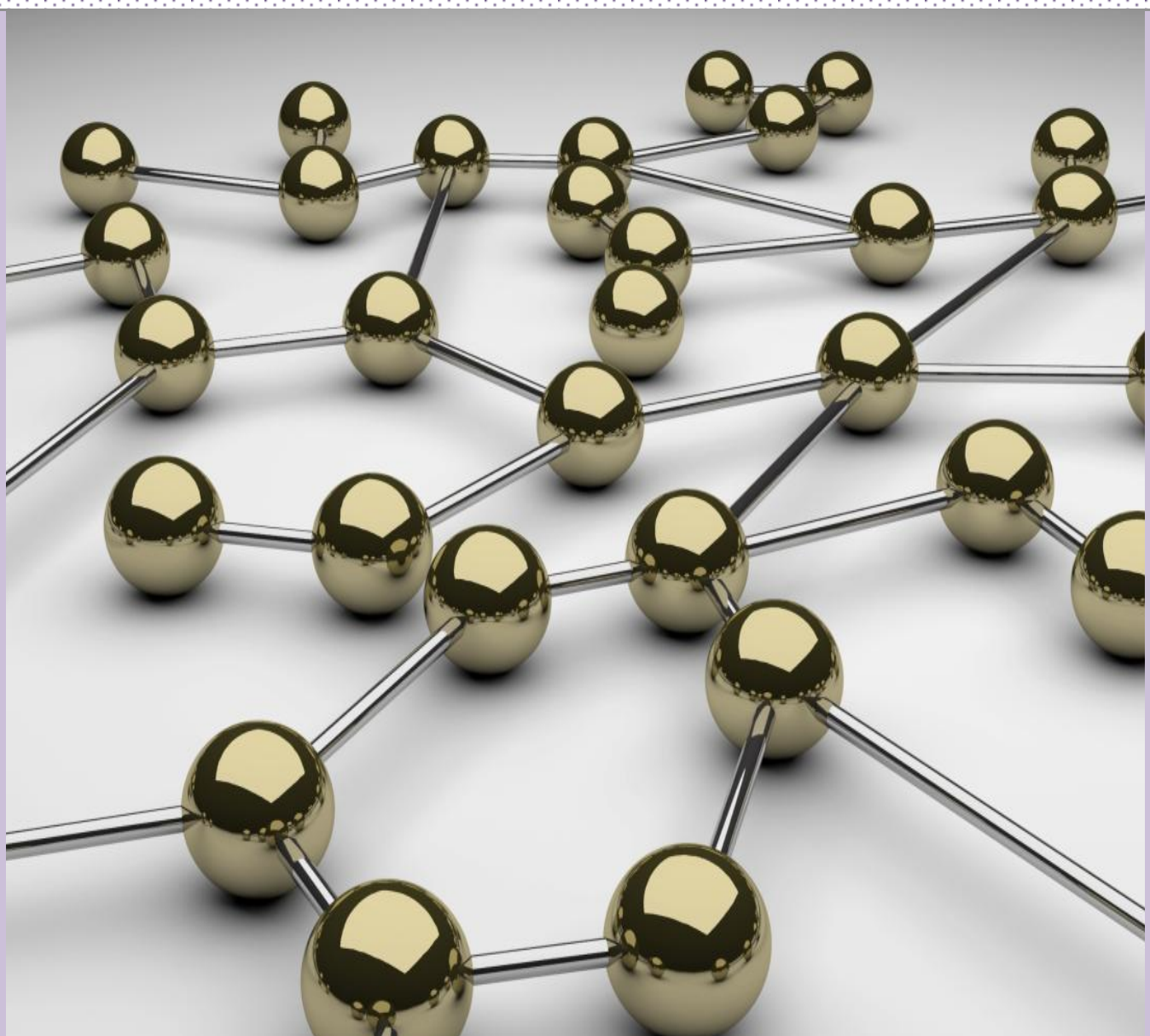
Greece- Fake profile with nude pictures posted by the ex-boyfriend on Facebook

In October of 2009, the Greek Hotline which receives reports for illegal Internet content (SafeLine) received a report from a woman who claimed that after she broke up with her boyfriend, he created a fake profile of her on Facebook, posting pictures of her naked. The woman immediately realised that the only person who could have access to those pictures was her ex-boyfriend and so she reported him. Following the report, the specific account has been removed.

UK – Payout for data misuse on Facebook

In the UK a businessman sued an old school friend for creating a fake Facebook profile of him. The plaintiff claimed that the set up profile contained personal information 'for all to see' including false information about his sexual orientation and political views. The victim sought damages for libel and misuse of private information and won the case at the High Court which condemned the defendant to pay the damages.

PART 4- EUROPEAN DIRECTIVE ON DATA PROTECTION



What is the right to privacy and how is it protected by European legislation?

The right to privacy is a negative right of not interfering in someone's private and family life ([38]). On the other hand, data protection is a positive concept that implies that everyone has the right to the protection of personal data concerning themselves and that such data must be processed fairly, with a purpose limitation and with the consent of the person concerned or on a lawful basis ([39]). The existing data protection framework is constituted by:

- ✓ Directive 95/46/EC on data protection ([40]) ('DPD' or 'directive').
- ✓ Directive 2002/58/EC on e-privacy ([41]).
- ✓ RFID recommendation ([42]).

Italy – Social network: watch out for side effects

In May 2009, a nurse, working at a hospital in Udine, published on her Facebook profile almost 50 pictures taken inside the intensive care unit. In some of the photos, patients receiving medical treatment were visible. The Italian Data Protection Authority (DPA) decided to open a preliminary investigation in order to ascertain a possible breach of the right to privacy. Earlier the same year, another case took place at a hospital in Turin, where a nurse published on her Facebook profile a picture of an unconscious, drunk patient after adding some offensive comments. The nurse was suspended for ten days. Since these two alarming cases, highlighting the lack of users' awareness when accessing SNSs, the Italian DPA has released a short guide to '*help those planning to sign up to a social network and those who have already joined a social network to use this new tool knowledgeably*'.

The scope of the DPD is to apply to the processing, wholly or partly, by automated and non-automated means, of personal data which form part of a filing system or are addressed to be part of it ([43]). Member States, in line with the DPD, shall consequently protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy in relation to the processing of personal data ([44]). The e-privacy directive specifies and complements the DPD ([45]) in order to ensure a harmonisation of the Member States' provisions thereby ascertaining an equal level of protection of fundamental rights and freedoms.

([38]) See Article 7, Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.
([39]) See Article 8, Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.
([40]) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.
([41]) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002. The Council of the European Union adopted, on 26 October 2009, a directive amending, amongst others, the e-privacy directive. The amendments include an obligation for Internet service providers to notify data breaches to the competent national regulator. The directive needs to be signed by the presidents of the Council and the European Parliament and will enter into force the day following publication in the *Official Journal of the European Union* (OJ).
([42]) Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, OJ L 122, 16.5.2009.
([43]) See Article 3, DPD.
([44]) See Article 1, DPD. The status of implementation of the DPD in each Member State is available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited on 20 October 2009).
([45]) See Article 1, 2 para., e-privacy directive.

The RFID recommendation provides guidance on measures to be adopted for the deployment of RFID ([46]) applications to ensure the respect of national legislation implementing the DPD and the directive on e-privacy ([47]). The DPD and e-privacy directive are wholly applicable to the RFID applications that process personal data ([48]).

Directive 95/46/EC on data protection

A general overview

The DPD provides a definition of personal data as any information related to a data subject (as an identified or identifiable natural person) and referring to physical, economic, cultural or mental factors. Any operation performed upon personal data, such as collection, storage or disclosure is a processing of personal data, the purpose and means of which are determined by the data controller that according to the law can be any natural or legal person, public authority, agency or any other body ([49]).

Member States shall provide that personal data must be:

- ✓ Processed fairly and lawfully.
- ✓ Collected for specified, explicit and legitimate purposes and used accordingly.
- ✓ Appropriate and relevant in relation to the purpose for which they are processed.
- ✓ Accurate and kept up to date.
- ✓ Kept no longer then the time necessary for the purpose for which they are processed ([50]).

Personal data can be processed if:

- ✓ The data subject has been adequately informed and has given unambiguously his consent for the collection and further use of his data.
- ✓ Processing is necessary to perform a contract having as a party the data subject or to enter into a contract requested by the data subject.
- ✓ A legal obligation requires the processing of personal data.
- ✓ Processing data is necessary in order to ensure the essential interests of the data subject;
- ✓ Processing is necessary to perform tasks of public interests or carried out by an official authority.
- ✓ The data controller has a legitimate interest in processing the personal data of the data subject; this interest, however, has to be necessary balanced with the right to privacy of the data subject ([51]).

([46]) Radio-frequency identification (RFID) is a technology enabling the processing of personal data, including personal data. In particular RFID applications allow the processing of personal data stored on the tag (see Recital 4, RFID recommendation).
([47]) See Article 2, RFID recommendation.
([48]) See Recital 10, RFID recommendation.
([49]) See Article 2(a), (b) and (d) of the DPD. In practical terms a data controller can be, for example, a medical practitioner that would usually be the controller of the data processed on his clients or a company would be the controller of the data processed on its clients and employees.
([50]) See Article 6, DPD.
([51]) See Article 7, DPD.

The data subject has the right to ([52]):

- ✓ Be informed of any processing of his data.
- ✓ Access data concerning him.
- ✓ Object to the processing on compelling and legitimate grounds.

The household exemption

As provided in Article 3(2) of the directive, the obligations related to the processing of personal data do not apply in two specific circumstances:

- ✓ In any case of processing activities that fall inside the public security, defence or criminal law enforcement's areas that are not part of the competence of the EC and remain a national prerogative.
- ✓ In the course of a *purely* personal or household activity (i.e. the household exemption) ([53]).

The scope of this last provision is further clarified by Recital 12 of the DPD which states that the processing of data carried out by a natural person in the exercise of activities which are *exclusively* personal or domestic, such as correspondence and the holding of records of addresses ([54]), should be excluded from the protection principles of the directive.

The Court of Justice of the European Communities (CJ) expressed its position on the application of the household exemption in the *Lindqvist* case ([55]). Mrs Lindqvist, a worker for a local Swedish parish, published on a web page, for religious purpose, information (such as name, last name, telephone number) of her parishioners without their consent. She was prosecuted for violation of the national law on personal data. The CJ found that the exemption provided by Article 3(2) of the directive could not be applicable since it is related 'only to activities which are carried out in the course of private and family life of individuals, which is not clearly the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people' ([56]).

The case mentioned above has added another element in order to determine whether the household exemption should be applicable but at the same time it is not clear when the number of people, to which data are available, should be considered indefinite.

The issue is still open ([57]).

([52]) See Article 10 et seq., DPD.
([53]) See Article 3, para. 2, DPD.
([54]) See Recital 12, DPD.
([55]) Court of Justice, Case C-101/01, *Criminal proceedings against Bodil Lindqvist*, OJ C 7, 10.1.2004.
([56]) Court of Justice, Case C-101/01, *Criminal proceedings against Bodil Lindqvist*, OJ C 7, 10.1.2004, para. 47.
([57]) Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: Are users also bound by data protection regulations?*, published online on 1 October 2009, available at http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4 (last visited on 20 October 2009); Rebecca Wong, Joseph Savirimuthu, *'All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet'*, John Marshall Journal of Computer & Information Law, Vol. 25, No 2, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1003025# (last visited on 20 October 2009).

What can the data subject do in case of violation of his rights?

In each Member State one or more public authority should be responsible for ensuring the proper application of the DPD ([58]). The supervisory authority has investigative and effective power of intervention and, when the national provisions adopted in accordance with the directive have been violated, it has the power to engage in legal proceedings or to bring these violations to the attention of the judicial authority.

The data subject can submit his complaint to the supervisory authority, which must examine the claim and may temporarily prohibit the data processing. If the DPD has been violated then the supervisory authority can intervene by ordering to erase, destroy or ban in a definitive way the data processing. If the claim to the supervisory authority did not lead to a satisfactory result, the data subject, with the support of a legal adviser, can submit his case to the judgment of a court ([59]).

Data Protection Working Party

The Working Party is an independent European advisory body, set up under Article 29 of the directive, composed of data protection commissioners of each Member State, of a representative of the Commission and of a representative of the authority or authorities established for the Community institutions and bodies ([60]).

The tasks of the Working Party are:

- ✓ Supporting the uniform application of the national measures adopted under the directive;
- ✓ Providing the European Commission with an opinion on the level of protection in the Community and third countries.
- ✓ Advising the European Commission on any proposed amendment of the DPD, on any additional and specific measures to protect the rights and freedoms of natural persons regarding the processing of personal data.
- ✓ Giving an opinion on codes of conduct drawn up at Community level.

Moreover, the Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community ([61]).

([58]) An overview of national data protection authorities is available at http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last visited on 21 October 2009).
([59]) 'Data protection in the European Union', online guide available at http://ec.europa.eu/justice_home/fsj/privacy/guide/index_en.htm (last visited on 20 October 2009).
([60]) The list of members of the Working Party is available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/members_en.htm#chairman (last visited on 21 October 2009).
([61]) See Article 30(1) and (3) of the DPD.

Data Protection Working Party Opinion 5/2009

Social network providers under the lens of the directive

In June 2009, the Working Party issued an opinion on online social networking ([62]) (the 'Opinion'), aiming to provide SNS providers with guidance on the technical and organisational measures to adopt in order to comply with the European data protection legislation. According to the Opinion, the provisions of the directive apply to SNS providers in most cases, even if their headquarters are located outside of the European Economic Area.

SNS providers as data controllers

SNS providers are data controllers under the directive since they determine the purposes and means of personal data by providing the tools and services related to user management. According to Article 10 of the directive, SNS providers should make users aware of their identity and of the different purposes for which they process personal data. In particular the Working Party recommends SNS providers to:

- ✓ Make aware SNS users about the privacy risks to themselves and to others when they upload information on the SNS.
- ✓ Remind SNS users that uploading information about other individuals may violate their privacy.
- ✓ Advise SNS users on the fact that uploading pictures or information about other individuals should be done with the individual's consent.
- ✓ Offer privacy-friendly default settings, which allow users to specifically and freely consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties.
- ✓ Provide the SNS's homepage with a link to a complaint facility, for any data protection issues.
- ✓ Delete personal data provided by a user when he registers on an SNS as soon as either the user or the SNS provider decides to delete the account; moreover, when a user decides not to use the service for a defined period of time, the profile should be set to inactive.

SNS users as data subjects

Users, in most cases, are considered data subjects, as far as their activities on an SNS are carried out in the course of a purely personal or household activity. In fact, generally speaking, their activities are covered by the household exemption that allows them not to comply with the obligations provided for a data controller. As a consequence users have the right to be informed of any processing of their data, to access them or to object to a specific data processing. The Opinion also stresses the importance of allowing users to use a pseudonym instead of their real identity. SNSs may need, to register a user, some personal data but still do not need to publish the real names of members on the Internet since security measures to protect personal data, such as authentication mechanisms, can still be implemented with the usage of a pseudonym.

([62]) Article 29 — Data Protection Working Party — Opinion 5/2009 on online social networking, 12.6.2009, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm (last visited on 21 October 2009).

Applicability of the directive to non-EU based social networks

The connecting criteria for the application of the national legislation adopted according to the directive are set out in Article 4 of the DPD which provides that the data protection laws of the Member States shall apply when:

- ✓ The data controller is established in the territory of a Member State.
- ✓ The data controller is not established in the territory of a Member State but in a place where its national law applies, according to international public law.
- ✓ The data controller is located outside the European Community but makes use of equipment located in the territory of a Member States for processing personal data.

The use of equipment for processing personal data is considered a decisive element for the application of the directive. The degree of disposal given to the data controller over the equipment that triggers the application of the DPD is the one that allows him to determine the purpose and the procedure of data processing ([63]). The use of cookies ([64]) and similar software devices by an online social service provider can also be seen as the use of equipment in the Member State's territory, thus invoking that Member State's data protection law ([65]). In Europe, many of the best-known US-based social networks, such as Myspace ([66]), Facebook ([67]), LinkedIn ([68]) and Twitter ([69]), use cookies. The Working Party states ([70]) therefore that the national law of Member States, where the user's personal computer is located, applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk ([71]). Based on this consideration the Working Party has concluded that the directive should be applicable to non-EU based social networks.

([63]) Article 29 — Data Protection Working Party — Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, 30.5.2002, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm (last visited on 22 October 2009).

([64]) Cookies are pieces of data created by a web server that can be stored in text files that may be put on the Internet user's hard disk, while a copy may be kept by the website.

([65]) Article 29 — Data Protection Working Party — Opinion 1/2008 on data protection issues related to search engines, of 4.4.2008, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm (last visited on 22 October 2009).

([66]) Myspace privacy policy available at http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last visited on 22 October 2009).

([67]) Facebook privacy policy available at http://www.facebook.com/policy.php (last visited on 22 October 2009).

([68]) LinkedIn privacy policy available at http://www.linkedin.com/static?key=privacy_policy#pri-top (last visited on 22 October 2009).

([69]) Twitter privacy policy available at https://twitter.com/privacy (last visited on 22 October 2009).

([70]) Article 29 — Data Protection Working Party — Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, 30.5.2002, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm (last visited on 22 October 2009).

([71]) For a deeper analysis see Aleksandra Kuczerawy, *Facebook and its EU Users — Applicability of the EU Data Protection Law to US Based SNS*, in Bezzi M., Duquenoy P., Fischer-Hübner S., Hansen M. (eds.), Post-Summer School Proceedings of the IFIP/PrimeLife Summer School on "Privacy and Identity Management for Life", Nice, France, 7-11 September, Springer-Verlag (2010, forthcoming).

Is the SNS user responsible for compliance with the directive?

The responsibility for the unlawful processing of third-party data may lie with the user himself according to Member States' criminal and civil law provisions (i.e. defamation, penal liability, right of personal portrayal, etc.). However, at this point, some considerations and evaluations have been made by researchers and scholars in order to understand if and to what extent the data-processing operations carried out by an SNS user could be considered subject to the directive.

SNS users as data controllers

Based on the definition provided by Article 2(d) of the directive a data controller is:
'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the *purpose* and *means* ([72]) of processing of personal data [.....]'.

In order to qualify a user as a data controller it is necessary to analyse what the purpose and means of data processing available to an SNS user are and what decision-making power he has with regards to both ([73]). As in most cases the purpose of SNS providers is economic, since they generate much of their revenue through advertising and marketing ([74]). For the SNS user, the main aim is entertainment, such as interacting with friends or meeting new people. In some cases, for example when a business-oriented social network is chosen, such as LinkedIn, the purpose can be related to business and career opportunities. In any case the scope of data-processing operations is chosen freely by the user when he decides to access a specific social network.

The major features and settings of an SNS are provided and set up unilaterally by the SNS provider, which decides how to carry out the data processing. In this context, as it has been observed ([75]), a small margin of decision-making power still remains with the user regarding the means by which the data are processed. The user in fact can still decide, when accessing an SNS, what information to upload and by which means among the ones available and, as a consequence, it could be stated that he only acts as a controller '*with regards to the content he chooses to provide and the processing operations he initiates*' ([76]).

([72]) Emphasis added.
([73]) Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4 (last visited on 20 October 2009).
([74]) Article 29 — Data Protection Working Party — Opinion 5/2009 on online social networking, 12.6.2009, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm (last visited on 21 October 2009).
([75]) Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4 (last visited on 20 October 2009).
([76]) Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4 (last visited on 20 October 2009).

This statement does not exclude the margin for the application of the household exemption, which still remains the most questionable point. As described above, the exemption provided by Article 3(2) of the DPD should not be applicable any time the data entrusted to the Internet are made available to an indefinite number of people. Considering nevertheless that no further elements are provided by the law or jurisprudence, regarding the applicability of Article 3(2) of the DPD, it could be argued that at least those SNS users who choose a public setting for their account fall within the scope of the directive. In fact, in general, private profiles are only accessible to those with whom a connection is shared but even in this case 'a large private public' could access the data uploaded ([77]).

Consequences deriving from the qualification of SNS users as data controllers

The implication deriving from the qualification of an SNS user as a data controller is to ensure that his processing activities are carried out in accordance with the main provisions of the directive ([78]), such as:

- ✓ The criteria set forth in Article 7 for making the data processing legitimate (such as obtaining the unambiguous consent of the individual to whom the data are related, necessary processing, etc.).
- ✓ The rights of the data subject to obtain information (Article 10), to access data (Article 12), to object (Article 14).
- ✓ The confidentiality and security of processing as set forth in Articles 16 and 17.

This framework basically defines what the liability of the SNS user as a data controller should be towards data subjects in case of breaching data protection principles.

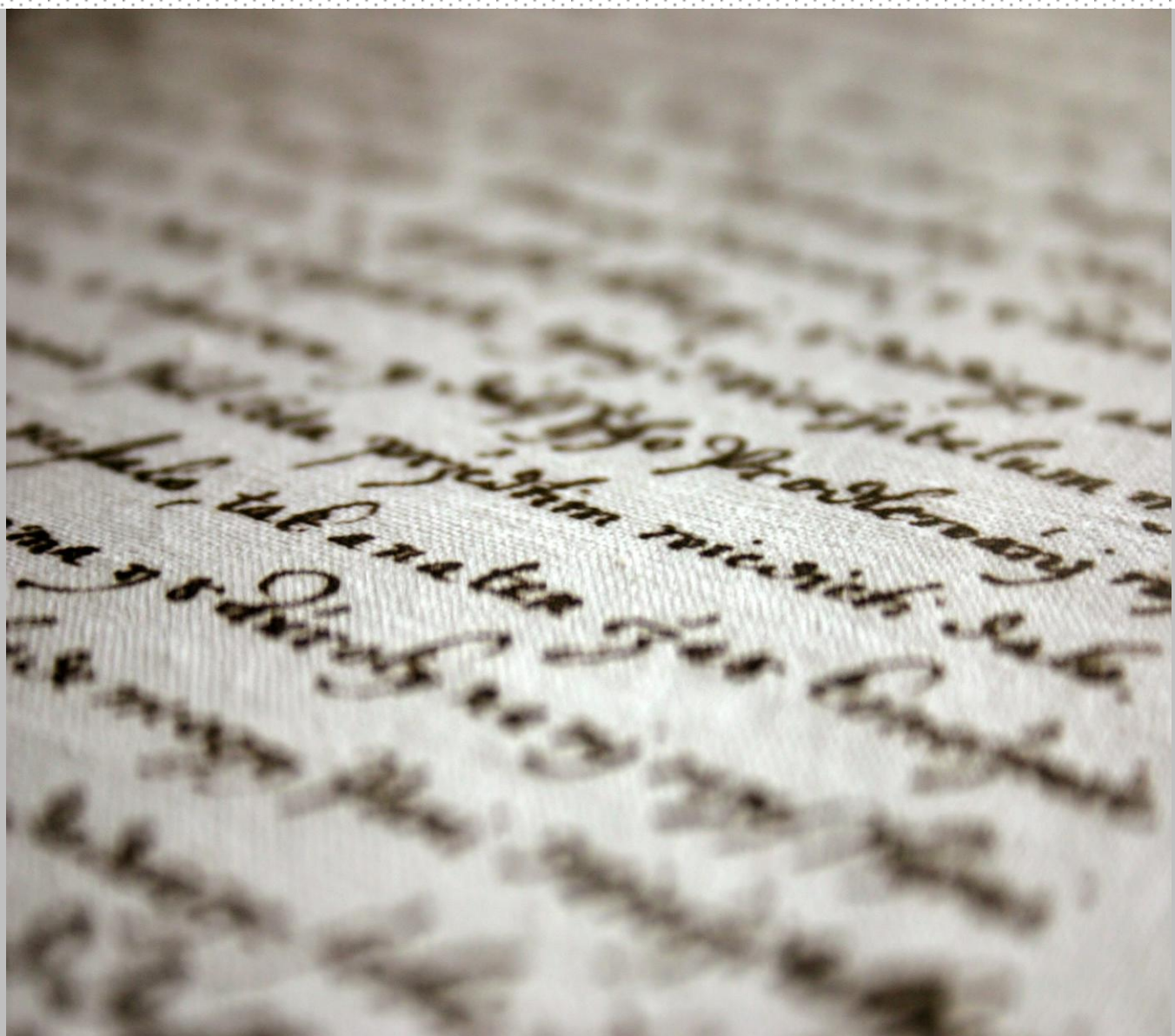
Considering the extraordinary development of social networks and the increasing number of users involved in social networking activities, it is evident that the evaluations and considerations above underline the necessity for a legislative review and interpretation to clarify this grey-area such as the responsibility of data controllers who are not legal persons. The SNS users' activities should be clearly regulated for example by setting a limit on the collection of personal data over which natural persons become subject to the provision of data protection legislation ([79]).

([77]) Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4 (last visited on 20 October 2009).

([78]) Rebecca Wong, *Social networking: Anybody is a data controller*, posted online on 23 September 2008, last revised on October 3, 2008 available at http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=653673 (last visited on 23 October 2009).

([79]) ENISA, *Presentation to the LIBE Committee of the European Parliament. How to strengthen the EU legislation, improve international cooperation and secure the growing market of internet service*, 2008, available at http://www.enisa.europa.eu/act/it/library/pp/eu-leg

Part 5- Golden Rules



Golden rules

These safety tips draw on analysis of data and available research. This section is intended to provide, in one convenient place, recommendations to raise awareness about the risks and threats related to the misuse of social networks, in particular when accessed through mobile phone, with advice on how to avoid unwanted consequences.

Category	No	Recommendations	Description
Pay attention to what you post and upload	1	Consider carefully which images, videos and information you choose to publish	Remember that a social network is a public space; only post information or upload images you are comfortable with, keeping in mind that at a later stage you might be confronted with the content you uploaded, e.g. in a job interview. Information and pictures you post online should be considered permanent. They can be copied and stored by other individuals and can resurface years later in search engines.
	2	Never post sensitive information	Do not make information such as address, date of birth or financial data available in your profile. A criminal might access your profile and steal your identity.
	3	Use a pseudonym	You do not need to use your real name in an online profile. Using a nickname can help you protect your identity and privacy; only close contacts will know who is behind the nickname.
Choose your friends with care	4	Do not accept friend requests from people you do not know	Be selective about who you accept as a friend on a social network. You do not have to feel obliged to add someone to your friends' list. Politely refuse or simply ignore the request.
	5	Verify all your contacts	Ensure that the people you are in contact with or who sent a friend request are really who they say they are. Do not trust them immediately.
Protect your work environment and avoid reputation risk	6	When joining a social networking site use your personal e-mail address	Do not use your company e-mail address but your private one and do not post confidential or competitive information about your organization. Be careful about the information you reveal about your workplace, for example do not post pictures shot in front of your office with the company's address or logo on the background that may lead to your job or workplace address.
	7	Be careful how you portray your company or organisation online	Consider what your employer would think before posting any comments or material online about your company or organisation.

	8	Do not mix your business contacts with your friend contacts	You have no control over what your friends may post online or how they may portray you and consequently what your employer, colleagues and clients may be exposed to.
Protect your mobile phone and the information saved on it from any physical intrusion	9	Do not let anyone see your profile or personal information without your consent	Before accessing your profile through your mobile phone pay attention to the environment and people that are surrounding you. If someone is trying to see what you are doing access your profile in a safer place.
	10	Do not leave your mobile phone unattended	Someone with malicious intent could update your profile and status with false details. Remember to log out from the social network once your navigation is over and not to allow the social network to remember your password (this function is called 'Auto-complete').
	11	Do not save your password on your mobile phone	Mobile phones can be easily lost or stolen and if you save your password on your mobile device anyone who may have possession of it can access your profile, see your pictures and friends. Try to commit your password to memory and if you write it down be careful where you store it.
	12	Use the security features available on your mobile phone	Remember to lock the keypad when not in use and to protect the device with a PIN or a password. Backup your details to another device such a PC in case your mobile phone is lost or stolen. Configure connections (such as Bluetooth and Wi-fi), especially in airports and public spaces, to be secure and if your mobile device has a built in firewall remember to enable it.
Respect other people's privacy	13	Be careful what you publish about someone else	Do not upload pictures or personal information regarding other people without their consent. You might commit a criminal offence.
Inform yourself	14	Read carefully and in full the privacy policy and the conditions and terms of use of the social network you choose	Always be informed about who provides the service and how your personal information will be used and who has the right to access the information you post.
Protect your privacy with the privacy settings	15	Use privacy-oriented settings	Set the profile privacy level properly. Check the privacy settings of your profile — who can see your pictures, who can contact you and who can add comments in order to avoid making your profile available to everyone.
Report immediately lost or stolen mobile	16	Be careful when using your mobile phone and pay attention to where you put it	Report immediately stolen or lost mobile phone with contacts and pictures saved in its memory and personal information regarding you and your friends (e.g. those friends whose contacts on the SNS have been synchronized with the

			mobile phone).
Pay attention to the location based services and information of your mobile phone	17	Deactivate location based services when not using them.	Remember to deactivate location based features of your mobile phone if you don't need them.

Conclusions

The huge potential of mobile social networks in the immediate future let us imagine the enormous benefits that everyone could get from the integration of mobility, always-on connectivity, and social networking services. Such a reality could be a great advantage for lifelong learning, community living, and knowledge-sharing but, as boundaries between public and private spaces will blur, also new risk scenarios will emerge. Companies should assure that their staff members understand and explicitly accept the security and privacy requirements of the organization they work for. Employees should be educated to understand that the information placed in web profiles or in twitter streams may be misused by others looking for important facts and figures and may cause damage to the company's reputation and to their carrier. Every user should be aware of the fact that the information they entrust to an SNS are linked to their real identity, thus exposing them and eventually their friends to the risk and threat scenarios described in this paper.

The conducted analysis showed that many of the privacy issues originating from the web-based access to SNSs also apply to MSNs but there are also a number of unique risks and threats against MSNs. The real-time spread of information and data through social mobile can cause serious damage that can affect private and working environment, a lost or stolen mobile phone can cause the loss of important data, contacts, pictures, personal details and access codes, threatening the user's privacy and the one of his friends whose contacts on the SNS have been synchronized with the mobile phone.

Awareness raising and information security empowerment is the first line of defence and the first security measure related to private and working environment. ENISA hopes that this paper will provide social mobile users with a valuable tool to understand the risks and threats scenario arising from the usage of social mobile and the related privacy issues, also providing a set of recommendations for raising awareness of users.

Acronyms

CJ	Court of Justice of the European Communities
DPD	Directive 95/46/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
MSN	Mobile social network
RFID	Radio Frequency Identification
SNS	Social networking site

References and sources for further reading

20minutes.es, *Rajoy, Lucía Etxebarría o José Mota, suplantados en las redes sociales,* 6 July 2009, http://www.20minutos.es/noticia/477404/0/internet/identidades/falsas/ (last visited on 9 November 2009).

20minutes.fr, *La RATP ouvre une enquête sur une vidéo d'agression dans un bus*, 7 April 2009, http://www.20minutes.fr/article/318507/France-La-RATP-ouvre-une-enquete-sur-une-video-d-agression-dans-un-bus.php (last visited on 9 November 2009).

Aleksandra Kuczerawy, *Facebook and its EU Users — Applicability of the EU Data Protection Law to US Based SNS*, in Bezzi M., Duquenoy P., Fischer-Hübner S., Hansen M. (eds.), Post-Summer School Proceedings of the IFIP/PrimeLife Summer School on "Privacy and Identity Management for Life", Nice, France, 7-11 September, Springer-Verlag (2010, forthcoming).

Alessandro Acquisti, Ralph Gross, *Imagined Communities: Awareness, Information sharing, and Privacy on the Facebook,* 12 December 2006, available at http://www.springerlink.com/content/gx00n8nh88252822/?p=62d211a0d9c94b26bf709f93ddf44781&pi=0 (last visited on 19 November 2009).

Alexander Gostev, Denis Maslennikov, *Mobile malware evolution: An overview, Part 3*, 29 September 2009, available at http://www.viruslist.com/en/analysis?pubid=204792080 (last visited on 9 November 2009)

Alexander Richter and Michael Koch, *Functions of social networking services,* in: Proceedings of the 8th International Conference on the Design of Cooperative Systems, Carry-le-rouet, France, Institut d'Etudes Politiques d'Aix-en-Provence, 2008, available at http://www.kooperationssysteme.de/docs/pubs/RichterKoch2008-coop-sns.pdf (last visited on 5 November 2009).

Art.29-Data Protection Working Party – *Opinion 1/2008 on data protection issues related to search engines*, of 04.04.2008 available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm (last visited on 19 November 2009).

Art.29-Data Protection Working Party – *Opinion 4/2007 on the concept of personal data*, of 20.06.2007 available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm (last visited on 19 November 2009).

Article 29 — Data Protection Working Party — *Opinion 1/2008 on data protection issues related to search engines*, of 4.4.2008, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm (last visited on 22 October 2009).

Article 29 — Data Protection Working Party — *Opinion 5/2009 on online social networking*, 12.6.2009, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm (last visited on 21 October 2009).

Article 29 — Data Protection Working Party — *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites*, 30.5.2002, available at

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm (last visited on 22 October 2009).

AVG, *Bringing social security to the online community,* 26 August 2009, available at www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf (last visited on 19 November 2009).

Bernardo A. Huberman, Daniel M. Romero, Fang Wu, *Social networks that matter: Twitter under the microscope,* December 12 2008, available at http://www.hpl.hp.com/research/scl/papers/twitter/ (last visited on 19 November 2009).

Blitz quotidiano, *Facebook, diffamazione contro una donna: indagati tutti i 67 Marco Girardi iscritti al network,* 6 September 2009, available at http://www.blitzquotidiano.it/tag/marco-girardi/ (last visited on 1 November 2009).

Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: Are users also bound by data protection regulations?*, published online on 1 October 2009, available at http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4 (last visited on 20 October 2009).

Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.

CNN.com, *Smartphone security threats likely to rise,* 29 October 2009, available at http://edition.cnn.com/2009/TECH/10/25/smartphone.security/index.html (last visited on 19 November 2009).

Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, OJ L 122, 16.5.2009.

comScore press release, 15 April 2009, available at http://www.comscore.com/layout/set/popup/Press_Events/Press_Releases/2009/4/Facebook_Top_Social_Network_in_Spain (last visited on 5 November 2009).

comScore press release, 17 February 2009, available at http://www.mediametrix.com/Press_Events/Press_Releases/2009/2/Social_Networking_France (last visited on 5 November 2009).

Corriere della sera.it, *Critiche all'azienda online, Licenziata per Facebook*, 21 May 2009, available at http://milano.corriere.it/milano/notizie/cronaca/09_maggio_21/licenziata_facebook_critiche_azienda-1501380122088.shtml (last visited on 9 November 2009).

Corriere della sera.it, *Pazienti intubati su Facebook, il Garante avviera' un'istruttoria,* 14 May 2009, available at http://www.corriere.it/cronache/09_maggio_14/garante_ospedale_udine_dc70f560-409b-11de-aa9a-00144f02aabc.shtml (last visited on 9 November 2009).

Court of Justice, Case C-101/01, *Criminal proceedings against Bodil Lindqvist*, OJ C 7, 10.1.2004.
Data protection in the European Union, online guide available at http://ec.europa.eu/justice_home/fsj/privacy/guide/index_en.htm (last visited on 20 October 2009).

Deloitte, *Losing Ground -2009 TMT Global Security Survey, Key findings*, 2 June 2009, available at http://www.deloitte.com/view/en_US/us/Industries/MediaEntertainment/article/e510f6b085912210VgnVCM100000ba42f00aRCRD.htm (last visited on 19 November 2009).

Deloitte, *Social networking and reputational risk in the workplace,* 28 May 2009, available at http://www.deloitte.com/view/en_US/us/About/EthicsIndependence/article/8aa3cb51ed812210VgnVCM100000ba42f00aRCRD.htm (last visited on 19 November 2009).

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

EESC, *Opinion On The Impact of Social Networking Sites on Citizens*, September 23 2009, available at http://www.edri.org/edri-gram/number7.18/eesc-social-networking-websites (last visited on 19 November 2009).

Electronic Privacy information Center available at the website http://epic.org/privacy/facebook/ (last visited on 5 November 2009).

elmundo.es, *Burlas y venganzas circulan por la Red detrás de identidades falsa,* 7 July 2009, available at http://www.elmundo.es/elmundo/2009/07/05/navegante/1246809687.html (last visited on 9 November 2009).

eMarketer, April 2008, available at http://www.emarketer.com/Report.aspx?code=emarketer_2000489 (last visited on 2 November 2009).

ENISA, *Security issues in the context of authentication using mobile devices (Mobile eID),* 2008, available at http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security issues mobile devices

ENISA, *Presentation to the LIBE Committee of the European Parliament. How to strengthen the EU legislation, improve international cooperation and secure the growing market of internet service,* 2008, available at http://www.enisa.europa.eu/act/it/library/pp/eu-leg

ENISA, *Security Issues and Recommendations for Online Social Networks*, 2007, available at http://www.enisa.europa.eu/act/it/oar/social-networks/security-issues-and-recommendations-for-online-social-networks

ENISA, *Technology-induced challenges in Privacy & Data Protection in Europe*, 2008, available at http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe/?searchterm=technology in

ESET, *Global Threats Trends –September 2009,* available at http://www.eset.com/threat-center/threat_trends/Global_Threat_Trends_September_2009.pdf (last visited on 19 November 2009).

Facebook press room, statistics available at http://www.facebook.com/press/info.php?statistics (last visited on 5 October 2009).

Facebook privacy policy available at http://www.facebook.com/policy.php (last visited on 22 October 2009).

Graham Cluley, *Social networks: The new frontier for Malware, Spam and Identity Theft,* ICT Forum 2009 Conference, 15 July, available at

http://www.ictf.ox.ac.uk/conference/2009/programme.html#Plenary3 (last visited on 19 November 2009).

Hanna Krasnova, Oliver Günther, Sarah Spiekermann, Ksenia Koroleva, *Privacy concerns and identity in online social networks,* published online 1 October 2009, available at http://www.springerlink.com/content/l371174132178uwm/?p=ef2d38c4f2ce4bd78341b65ed1ccd940&pi=1 (last visited on 19 November 2009).

ICT Statistics Newslog, *Email and Social Networking Most Popular Mobile Internet Activities,* 15 May 2009, available at http://www.itu.int/ITU-D/ict/newslog/Email+And+Social+Networking+Most+Popular+Mobile+Internet+Activities.aspx (last visited on 19 November 2009).

Il Corriere del mezzogiorno, *La camorra di Pomigliano cerca adepti: gruppo su Facebook fondato da giovani,* 28 September 2009, available at http://corrieredelmezzogiorno.corriere.it/notizie/cronaca/2009/28-settembre-2009/camorra-pomigliano-cerca-adeptiil-gruppo-facebook-giovani-iscritti-1601817500073.shtml (last visited on 2 November 2009).

InfoWorld, *Hackers put social networks such as Twitter in crosshairs,* 17 August 2009, available at http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-crosshairs-832?source=IFWNLE_nlt_sec_2009-08-17 (last visited on 19 November 2009).

INTECO, *Study on the privacy of personal data and on the security of information in social networks,* February 2009, available at http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en (last visited on 24 November 2009).

INTECO, *Security in twitter clients,* November 2009, available at http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_est_twitter_clients_securityen.pdf (last visited on 7 January 2010).

Italian Data Protection Authority press release, available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1614095 (last visited on 9 November 2009).

Italian Data protection Authority, *Social network: watch out for side effects*, May 2009, available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1614258 (last visited on 9 November 2009).

Joseph Bonneau, Sören Preibusch, *The privacy jungle: On the market for data protection in social networks*, Eighth Workshop on the Economics of Information Security (WEIS 2009), 24–25 June 2009, available at http://weis09.infosecon.net/files/156/index.html (last visited on 5 November 2009).

Juniper Research, *Mobile advertising, because I'm worth it,* extract from Mobile advertising delivery channels, strategies & forecasts 2008-2013, 2008, available at http://www.c2mweb.eu//files/Whitepaper_Mobile_Advertising.pdf (last visited on 30 November 2009).

La Repubblica.it, Turin, *Taroccato su Facebook il profilo del Professore*, 7 May 2009, available at http://torino.repubblica.it/dettaglio/taroccato-su-facebook-il-profilo-del-professore/1629649 (last visited on 9 November 2009).

La Stampa.it*, Facebook—Hospital infermiera fotografa sospesa 10 giorni le molinette: non prendera' lo stipendio il primo provvedimento disciplinare*, 9 January 2009, available at http://archivio.lastampa.it:80/LaStampaArchivio/main/History/tmpl_viewObj.jsp?objid=9011456 (last visited on 10 November 2009).

La Stampa.it, *Facebook, rubata l'identita' a un Professore di Trento,* 5 January 2009 available at http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5580&ID_sezione=38&sezione=News (last visited on 26 November 2009).

La Voce del Nord Est, Udine, *Infermiera carica su Facebook le foto dei pazienti intubati,* 14 May 2009, available at http://www.lavocedelnordest.it/articoli/2009/05/14/2023/udine-infermiera-carica-su-facebook-le-foto-dei-pazienti-intubati (last visited on 9 November 2009).

LaStampa.it, *Infermieri e medici pazzi di Facebook*, 6 January 2009, available at http://www.lastampa.it/multimedia/multimedia.asp?p=38&pm=&IDmsezione=14&IDalbum=14701&tipo=FOTOGALLERY#mpos (last visited on 19 November 2009).

Libération.fr, *Un policier soupçonné d'avoir diffusé la vidéo de l'agression dans un bus,* 8 April 2009, available at http://www.liberation.fr/societe/0101560932-agression-dans-un-bus-la-police-des-polices-saisie (last visited on 9 November 2009).

LinkedIn privacy policy available at http://www.linkedin.com/static?key=privacy_policy#pri-top (last visited on 22 October 2009).

List of members of the Working Party, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/members_en.htm#chairman (last visited on 21 October 2009).

MailOnline, *Second investigation launched after BA check-in staff post comments about 'smelly' passengers on Facebook,* 3 November 2008, available at http://www.dailymail.co.uk/news/article-1082437/BA-check-staff-post-comments-smelly-passengers-Facebook.html (last visited on 11 November, 2009).

MailOnline, *Teacher is suspended for jibe on Facebook about her class*, 1 August 2009, available at http://www.dailymail.co.uk/news/article-1202210/Teacher-suspended-jibe-Facebook-class.html (last visited on 26 November 20009).

Mariano Rajoy and Lucía Extebarrías's forged profiles available at http://twitter.com/marianorajoy and http://twitter.com/luciaetxebarria (last visited on 9 November 2009).

Martin Pekárek, Ronald Leenes, *Privacy and Social Network Sites: Follow the Money!* January 15-16, 2009, available at www.w3.org/2008/09/msnws/papers/tilt.pdf (last visited on 24 November 2009).

Martin Pekárek, Stefanie Pötzsch, *A comparison of privacy issues in collaborative workspaces and social networks*, published online 28 July 2009, available at http://www.springerlink.com/content/g54qk93430581554/?p=dae26d8123004ccf88e5004aa1aba269&pi=0 (last visited on 5 November 2009).

Mashable, The social media guide, *Exploring best practices for building and monetizing mobile social networks*, 3 October 2008, available at http://mashable.com/2008/10/03/mobile-social-networking/ (last visited on 30 November 2009).

Myspace privacy policy available at http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last visited on 22 October 2009).

news.bbc.co.uk, *Payout for false Facebook profile*, 24th July 2008, available at http://news.bbc.co.uk/2/hi/uk_news/7523128.stm (last visited on 16 November 2009).

Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking*, July-September 2008 – available at http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (last visited on 18 November 2009).

Overview of national data protection authorities, available at http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last visited on 21 October 2009).

Privacy setting for social networks, available at http://blog.safetyclicks.com/2008/09/03/social-networks-and-privacy-settings/ (last visited on 5 November 2009).

Rebecca Wong, Joseph Savirimuthu, *All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet,* John Marshall Journal of Computer & Information Law, Vol. 25, No 2, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1003025# (last visited on 20 October 2009).

Rebecca Wong, *Social networking: Anybody is a data controller*, posted online on 23 September 2008, last revised on October 3, 2008 available at http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=653673 (last visited on 23 October 2009).

SafeLine Greek Hotline, website available at www.safeline.gr

SearchSecurity.com, *Kaspersky system analyzes malicious URLs on Twitter for malware,* 29 October 2009, available at http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1372955,00.html (last visited on 19 November 2009).

Status of implementation of the DPD in each Member State available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited on 20 October 2009).
Telegraph.co.uk, *Man sues friend over fake Facebook profile*, 1 July 2008, available at http://www.telegraph.co.uk/news/2226803/Man-sues-friend-over-fake-Facebook-profile.html (last visited on 16 November 2009).

The daily bit, *Un fenomeno chiamato mobile social networking*, September 2008, available at http://www.thedailybit.net/index.php?method=section&action=zoom&id=2489 (last visited on 18 November 2009) and Lastampa.it, *In Europa il social network piace sul cellulare*, August 2008, available at http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5054&ID_sezione=38&sezione=News (last visited on 18 November 2009).

The Nielsen Company, *Global faces and networked places*, March 2009, available at http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/ (last visited on 5 October 2009).

The Nielsen Company, *Mobile media nei mercati emergenti e in Italia*, IAB Seminar, 16 July 2008, available at http://www.iabseminar.it/video.aspx?IDSessione=12 (last visited on 5 November 2009).

The Nielsen Company, *To Mobile or Not to Mobile,* 15 September 2009, available at en-us.nielsen.com/etc/medialib/nielsen_dotcom/en_us/documents/pdf/webinars.Par.81596.File.pdf (last visited on 19 November 2009).

The Register*, Virgin probes Facebook safety, chav claims,* 24 October 2008, available at http://www.theregister.co.uk/2008/10/24/virgin_facebook_investigation/ and http://www.theregister.co.uk/2008/11/03/virgin_sackings_ba_rudeness/(last visited on 11 November, 2009).

Thierry Nabeth, *Social web and identity: a likely encounter,* published online 1 October 2009, available at http://www.springerlink.com/content/l84mt42267347524/ (last visited on 19 November 2009).

Online as soon as it happens

ISBN: 978-92-9204-036-9

Catalogue number: TP-80-09-988-EN-N

DOI : 10.284/15183

TP-80-09-988-EN-N

ISBN: 978-92-9204-036-9

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu