Cloud based social network sites

Moiny, Jean-Philippe

Published in:
Investigating cyber law and cyber ethics

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Chapter 9
Cloud Based Social Network Sites: Under Whose Control?

Jean-Philippe Moiny
University of Namur, Belgium

ABSTRACT

In studying Social Network Sites (SNSes), this chapter starts from the identification of a loss of users' control over personal information. It briefly defines what SNSes are and links them to "cloud computing." Its purpose is to identify how American and European (or as the case may be, Belgian) laws empower users to recover some control where they lack technical means to control information related to them. It will be shown that user's consent is central to numerous legal dispositions. To this end, four legal themes are studied: privacy, data protection (consent and right of access), confidentiality of electronic communications, and the prohibition of unauthorized access to computers (hacking). Through these reflections, the American and European perspectives are compared, and the differences between these inevitably lead to a final title underlying the importance of rules governing prescriptive and adjudicative jurisdictions concerns. These rules are finally sketched, before the conclusion finally summarizes the whole purpose.

As the author of this chapter is a European jurist, European law constitutes the point of departure of the reflections, and can be sometimes (titles I and IV) the sole legal framework of the discussion. The information in this chapter is current up to January 28, 2010, save as otherwise stipulated. It should be noted that the information that is studied in context is constantly changing.

DOI: 10.4018/978-1-61350-132-0.ch009

INTRODUCTION

Two quotations illustrate a claim for control coming from the users of Social Network Sites (SNSes). From the US civil liberties association, before the American Federal Trade Commission [FTC], "EPIC urges the Commission to [...] require Facebook to give users meaningful control over personal information" (EPIC v. Facebook 1, 2009, no. 3)[1], "[c]ompel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers" (EPIC v. Facebook 1, 2009, no. 118)[2]. Actually, "users desire control over the collection and use of information about them" (UC Berkeley, School of Information [UCBSI], 2009, p. 5). More recently, a modification of Facebook's privacy settings lead to a new complaint of EPIC noticing that users are now forced to make public data they could formerly keep restricted (EPIC v. Facebook 3, 2010). It has notably been claimed that Facebook "Converted Facebook Users' Private Information into "Publicly Available" Information" (EPIC v. Facebook 3, 2010, nos. 35 and ff.) and "Discloses the Personal Information of Facebook Users without Consent" (EPIC v. Facebook 3, 2010, nos. 65 and ff.). As regards the European Union and the group known as the Berlin Working Party, SNSes providers were already advised to "[i]mprove user control over use of profile data" (International Working Party on Data Protection [IWGDPT], 2008, pp. 6-7).

In the context of SNSes (I), Internet surfers seem to partially lose the legitimate[3] *ownership* of data relating to them. They suffer a *loss of control*[4] (II). To some extent, law – at least, the fields studied here – faces this concern. But how is and should it be done (III)? American and European regulatory systems both need to be referred to, and their differences brought into focus. While individuals are not generally bothered by these differences, these SNSes often have a foot in Europe and the other in the United States – frequently California (Facebook, LinkedIn, and Second Life). But which law and which judges are in control (IV)?

This chapter defines what SNSes are, legally and technically. It also suggests some consideration related to the SNSes market. For the needs of the whole purpose, Facebook is taken as a recurrent example. SNSes generally constitute information society services pertaining to cloud computing technology. Therefore, some ideas can be extended to cloud computing in general. The technology used and the functioning of SNSes lead to identifying a certain loss of control over their personal data by users. Some legal issues related to this loss are therefore addressed. Moreover, privacy and data protection are studied in this chapter. A legal conception of privacy which empowers users is chosen as regards American and European perspectives. In this respect, the horizontal effect of the fundamental right to privacy is discussed. The focus then moves to specific concerns related to data protection. The quality of consent of the data subject, apparently omnipresent in the context of SNSes, is discussed. The data subject has to be informed by SNS providers. His consent should be separated from his consent to the general terms and conditions of the SNS. And finally, such consent has to be freely given. This last point requires to be linked with the considerations related to the SNS market. The relevance of the data subject's right of access in the context of SNSes is then examined, before the confidentiality of electronic communications is brought into focus. The use of cookies by the SNS provider is specifically discussed in this framework. And some reflections relate to the qualifying an SNS as an electronic communications service. Mainly, this chapter identifies which communications are protected. The interest then moves to the protection of the user's terminal. The prohibition of hacking is discussed in the context of SNSes. It is questioned if a breach of the terms of use of an SNS by a user

in fact makes them a "hacker." Other specific developments related to cookies are scrutinized. Finally, the text briefly discusses European private international law from the prescriptive and adjudicative jurisdictions[5] viewpoints. Due to the differences between American and European law, the question of the applicable law becomes particularly relevant in a context where different legal systems and cultures collide.

THE CONTEXT OF SOCIAL NETWORK SITES

This section describes what SNSes are from the technical and legal viewpoints. It also tries to describe the relevant market of SNSes. This latter will then reveal relevant as regards the consent of SNSes users. To these ends, only European law is taken into account.

Social Network Sites and Cloud Computing

Briefly and technically, an SNS "can be defined as [a] website whose main purpose is to act as a connector among users" (Levin & Sánchez Abril, 2009, p. 1017) [6]. In particular, we could call Facebook and similar SNSes[7] "meta-SNS." This means SNSes that relate to indeterminate contexts. Through them, users can share whatever kind of information they want, from individualized and, generally, nominative profiles. Data – whether personal or not – and their exchange, are essential attributes of SNSes[8]. Providers host and manage the profiles completed by users, and what these users share. Applications can sometimes also be added to the profiles[9]. This constitutes the principal business promoted by SNS providers: Hosting and making available data to members of the social network[10], according to the sharing rules chosen by these users among a range of options (*e.g.* Facebook's privacy settings) defined by SNS providers.

SNSes also use what is called "cloud computing." Cloud computing is "a different form of IT infrastructure" (Joint, Baker, & Eccles, 2009, p. 270). SNSes usually embed different kinds of cloud computing services[11]. They consist of applications utilized by users from their browser, on remote third-party servers. In this respect, an SNS is "software as a service." Users' data (texts, images, videos, etc.) are also stored in datacenters, generally located abroad (*e.g.* in the U.S. as regards Facebook[12]), and not on the users' own personal computers. These datacenters are managed by the SNS provider (or their subcontractor) who then provides "data storage as a service" (or, more generally, "infrastructure as a service"). Finally, looking at Facebook-like SNSes, a "platform as a service", the application programming interface [API] is also provided to developers. Such API enables them to create applications (software) running through the SNS[13].

In European legal terms, these kinds of services are Information Society Services in the sense of the E-commerce Directive[14]. In fact, SNSes are normally "provided for remuneration." Their providers pursue an economic activity[15]. Indeed, SNSes "are usually for-profit businesses" (Levin et al., 2009, p. 1019)[16]. In the case of Facebook, advertisement banners and the targeted advertisement service *Ads* (and its variants *Social Ads* and *Engagement Ads*[17]) secure an economic counterpart for Facebook Inc. These applications, for which you have to pay, are integrated to the social network. *Ads* offers companies – or anyone – the ability to target a defined audience of the network, according to criteria they choose – e.g. sex, age, location or other criteria corresponding to certain fields of the user's profile –, to promote services or products. The *Insights* tool can be cited too. It permits the assessment of the effectiveness of the ordered targeted ads. The *Gifts* application can also be noted, enabling people to send gifts ($1 per gift) to friends. Finally, *Polls*, to carry out polls through the network, is also for a charge. Facebook is not the only one

SNS with advertisement functionalities. Indeed, LinkedIn and MySpace also offer a user targeted advertisement function (Office of Privacy Commissioner of Canada [OPCC], 2009, pp. 22 and 30). Moreover, licenses granted by users to SNS providers allow the latter to commercially use the copyrighted content of the former. Some of these licenses go beyond the sole technical needs for the functioning of the provided service. In this respect, these licenses might also constitute this kind of economic counterpart[18].

This chapter will discuss the consent of an SNS user is usually central to the legal rules that are identified to empower users to recover control over their personal data in the abovementioned context. Since the free character of the users' consents will partially depend on the SNSes market, this latter is then now discussed.

The Market of Social Network Sites

European competition law and the economic tools it relies on are useful to give an insight into the SNS market. Taking Facebook as a point of departure, the SNS relevant market has first to be identified. This leads "to identify in a systematic way the immediate competitive constraints faced by an undertaking" (EC DG Competition, 2005, no. 12). If there are a lot of SNSes providers in the relevant market of the SNS, the user will be free to choose one or another, depending on his preferences as regards, for instance, price, functionalities, data processing, etc. However, it would still be necessary that these providers compete as regards these elements – e.g. data protection.

After the relevant market has been identified, it is interesting to observe if a SNS provider has a dominant position on this market. Because of this situation a dominant position could make this provider insensitive to the claim of control arising from society[19]. Such a situation can prevent the web surfers to effectively choose. Moreover, competition law would prohibit the dominant SNS provider from abusing his position[20]. That is to say that the company could be forbidden from adopting certain conduct that other companies are free to adopt. For instance, could a dominant SNS provider prevent an application developer from building an application on the SNS API (refusal to supply) offering the users the possibility to easily retrieve all their data from the SNS, in a convenient format, to easily leave the network? Could the SNS provider rely on targeted advertising and processing of personal data of its users (or even the sale of personal data) to finance its service and offer them for "free" to its users (predatory pricing)? Although these questions are interesting, the purpose only concentrates on the definition of the relevant market and the potential identification of a dominant position.

In regards to the relevant market, SNS is a wide concept that covers different services that can generally be qualified as "multi-sided platform." "A multi-sided platform provides goods or services to two or more distinct groups of customers who need each other in some way and who rely on the platform to intermediate transactions between them" (Evans, 2008, pp. 8-9). For instance, Facebook proposes targeted advertisement services to businesses (*Ads*), services to those who promote political, businesses, etc. (*Pages*), services to "friends" (the average user Profile), an application programming interface [API] for any developer of application, etc. To some extent, these groups of customers are dependant. The more users there are users, the more companies are interested in advertising over the network. The more there are applications on the network, the more users want to join the network, and vice versa. The more companies advertise through the network, the more the provider earns money, the longer the service remains free for its users and can be permanently innovating, the more users will be inclined to join and remain on the network, etc. As D.S. Evans (2008, p.10) writes, "many multi-sided platforms make their money from one side and make access to the platform available to another side for a price that does not cover the

cost of provision. Facebook, for example, is free to users and makes money by selling advertising." The functionalities of Facebook for which we have to pay will therefore lead to the providing of free users profiles.

A priori, there is no one global market for SNSes. And the purpose does not delimit the *markets* of SNSes. It only gives some elements for reflection. For instance, one division could be made between what would be called a *large or narrow thematic centered SNS* – e.g. a network related to movies (Flixster), to business (LinkedIn), to sexuality, etc. – and *meta-SNS,* unrelated to specific topics – e.g. Facebook, Netlog, Bebo, MySpace, etc. SNSes can also be targeted to a particular geographic region or to the whole world. Another division could follow from the functionalities, the "tools", provided by the SNS. For instance, YouTube is content broadcasting oriented, while Twitter was more a text messages communication tool. Facebook is at once a text messages communication tool, a content broadcasting tool and a platform for third party applications. If Twitter and Facebook are not thematic-centered, they nonetheless diverge as regards the functionalities provided.

But whatever the case, the *network of users* is critical in regards to the success and the lure of the SNS concerned. This is true from a *quantitative* viewpoint – *how many* users does the network involve and *how much* are they involved? What could be called the *quantitative users network*? This is extremely relevant in regards to YouTube-like SNS and meta-SNS such as Facebook. Moreover, the network of users can be relevant from a more subjective *qualitative* viewpoint – *Who* is in the network (e.g. are my friends there)? What could be called the *qualitative users network*? From this last viewpoint, the *temporal dimension* is particularly relevant, as the following scenario shows: The more a user uses an SNS, the more he is captive of this SNS. Because, on the one hand, he brings his own individual network in the SNS; and, on the other hand, he creates a network of individuals he wants to keep alive. Then, to leave the SNS – for example to search for better data protection[21] –, he will have to convince his relational network to do the same. Knowing that in the latter situation, they would not necessarily wish to migrate. Such *qualitative users' network* would be more important (i.e., Facebook-like SNSes than YouTube-like ones).

These three identified elements – the purpose(s) of the network, the offered functionalities and, specifically, the network of users – lead to the possibility that SNSes are *not substitutable* or *interchangeable* goods (or services) from the consumers' viewpoint. "This approach to product market definition uses a 'functional interchangeability' yardstick based on the 'qualitative' criteria of characteristics, price and intended use" (Jones & Sufrin, 2008, p. 62). Therefore, different SNSes in the broad sense of the concept can pertain to different relevant markets[22]. For instance, Facebook and YouTube (purchased by Google, Inc. in 2006) are clearly not in the same market. The launch of Google Buzz demonstrated it. Facebook and eBay are not in the same relevant market[23]. Due to their different purposes, Facebook and LinkedIn could arguably be deemed to pertain to different relevant markets, despite the fact that Facebook offers the possibility to join a "work" network. Arguably, Facebook and Twitter are not in the same relevant market, diverging as regards their functionalities. Twitter was originally oriented to the sharing of short messages. While Facebook gives a wider range of functionalities. T. Eisenmann, G. Parker and M. Van Alstyne (2009, pp. 12 and 14) identify Facebook and Twitter as "weak substitutes." That is to say that they "serve the same broad purpose but satisfy different sets of user needs because they rely on different technologies." They also provide another example:

Monster.com and LinkedIn.com use different approaches in helping users find and fill jobs: searchable listings and social networking, respectively. These approaches offer different

advantages: listings are valuable when parties wish to conduct a comprehensive search, whereas social networks provide a mutually trusted third party's assessment of fit.

Anyway, it needs to be underlined that the offered functionalities and the offered websites can quickly evolve. What "matters is that a sufficiently large number of consumers do consider that a product is a good substitute for the product supplied by the undertaking concerned" (EC DG Competition, 2005, no. 18)[24]. The purpose here is not to say that each SNS equals a specific relevant market. For instance, YouTube and Dailymotion are direct competitors. They share the same purpose and propose similar functionalities. Facebook and MySpace could also be deemed to pertain to the same relevant market. But if these two latter are both intended to (notably) socialize, how taking into account what we called the *qualitative users network*? If too much importance is given to the fact that the friends and contacts of a particular user are located only on one SNS and not on another, this could lead to a too narrow definition of the relevant market. But if no importance is given to such a question, the risk would be then to miss the fact that there is no concrete alternative for a particular user. And that this latter has therefore no real possibility to choose.

In any case, the "demand substitutability"[25] can be low since, notably, SNSes produce positive and direct (and indirect) network effects. "A network effect, as defined in [Spulber's] discussion, refers to the dependence of a consumer's benefit on the consumption of another consumer. In short, "network effects are mutual benefits of consumption" (Spulber, 2008, p. 10)[26]. This is directly linked to the multi-sided platform markets above-mentioned. And this also implies, on the one hand, that users bear high switching costs if they want to migrate. Their profile, data and network are anchored in a particular SNS[27]. On the other hand, new entrants in a SNSes market are confronted with a huge barrier to entry. However, these latter are not necessarily irremediably closed to the market. Entering the market – or even, creating a new market – by elaborating a new functionality and being really innovative (e.g. Twitter) is a solution[28]. As T. Eisenmann, G. Parker and M. Van Alstyne (2009, p. 1) write, "revolutionary functionality" is a path to enter the market. Moreover, the authors pointed out that "platform envelopment" is another way[29]. A new entrant could also try to leverage the position he has in a second market (e.g. webmail such as Gmail) in the SNS market (Google Buzz). In so doing, the entrant is able to profit from the network of users it has in this second market, simply adding a new functionality to the platform he manages. Of course, SNS providers inspire each other. A company can also enter the market by purchasing an incumbent firm. For example, Google bought Youtube and Facebook tried to buy Twitter[30]. Finally, free data portability – and more generally, interoperability of cloud computing services, *would* contribute to making it easier to enter a market. However, this is not the case. Indeed generally, "[o]ne of the most pressing issues with respect to cloud computing is the current difference between the individual vendor approaches, and the implicit lack of interoperability" (Jefferey & Neidecker-Lutz, 2010, p. 31). Anyway, the data portability seems possible even in the present technology context as was stated in a workshop organized by the W3C[31]. It would permit the migration from one SNS, reinforcing individuals' freedom. However, it could also be a threat for privacy and data protection if it is not well designed – what about the export of privacy settings (Grimmelmann, 2009)[32]?

These elements show that the SNSes market is not so easy to draw, and that it can rapidly change. This is not without consequences as regards the potential dominant position of an SNS provider. While alone today in his own market, he could tomorrow face numerous new competitors. To remain in a dominant position, the SNS provider,

Facebook for instance, should have significant market power[33] in the relevant market of "meta-SNS." In other words, Facebook will have to be able to act "independently" of its customers, its competitors and of consumers[34]. It constitutes "the largest social network service in the United States"[35] and its significant presence in the European market cannot be ignored. But while its market share could be high, an oligopoly could exist (e.g. Facebook, MySpace, Bebo and Netlog). And the difficulty to enter the market might also be relative. It has moreover to be noted that in the "new economy"[36], "[d]ominant positions are often temporary and fragile" (Jones & Sufrin, 2008, p. 429), and "[c]ompetition is dynamic", taking place "*to satisfy* the market." Firms compete "to dominate the market" and are "fragile monopolists" that have to continuously innovate (Ahlborn, Evans, & Padilla, 2001, p. 160). So, even assuming that Facebook has a high market share, the dynamics of the new economy lessens the relevance of this observation (Ahlborn, Evans, & Padilla, 2001, p. 163)[37]. "[C]urrent market shares may overstate or understate probable future competitive significance" (Antitrust Modernization Commission, 2007, p. 40). Moreover, it shouldn't be ignored that "competition to *obtain* a monopoly is an important form of competition" (Posner, 2001, p. 117)[38].

These considerations sketched the SNSes markets and underlined a potential lack of choice – of liberty – that users could suffer. These elements have to be kept in mind each time law takes into account the consent of the SNS user.

USERS' LOSS OF CONTROL

Users' loss of control in SNSes can be noticed at three levels: The creation of personal data, their accessibility and their deletion. Facebook will be the principle example used in this section. The focus of this examination is the "average user" of the SNS. The "average user" of the SNS is someone who does not develop applications (developers), does not order targeted ads, etc. Although, there exist other users of the services provided through the network.

Initially, a user controls the production of personal data relating to him/herself on an SNS. The user decides which data they reveal. However this primary control over personal data is limited. First, other users can disseminate data through the network; or more insidiously, for instance, when they synchronize their iPhone with Facebook[39]. Second, SNSes providers could spontaneously and automatically collect data from other sources, such as other websites (e.g. via Facebook *Beacon*[40]), cookies[41], data brokers, etc., pursuing "enhancement" to get more accurate profiles (UCBSI, 2009, p. 9). SNSes providers can also compel users to disclose data such as their real name, date of birth and email address[42]. The user in question does not have any practical control over this production of data. Admittedly, as regards what they have to disclose, users can lie... The cookie method[43], contested in DoubleClick (2001)[44], and the recording of clickstream data "generated by our cyber-activity" (Kang, 1998, p. 1119)[45] (also known as "clicktrail" (Kang, 1998, p. 1227)) are good examples. The SNS provider is able to record the user's use of – or his behavior on – the social network. What the users do when logged on and when they are not; provided the fact that the use of a cookie is necessary in this latter case[46]. For instance, Facebook's privacy policy[47] permits Facebook to record clickstream data relating to its users[48]. So it could store which pages the users consulted, which searches have been made, the groups they joined[49], etc.

Subsequently, by choosing privacy settings, SNS members have the feeling they control the dissemination of personal data related to them. However, again, this control is limited. First and foremost, users cannot control personal data they didn't personally disclose. Then, the privacy settings are themselves limited. In fact, users do not define their content. Their options are set out by

the SNS provider and can evolve as the provider wishes (e.g. modifying the functionalities of the website or directly changing the settings). The infrastructure where users socialize can transform out of their control, even against their wishes. This lack or loss of control is reinforced by the use of cloud computing technologies[50]. In addition, the content of the privacy settings have to be technically secure[51]. Furthermore, privacy settings generally concern the communication of data between users and not as concerns the SNS provider. This means that "once information is 'out', forget about maintaining exclusive control over it" (Kang & Buchner, 2004, p. 242). Once data are accessed by other users, an individual cannot control subsequent uses of the data by them. Facebook's evolution illustrated the relativity of privacy settings and their fluctuations. Originally, only the name of the members and the sub-networks they joined (professional, geographic, etc.) had *necessarily to be shared* through the global Facebook network[52]. But thereafter, the user's profile photo, their friends list, the 'Pages' they are a fan of, their sex and geographical location[53] were considered by Facebook to be public information. But this has again evolved[54]. Anyway, this was crucial as regards Facebook Platform and Applications. Indeed, according to Facebook's former privacy policy: "Applications will always be able to access your publicly available information (name, Profile picture, gender, current city, networks, friend list and pages) and information that is visible to everyone." EPIC's recent complaint before the FTC illustrates the importance of the modification[55]. As a matter of interest, this previous modification of the privacy settings seemed to have gotten Mark Zuckerberg, Facebook's CEO, into trouble when his own photos were publicized... (EPIC v. Facebook 1, 2009, no. 41). But for all that, positive evolutions cannot be denied. In this respect, a user can now, admittedly to a limited extent, control Facebook's use of their name as regards Social Ads and the affixing of this name to advertisements delivered to their friends, telling them the 'Pages' they are a fan of. Moreover, the user can also specify to which friends are addressed the posts they make on their 'Wall'. The complaint of EPIC also had effect over Facebook since, for instance, users are now able again to make their friend list confidential[56]. A huge concern is that in a short period of time, due to the processing capabilities of today's computers, vast amounts of data can be extracted from the network. No matter if the privacy settings come back later to their original status.

Finally, the user's last means to control the proliferation of data related to them is outright deletion, which is equally limited as regards data not directly produced by the user. Moreover, SNS providers sometimes reserve the right to keep data after the deactivation of the user's account or during a certain period of time in backup copies. Once again, when data are downloaded by other users, they cannot be deleted. This SNSes practice illustrates the lack of control over the deletion of data. For instance, the reactivation option of Hi5 suggests that data will be kept (OPCC, 2009, p. 17)[57]. In regards to LinkedIn when a user wishes to terminate his account and permanently delete their data, they must send an email to LinkedIn (OPCC, 2009, p. 24)[58]. LiveJournal keeps a users' data thirty days after the suppression of their account (OPCC, 2009, p. 29)[59]. And finally, concerning Facebook, originally a member couldn't delete their account, while now they can choose between deactivation and permanent suppression of their account; the bleeding occurred and is not reversible.

USERS EMPOWERED TO CONTROL

When a specific loss of control has been identified, law – but not only law – might bring a solution. Hearing that the present paper is focused on law, how does the law – or specific parts of it – deal with the identified loss of control? Privacy and Data Protection are first studied, from general

U.E. and U.S. perspectives. Then, two specific topics are evoked: Consent and contract, and the data subject's right of access. The confidentiality of electronic communications is discussed secondly, in general and as regards more specifically cookies. Finally, the protection of Internet surfers' computer terminals is approached as regards hacking in general, a specific concern related to cookies being then addressed.

PRIVACY AND DATA PROTECTION

General Discussion

This section examines users' loss of control, users' understanding of privacy, and addressing these concerns from EU and US perspectives. Solove (2002) interestingly pointed out that: "Not all privacy problems are the same and different conceptions of privacy work best in different contexts. Instead of trying to fit new problems into old conceptions, we should seek to understand the special circumstances of a particular problem." Such conceptions of privacy will empower the user to recover some control. (Solove 2002, p. 1147)

European Union

Numerous legal instruments relate to privacy and data protection. The main rules the purpose takes into account are Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR] and the directives 95/46/EC and 2002/58/EC[60]. Without defining privacy – one cannot[61] and others have already studied this concept in depth[62] –, the purpose is focused on a useful understanding of privacy. The latter ensures individuals, using data protection rules, a certain power of control in the context of SNSes. They receive control such as regards their "informational environment" and the "circulation of their image", the processing activities of the data controller being then restricted (Poullet, 2008, p. 41). Privacy, under the view suggested by Y. Poullet and A. Rouvroy, can be defined as the right to "informational self-determination", as identified in 1983 by the German *Bundesverfassungsgerichtshof* (Poullet & Rouvroy, 2009/1, pp. 52-58). According to the authors (2009/1, p. 75), one of the facets of privacy is that we have a certain control over a number of aspects of our personalities that we project to the world.

Data protection can be seen as an evolution of privacy due to the new challenges raised in our information society and the new privacy threats (Poullet, 2008, p. 38). It is aimed at ensuring the respect of privacy (Docquir, 2008, p. 84) – but not only privacy[63] –, and the EHR Court links data protection directly to the human right to have their private and family life respected[64]. As we will see, data protection notably proceeds to the "horizontalization" of privacy. "[D]ata protection and privacy are clearly substantially overlapping concepts" (Walden, 2007, p. 461). But data protection has its own legal regime (Docquir, 2008, p. 86). And "the right to data protection is recognized as an autonomous fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union" (Working Party 29, WP168, p. 5). It provides data subjects with legal means to exercise a control over personal information. It also frames the activities of the data controllers. In this respect, the fundamental purpose[65] and data quality[66] principles, enshrined in directive 95/46/EC, are crucial. And to some extent, they mirror H. Nissembaum's conception of privacy as "contextual integrity" (Dumortier, 2009, p. 13), discussed later. As regards the relations between privacy and data protection, according to P. De Hert and S. Gutwirth (2006, pp. 67-69 and 71-76), privacy could be viewed as an "opacity tool", protecting individuals against public and private actors' interference in their individual matters. While data protection would be a "transparency tool" aimed at compelling these actors to use good practice, focusing on the transparence of their procedures and acts (De Hert & Gutwirth,

2006, pp. 69-70 and 76-82). In this respect, privacy has a prohibitive nature and data protection offers various procedural guarantees, channeling powers to protect the individual's privacy and to promote accountability. Consistent with this model, privacy would restrict the reduction of the control that individuals enjoy as regards personal data. While data protection would determine the terms according to which such reductions could be accepted. As a working rule, we could retain that data protection implements privacy in practical terms, within the context of computing and Internet technologies, arming data subjects with specific subjective rights against data controllers. This partly answers a question that now needs to be briefly addressed, that is, the horizontal effect of Article 8 ECHR. And this also avoids some speculative reflections about what the ECHR could impose on the States as regards the private relations involved in the (contractual) context of SNSes.

The human rights enshrined in the ECHR – and more precisely Article 8 ECHR [67] – can have a horizontal effect[68]. It is also referred to as the German theory of "*Drittwirkung*" ("third party effect of human rights"). Originally human rights only concerned the relations between, on the one hand, individuals, and on the other hand, the State. This is the "vertical effect" of Human rights. Nowadays, it is well established that they also concern interpersonal relations. This is their "horizontal effect." The State has an "obligation to protect human rights" and, in this respect, "to avoid human rights violations by private person" (Nowak, 2003, p. 50). Generally, the horizontal effects of the ECHR are brought in by legislative measures of the Member States of the Council of Europe protecting fundamental rights (data protection rules could be an example as regards Article 8 ECHR, criminal law as regards Articles 2 and 3, etc.). *Before a national Court*, the horizontal effect of the ECHR – or, more generally, of constitutional rights – can manifest itself in two general ways: directly horizontal or indirectly horizontal. And this latter can be subdivided into different subcategories. For instance in the UK, R. Clayton and H. Tomlinson (2001, pp. 204-207 and 223-238) identify five "horizontal" impacts that the Human Rights Act (1998) can have on disputes between private litigants. To sum up, a right of the ECHR has a *direct horizontal effect*[69] when a Court can deduce from the ECHR's pronouncements, the legal effects directly applying to private legal relations. Whereas the same disposition of the ECHR would have an *indirect horizontal effect* if the Court had to rely on previously existing private law applying to the particular case at stake, then construing these rules in the light of the ECHR[70]. For instance, in the UK, the ECHR has an indirect horizontal effect (Clayton & Tomlinson, 2001, pp. 217-218; Phillipson, 1999). This is also the case in Germany, and more or less the case in Belgium, the situation in The Netherlands and in France being less clear (van der Plancke & Van Leuven, 2008, pp. 201-202)[71].

A crucial question is to determine to what extent a State is *obliged* under ECHR to ensure that private relations are compatible with human rights (van der Plancke & Van Leuven, 2008, p. 210) and, in particular as regards the present point, the right to privacy. Horizontal effect is clearly linked with the positive obligations falling to the States. "[P]ositive obligations are a *source* of horizontal effect" (Gardbaum, 2006, p. 770). However, "the actual extent to which the state [(*i.e.* its organs including the Courts[72])] is to protect private persons is highly controversial and unclear in theory and practice as yet" (Nowak, 2003, p. 50). And the States have a margin of appreciation to this end, the proportionality principle also applying[73]. It can here be referred to what is called the "diagonal effect" of the ECHR (Dickson, 1999, pp. 59 and ff.)[74]. In this respect, *the State* can be held responsible by the European Court of Human Rights for the violation of rights enshrined in the ECHR *by private parties* if such a violation is permitted by its *inaction*[75], "by tolerating the occurrence of the prohibited acts" (Meron, 2000, no. 11). And such

inaction could be the fact of *a court* denying, for instance, the right to privacy of an individual vis-à-vis another individual, and failing to remedy a violation of the ECHR. In such case, the violation of the ECHR by an individual could then be only *indirectly* (Zwaak, 2006, p. 29) brought to the European Court of Human Rights, which would give a ruling as regards the state responsibility[76].

A good example arises from the SNSes context – and more generally cloud computing – to illustrate the usefulness of the *judicial* (before a Court) potential of the indirect (or direct) horizontal effect of Article 8 ECHR. Let's take as the premise that the directive 95/46/EC – and its implementation in a particular Member State – does not apply to a particular user subscribing to an SNS, due to a domestic use exemption[77]. In such a case, the European regime related to transborder data flows will then not apply. Though, this user could send personal data concerning other individuals (data subjects) to a foreign State where the facilities – data centers – of the SNS provider are located, no matter if the data protection afforded by this State is or is not adequate. If this provider then processes the data for its own purposes or subsequently discloses the data collected in any way, the "data subjects" could suffer damage, just as the privacy of the subscriber to the SNS himself could be threatened. If it were the case, Article 8 ECHR and its horizontal effect would ensure the protection of the data subjects and the privacy of the user at stake. For instance, in Belgium, a lawsuit could be initiated on the basis of Article 1382 of the Belgian Civil Code (general rule as regards extra-contractual liability) coupled with Article 8 ECHR. In other words, the horizontal effect of Article 8 ECHR could help to fill the gaps in data protection rules in the SNSes – or cloud computing – context, ensuring the data subject the recovery of control.

To sum up, data protection and privacy give the users of SNSes a certain legal control over their personal information, empowering them, to some extent, to prevent or limit what can be done as regards personal data related to them when they are not technically able to do so themselves. And if data protection rules do not apply for any reason, the indirect horizontal effect of Article 8 ECHR could be invoked.

United States of America

Originally in the United States[78], privacy was conceptualized in common law from S. Warren and L. Brandeis's paper (1890). Privacy was identified as the "right to be let alone." Later, it was systematized by W. Prosser, in four privacy torts: Intrusion Upon Seclusion, Appropriation of Name or Likeness, Publicity Given to Private Life (also known as Public Disclosure of Private Facts) and Publicity Placing Person in False Light (Richards & Solove, 2007, pp. 146-156; Dunne, 2009, pp. 195-197)[79]. Among these torts, confirmed in the Second Restatement of Torts, the purpose essentially focuses on the Public Disclosure of Private Facts Tort, preventing the disclosure of data. The torts relate to inter-individual relations. The American federal Constitution enshrines the right to privacy. The Fourth Amendment is notably a cornerstone to this end[80]. Some constitutions of federated States also enshrine the right to privacy. But "the state charters, like the federal constitution, do not regulate interactions among citizens" (Schwartz & Reidenberg, 1996, pp. 9-10). In other words, "[t]he state constitutions emphasize the powers of government and the limits on them, rather than the regulation of relations between citizens" (Schwartz & Reidenberg, 1996, pp. 9-10). They primarily concern relations between States and individuals (vertical effect), requiring a "state action" to apply. Nonetheless, "the development of 'state action' doctrine shows that even where the constitutional rights are defined in vertical terms, the courts will extend constitutional guarantees to some relationships between private individuals" (Clayton & Tomlinson, 2001, p. 208). The American Constitution can in fact be considered to have an indirect horizontal

effect (Gardbaum, 2005, p. 415)[81]. In California for instance, the "constitutional right to informational privacy has been found to apply to both the public and the private sector" (Schwartz & Reidenberg, 1996, pp. 133-134). Referring to the common law (privacy tort) and the Californian Constitution, the Supreme Court of California, in Hernandez v. Hillsides (2009), recently underlined that these "two sources of privacy protection 'are not unrelated' under California law." Citing another decision, the Court recalled that the right to privacy in the California Constitution "creates at least a limited *right of action* against *both private and government* entities"[82] (emphasis added by the author). However that may be, under the American Constitutional system, States do not have any "positive obligations" according to the Constitution (Schwartz & Reidenberg, 1996, p. 35). In this respect, constitutional systems generally reject positive obligations; "like in the United States, are thereby rejecting an important source of indirect horizontal effect", (Gardbaum, 2005, p. 770).

Privacy suffers substantial weaknesses in the context of SNSes. The only one that holds our attention is its dependence on the well-known "reasonable expectation of privacy" [83] [84]. If technological progress sometimes creates such expectations, it often erodes them (Sprague, 2008, p. 89)[85]. The more technologies are used to monitor individuals, the less they have expectations of privacy (Solove, 2002, p. 1142). In the same sense, "[w]ith every click of the mouse on the Internet, the expectation of privacy diminishes and a voyeuristic society expands" (Kane & Delange, 2009, p. 347). Informing individuals about data processing could also have the same pernicious effect[86]. So, a *duty* to inform could, in this respect, be problematic. "The problem [...] is that [the] protection [of privacy] dissipates as technology develops and enters general public use" (Sprague, 2008, p. 121). In other words, "[e]xpectations of privacy are established by social norms" (Sprague, 2008, p. 129)[87]. In City of Ontario v. Quon (2010), the US Supreme Court did not hesitate, recently, to watch for the setting of these social norms before deciding on the question of reasonable expectation in the context of work and communication technologies[88]. It explicitly avoided the discussion. And M. Zuckerberg claiming that "privacy is no longer a 'social norm'" (EPIC v. Facebook 2, 2010, no. 10) might be accepted.

Because of the necessity of a reasonable expectation of privacy, what is "knowingly exposed to the public" is not protected (Sprague, 2008, p. 125)[89]. So "there will be no cause of action if [the plaintiff] happened to reveal this information in cyberspace often regarded as public" (Purtova, 2009, p. 511). And yet, as we wrote above, the sharing of data – personal and otherwise – is at the core of SNSes. As an example, the U.S. Court of Appeals for the Ninth Circuit held, in USA v. Forrester (2007), that there is no reasonable expectation of privacy as regards "Internet Protocol ("IP") addresses of the websites the defendant visited", "and the total volume of data transmitted to and from the defendant's account"[90]. This reasoning has also already been transposed in the context of "electronic bulletin boards" where data are delivered to a huge number of users:

In Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2007), we concluded that users of electronic bulletin boards lacked an expectation of privacy in material posted on the bulletin board, as such materials were "intended for publication or public posting." Of course the public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients. (Steven Warshack v. USA, 2007) (Emphasis added by author).

Anyway, users have reasonable expectations of privacy as regards the content of their emails and email accounts, as it is illustrated by Steven Warshack v. USA (2007). So, useless to say that choosing privacy settings is a minimum a user *has to* do if he/she hopes to be protected.

So what place is left for privacy in SNSes? SNS providers and users seem to have a great deal of latitude with the personal data they can access. However, Warren and Brandeis (1980, p. 198) have already argued that "common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." And the US Supreme Court judged that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person" (U.S. Dept. of Justice v. Reporters Committee, 1989). "[I]nformation privacy" was thus already anticipated in the oldest American conceptualization of privacy. "Information privacy is 'an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed, and used'" (Kang, 1998, p. 1205, quoting the Principles for Providing and Using Personal Information produced by the Clinton administration's Information Infrastructure Task Force)[91].

Does American data protection fill the gap we identified? Its application is sectoral[92] and a general statute law related to "commercial data brokers"[93] – or the profiling industry – and "behavioral advertising"[94] is lacking. It can be pointed out incidentally, that the private sector is supposed to be virtuous when self-regulating. "Self-regulation, after all, is simply the ability to decide for oneself what the term 'reasonable' means" (Killingsworth, 1999, p. 71)[95]. That contrasts sharply with EU perspective where mandatory rules generally apply[96]. Therefore, "e-socialization" is regulated through privacy policies. These policies are mandatory under the Safe Harbor Principles[97] [SHP] and, sometimes, under State law[98]. But it has to be underlined that, more generally, different elements "have all recently converged to create a new environment in which implementing a privacy policy is a business necessity for most, and legally advisable for all" (Killingsworth, 1999, p. 59). Unfortunately, they suffer from vagueness as regards SNSes[99], and even as regards the Web more generally[100].

Commercial practices are also framed by FTC enforcement actions against unfair or deceptive practices within/or affecting commerce[101] which leads to a "growing 'common law' of privacy" (UCBSI, 2010, p. 10)[102]. As regards SNSes, Twitter has already had to deal with the FTC (In the Matter of Twitter Inc., FTC, 2010), as Facebook might do in the context of the EPIC et al. complaints (EPIC v. Facebook 1, 2 & 3, 2009, 2010). Finally, even if the SHP, (their weaknesses put aside) incorporate a limited "system of consumer control" (Manny, 2003, p. 6), these only relate to personal data coming from EU.

WHAT HELP CAN BE FOUND TODAY?

The concept of "limited privacy" could help. According to L. Strahilevitz (2004, p. 18),

Limited privacy" is the idea that when an individual reveals private information about themselves to one or more people, they may retain a reasonable expectation that the recipients of the information will not disseminate it further. (Strahilevitz, 2004, pp. 18-22).

An "expectation of limited privacy" would then be at stake. The prime example quoted by the L. Strahilevitz (2004, pp. 18-22) in this respect, in California, is based on the intrusion upon seclusion tort, other cases involving the public disclosure of private facts tort. But the courts unfortunately not necessarily accept it (Strahilevitz, 2004, pp. 22-25).

Some researchers have suggested remedies as regards privacy and data protection. One would be to create a specific "model of propertized personal information" that constitutes a "hybrid inalienability" model (Schwartz, 2004). Another solution would be to adapt trade secrecy default

rules "to the licensing of personal information" (Samuelson, 2000). Still another way would be to rely on a dynamic theory of informational privacy, being an "autonomy-based approach to data privacy protection" focusing on the meaningful autonomy of the individual (Cohen, 2000). According to L. Strahilevitz (2004), a possibility would result in defining reasonable expectations of privacy according to the "Social Network Theory" (Strahilevitz, 2004). Privacy would then depend on people to whom the data have been communicated.

Next to these interesting propositions, two other solutions seem particularly relevant in the context of SNSes. As a new "path" to take to enhance users' privacy protection, American common law and English common law could be linked (Richards & Solove, 2007, pp. 156-158). The English common law focused on the development of the breach of confidentiality[103] tort – highlighted by Warren, Brandeis and Prosser. Indeed, this latter tort takes into account the "limited purpose" for which data have communicated to third-parties, focusing on the "nature of the relationship" at stake, in spite of the "nature of the information" which has a main role as regards the American privacy tort. An "expectation of trust" would be protected (Richards & Solove, 2007, pp. 174-175). In this respect, it could be helpful to give the users of an SNS the ability to construct their own privacy policy they could contractually oppose other users when they access their profiles. For instance, before viewing the profile of a user – or before becoming a friend of this user –, another user could have to accept a preliminary page, clicking "I accept" and concluding a clickwrap contract with the user whose profile is going to be consulted. Such a privacy policy could also be opposed to applications developers, etc. However, to this aim, SNS providers would have to modify the software they offer. Another concern would then arise, that is to say: how far such contract could go as regards limitations to the freedom of expression of the user consulting the profile[104]?

The theory of H. Nissenbaum (2004), conceptualizing privacy as "contextual integrity", seems also particularly relevant concerning SNSes. According to her, privacy would ensure individuals a right to maintain the contextual integrity of the information at stake[105]. In this same sense, F. Dumortier (2009, p. 15) underlines that "European authorities could impose less multi-contextual content for SNSes by demanding the operators of such sites to limit their architecture in accordance with each user's specific intents." Both theories fit best the cases of "meta-SNS" like Facebook, where lots of contexts intertwine and when the service is offered with the so highly praised opportunity for users to control information related to them[106] – though it is still requested.

It is interesting to note that, to some extent, both theories focus on the *purpose* of the communication of data. Like the European general data protection directive 95/46/EC enshrines the fundamental purpose principle of the processing.

However, whatever theory is chosen to overstep the classically required reasonable expectation of privacy, concerns remain. On Facebook-like SNSes, the "misleading notion[s] of "community"" and "friends" (IWGDPT, 2008, p. 2) are "nebulous at best" (Kane & Delange, 2009, p. 319). Indeed, "OSNs have loosened traditional notions of intimacy and friendship and their respective nomenclature" (Levin & Sánchez Abril, 2009, p. 1018). This remains a practical hurdle to better privacy. This is all the truer when third-party applications are able to extract personal data from SNS databases. We conclude finally with N. Purtova (2009, p. 514), that "*the current* US data protection law offers virtually no tools to return control of personal data to individuals" (emphasis added by author). But it is necessary to add that a positive evolution could occur thanks to privacy scholars and civil liberties associations. And this would necessarily be through statute law or through a groundbreaking case-law.

SPECIFIC TOPICS

To confront SNSes with data protection and privacy does constitute a huge task. Therefore, this section focuses on two relevant concerns relating to data protection: Consent and contract, and the right to access. We discussed elsewhere the material applicability of directive 95/46/EC to SNSes providers, and take as a premise that it applies[107].

Consent and Contract

The Trade of Personal Data: Without explaining further the issues raised by the conclusion of a contract between SNS providers and their users – this was seen previously[108] –, a meeting of the SNS user's and SNS provider's minds can occur. Indeed, the former adheres to the latter's offer of a contract of adhesion[109]. This contract seems to be the place where, and above all the *means* by which, consent is given by data subjects – users of the SNS – to the SNS provider's processing of personal data related to them[110]. The economy of the proposed deal looks straightforward: "Let me process your data in order to deliver and target advertisements, I'll give you a "free" access to my network and I'll delete the data if you delete your account." Or, following a worst-case scenario, "let me do what I wish with your data (including selling it to data brokers, government agencies, potential employers, etc.), I'll give you access to my network that I can deny for any reason, and I reserve the right to keep your data even if you deactivate your account"[111].

In other words, using an SNS could lead to consent to the sale of personal data. It is well known that "[i]ntangible information has become a basic asset, the fuel driving the "Information Economy", and personal data comprises a substantial share of such information assets" (Walden, 2007, p. 459). Advertisements and behavioral advertisements – notably having recourse to the use of cookies and web beacons – drive a significant part of the web industry. This use of, for instance, cookies, is so common that, according to P. Polański (2007, p. 323), it could join the ranks of Internet customs[112]. Answering a complaint directed against Facebook, the Assistant Privacy Commissioner of Canada has recognized that, "[o]ur views with respect to advertising have adapted to the social networking site business model. We have accepted that a certain amount of advertising is something users have to agree to since use of the site is free and the company needs to generate revenue." (Denham, 2009, no.14)[113]

The very question is how far the freedom of contract can go. How to market personal data if one accepts that it can be marketed? Since one's image can be exploited[114], what about other personal data[115]? The answer lies between two extremes defining how one perceives personal data: "Ordinary commodity" or "absolute intangibility"[116]. A median path should be found *in concreto*, taking into account the place afforded by data protection to consent, the different subjective elements and the interest of the collectivity. In this respect, perceptions can vary significantly. Some think that "[t]he sanctity of personality is inconsistent with selling privacy in the marketplace, for baubles", and others not concerned about, "transform themselves into commercialized entertainment packages to satisfy their own exhibitionism and other people's voyeurism" (Kang & Buchner, 2004, p. 230). Taking Facebook as an example, if targeted advertising is necessary to the economic viability of the SNS – without any doubt, a valuable service for its users –, and limited to the possibility, for companies, to select some criteria to define an audience, without any access to personal data and any other transfer of personal data[117], this seems acceptable.

However that may be, beyond the "privacy prohibiting limits"[118], such marketing needs to be led according to data protection rules. Because data protection rules pertain to public order, they restrict the parties' autonomy. According to Belgian contract law, if the contract between the SNS provider and its user has an effect of creating

or maintaining a processing operation contrary to these rules, it is void[119]. It is true that consent has a limited value as legitimate ground for data processing (Poullet & Rouvroy, 2009/1, pp. 72-74). Anyway, as far as SNS providers recourse to the data subject's consent, this consent has to be a "freely given, specific and informed indication of his wishes" (Article 2, h) Directive 95/46/EC). It has to be "unambiguously given" (Article 7 a) Directive 1995/46/EC). A *qualified* consent is required. Moreover and notably, it can only relate to processing aimed at "specified, explicit and legitimate purposes" (Article 6.1, b) Directive 95/46/EC), and involving "adequate, relevant and non excessive data" (Article 6.1, c) Directive 95/46/EC) in relation to the purposes of the processing, data which can only be kept "for no longer than is necessary" for these purposes (Article 6.1, e) of directive 95/46/EC). This "qualified" consent is also limited as regards its objective[120]. The purpose next only focuses on the fact that consent is *qualified*, that is to say: Informed, specific and free. This latter point also directly echoes with our brief analysis of the SNS market.

A Qualified Consent: Consent has to be *informed*. SNSes and cloud computing technologies can seem impenetrable – where are the data?[121] While the purposes of the processing have to be specified and explicit. As far as targeted advertisements are concerned, better information is needed as E. Denham pointed it out (2009, nos. 134 and 139)[122]. It has been noted however above that privacy policies are usually vague, which is incompatible with directive 95/46/EC. Explanatory screens related to data protection – how privacy settings work?; what data are processed for which purposes?, etc. – could be of help before the user subscribes to an SNS. Although Facebook has already answered that such a process would dissuade web surfers from joining the network (Denham, 2009, no. 66). As E. Denham (2009, nos. 13 and 51) suggested, a real time information process, anterior to the processing of any personal data, could be useful. In cases like Facebook, the function of the API Platform has to be clearly explained to users. Indeed, personal data can be retrieved via such a platform; any developer of applications could be located anywhere in the world. This reinforces the density (complexity) and opacity of the "SNS cloud" at stake. Users should know where their personal information is or at least, where it *may be* processed (stored, made available, etc.)[123]. Moreover, no matter where data are collected (from the data subject or a third-party) information duties enshrined in directive 95/46/EC should have to be fulfilled *before* any contract is concluded[124]. This may be crucial due to the practice of clickwrap and browsewrap contracts. Such information is decisive as regards the will to enter into a contract and to use the service.

Consent has also to be *specific*. As regards SNSes, it is given, notably, when the user subscribes to the service and creates an account, clicking on "Create my account", "I accept" or similar formulations. When he clicks, he is considered to consent to terms of use and the privacy policy[125]. Firstly, consent can only target specific processing operations. Data subjects cannot concede a "thematic general power" to process personal data. "Consent in bulk for any future processing without knowing the circumstances surrounding the processing cannot be valid consent" (WP171, 2010, p. 14). Consent must be "limited." Secondly, and although consent to the processing of personal data is clearly linked with the concluded contract between the user and the SNS provider, it should be technically dissociated from the expression of the "blanket assent" to the general terms of use and privacy policy of the SNS in question[126]. It is here referred to about how consumers conclude (e-)contracts. " 'Blanket assent' is best understood to mean that, although consumers do not read standard terms, so long as their formal presentation and substance are reasonable, consumers comprehend the existence of the terms and agree to be bound to them" (Hillman & Rachlinski, 2001, pp. 33-34). " 'Blanket assent' means only that, given the realities of mass-market contracting, the con-

sumer chooses to enter a transaction that includes a package of reasonable, albeit mostly unfavorable to her, boilerplate terms" (Hillman & Rachlinski, 2001, pp. 33-34). In another but similar context, Working Party 29 declared itself in favor of such a procedural dissociation (WP115, 2005, p. 5)[127]. "[C]onsent means active participation of the data subject prior to the collection and processing of data" (Working Party 29, WP171, 2010, p. 15). It is not tacit acquiescence. And in the United States, the FTC (In the matter of Sears, 2009) might deem, in some particular cases, that the practice of a company is deceptive when it promotes its business without informing users *before they consent* to any terms of use and privacy policy, and outside these documents, about their practices related to personal data processing[128]. Irrespective of the fact that the processing occurs later, after that the individual has expressed consent.

The data subject's will, must finally be freely given. As stated O. De Schutter, studying the renunciation to fundamental rights, what is suspicious in a particular deal, is the commercial exploitation ("*marchandisation*") of the right at stake, specific constraints arising from trade banking on the individuals' needs (De Schutter, 2005, p. 457). Individuals' behaviors are dictated by their need of a material advantage or by financial incentives (De Schutter, 2005, p. 463). In the SNSes context, for instance, "the introduction of a fee should be considered as an additional option at the choice of the user for financing the service instead of the use of profile data for marketing" (IWGDPT, 2008, pp. 6-7). This is possible with LiveJournal[129]. But it has to be kept into mind that, "the interest in privacy is like the interest in receiving access to the electoral franchise, clean air, or national defense: it should not depend on socioeconomic status" (Schwartz, 2004, p. 2086). Behind any doubt, competition within the SNS market is relevant and could be decisive in regards to commercial use of personal data. If a user has no real choice, his consent is not free. With no possible alternative, the user can only accept to use the offered technology (SNS) or reject it. This directly refers to the short analysis of the SNSes market suggested above. It is impossible here to go into economic details of the "meta-SNS" market. It can only be emphasized that the history of Facebook shows that this latter has acted relatively independently from its customers – having then seemed to be dominant –, modifying the website, the privacy policies and the terms of use several times[130]. However, it cannot be denied that users' (often represented by American civil liberties unions) protests have also influenced the website and its policy. The intervention of public authorities has also had the same effect. Practically, the combination of both interventions had effect. Although "dominance is fleeting" (Evans, 2008, p. 17) in such markets, the KnowPrivacy (UCBSI, 2010, pp. 11-12) study underlined, as regards web privacy in general, that "there is not enough market differentiation for users to make informed choices [...; b]ecause [privacy policies] are all equally poor, users have no viable alternatives. This is a *market failure*" (emphasis added by the author). And "the argument that users should simply avoid certain websites is unrealistic [; m]ore and more of our social and political discourse is taking place on these popular websites" (UCBSI, 2010, p. 31) where we are unceasingly urged to be. So it has to be emphasized that consent expressed in the use of SNSes is often not free.

This is all the truer when the SNS provider proceeds to unilateral modifications to the privacy settings – or functionalities – of the network that have to be accepted if the user wants to continue using the network in the same way. This occurred several times as regards Facebook[131]. In such cases, if the user as no other alternative than leaving the network if he does not agree to changes, his consent is not free. Direct or indirect (through the evolution of the service) modifications of privacy settings restricting the original panel of choices the user could make are forbidden by data protection rules. With the exception that if the further processing implied by the modification is com-

patible with the original processing, which is not the case when the *degree* of accessibility to users' personal data over an SNS is increased. Indeed, if a user originally can limit the accessibility to such data, he cannot reasonably expect that such fundamental characteristic of the offered service will later be modified. Another exception is if the processing is based otherwise than on the data subject's consent. An archetype of such forbidden evolution of privacy settings would precisely be to consider as public information, information whose access to could originally be restricted by users.

Conclusion and Thoughts About the Safe Harbor Principles

Keeping the previous points in mind, it can be argued that an SNS provider like Facebook, as a data controller, often cannot legally rely on the consent of its users to process personal data related to them. Users are not clearly and willingly informed, their consent is usually non specific, and not free enough. Of course, it is impossible to suggest a conclusion as regards every possible case. Each processing operation requires particular study. And if consent is void, however, this does not mean that the processing involved is illegal for this reason. Indeed, their legitimacy can be founded on, for instance, Article 7, f) of directive 95/46/EC[132].

Across the Atlantic, Facebook and LinkedIn have adhered to the SHP[133]. According to the choice principle of the SHP, an SNS provider has to inform (European) data subjects "about the purposes for which it collects and uses information about them." What it does when they decide to access the offered service, therefore consenting to the processing operations at stake. Under SHP, a *qualified* consent is not required. In this respect and without an in-depth analysis, SHP does not directly seem to permit the aforementioned reasoning.

DATA SUBJECT'S RIGHT OF ACCESS

Article 12 of Directive 95/46/EC grants to every data subject "three fundamental rights" (Leberton, 2009, p. 320)[134] relating to the personal data processing at stake and towards the data controller: A right of access, a right of rectification and a right of erasure or blocking. These rights constitute a legal means afforded to data subjects against the previously mentioned lack of control they suffer in the SNS context. They are equipped against unlawful processing of personal data concerning them. They can seek out who is processing the data (the SNS provider, another user[135] (application developer or anyone else) or a third-party to the network), claiming the deletion of the data at stake if the data are conserved for too long a period of time, depending on the purposes of the processing (e.g. if the SNS provider keeps a user's data after this latter has chosen to delete his account). If the "average" user of an SNS falls within the scope of directive 95/46/EC – which is not necessarily the case[136] –, it has to be noted however that the right of access of the data subject could conflict with his right to the confidentiality of his electronic communications[137] and, as may be the case, with his right to the secrecy of his correspondence. But these concerns are not addressed here.

According to directive 95/46/EC (Article 12, a)), the data subject has a right to be informed, by the controller, about the recipients (or categories of recipients) to whom the data are and *have been* disclosed or communicated. The European Court of justice has recently ruled that, to ensure the aforementioned rights (rectification, erasure and blocking), the right of access must of necessity *relate to the past*. If that were not the case, the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered." (College van burgemeester en

wethouders van Rotterdam v. M.E.E. Rijkeboer 2009, no. 54) (Emphasis added by author.)

Needless to say, the right of access is a cornerstone of data protection as regards the transparency of processing operations and the effectiveness of data protection rules – that is to say, of data subjects' control over personal data. Thus, as a rule, SNS providers would have to store information about people who have had access to personal data related to their users physical persons[138], when they have been involved in such transfers as data controllers. Admittedly, as far as the past is concerned, the right of access can be limited. Limiting it, different factors can be taken into account: The possible exercise of the aforementioned rights implies an appreciation of: the length of time the personal data are to be stored; the obligation following from Article 6 (e); the more or less sensitive nature of the data; the risks represented by the processing; the number of recipients; and, finally, the burden (having regard to the state of the art and the cost of their implementation) that such a storage represent for the data controller (College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer 2009, nos 57-59)[139]. A balance has to be struck[140]. So to some extent, this fundamental right of access empowers the data subject to "track" the personal data related to them in and outside an SNS.

In the US, how the right of access has been enacted by the SHP can be deplored. Indeed, it is indirectly dependent on American privacy regulation:

[I]ndividuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated. (Access Principle and FAQ no. 8)[141] *(Emphasis added by author.)*

Moreover, it must be noted that "U.S. law will apply to questions of interpretation and compliance with the SHP." Therefore, if there is no risk for the individual's privacy, it is tempting to conclude that any burden supported by the data controller would be disproportionate. And as it has been mentioned above, in the SNS context, American courts could deem that the user of an SNS cannot have a reasonable expectation of privacy[142] – or reasonable expectation for "limited privacy." His privacy will thus not be threatened. Therefore, following American law, the right of access enshrined in the SHP could have shrunk to virtually nothing in the SNSes context.

It is finally of great interest, as the study KnowPrivacy – based on the fifty most consulted websites in the United States at the time of the study – has shown, to mention the sharing of information between affiliates (here, the SNS provider and its affiliated companies). Such sharing is usually foreseen in the privacy policies of websites. The study emphasized in this respect that "[b]ased on our experience, it appears that users have no practical way of knowing with whom their data will be shared" (UCBSI, 2009, p. 28) – what the European right of access can do. It notably underlined that "MySpace, one of the most popular social networking sites (especially among younger users), is owned by NewsCorp, which has over 1500 subsidiaries" (UCBSI, 2009, p. 28)[143]. And the study did not include "subsidiaries of subsidiaries." The European right of access could be especially useful and helpful to identify if such sharing of personal data occurred. It would also be useful if the SNS provider and the application developers were deemed to be joint controllers of the processing involved by the applications. As regards Facebook, is the pure creation of a platform permitting the access by an application to the data of the users who accept this application enough to make of Facebook and the developer joint controllers? If Facebook *compels the users* (technically or by contract) to share a minimum of information with such an application – i.e.

through the platform –, to be able to use it – and other application, making the access to the API Platform functionality conditional to the sharing of personal data –, it is a co-controller at least as regards these data. What about if Facebook does not compel users to share any personal information, the application developer having to require a specific authorization of the users adding his application? In this case, Facebook would seem not to be a data controller. When applications can access to data of an SNS, the question of joint control will depend on the particular functioning of the platform at stake and is crucial as regards the applicability of data protection rules. Anyway, if the SNS provider and an application developer were deemed joint controllers, they would be both compelled to monitor the applications. For instance, they would store a "log" of the personal data these applications accessed. And if the SNS provider is able to store the clickstream of its average users, it should be able to record this "access stream."

CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS

This section tries to identify in European (III.2.1.) and American (III.2.2) law, which communications are protected and when under the confidentiality of electronic communications protected by both laws.

European Law

According to Article 5.1 of directive 2002/58/EC, Member States have to ensure the confidentiality of electronic communications – exceptions of course existing[144]. This "e-Privacy" directive applies "to the *processing of personal data* in connection with the provision of *publicly available electronic communications services* in *public communications networks* in the Community"[145] (Article 3.1 of directive 2002/58/EC) (emphasis added by author). If the material scope of the directive[146] is circumscribed in such a manner, some of its dispositions nonetheless apply beyond, such as Articles 5.1, 5.3 and 13[147]. As regards the confidentiality of communications, the protected communications must be realized by means "of a public communications network and publicly available electronic communications services." Both concepts are defined by directive 2002/21/EC (Article 2, d) and c)) which definitions apply as regards directive 2002/58/EC (Article 2). To be public, the network and the electronic communication services have to be "available to all members of the public on the same basis" (EC Communication, 1998), "as opposed to use in a private or corporate network" (EC staff working document, 2004, no. 4.2); the Directive 2002/58/EC "focuses on public electronic communications networks and services, and does not apply to closed user groups and corporate networks" (Recital 55 of directive 2009/136/EC).

To apply the above-mentioned rule in the context of SNSes firstly requires identifying which electronic communication services and public networks are at stake. In this respect, our little knowledge of computers science inevitably limits the scope of the discussion. Secondly, the communications that are protected under directive 2002/58/EC are specified. And thirdly, the implementation of the latter directive in Belgian law is confronted to the analysis.

Electronic Communications Service(s) and Network(s)

When an individual uses an SNS, he first connects to and uses the Internet – a "public communications network" [PCN][148] – with his computer[149] through his own Internet access provider – a classical "electronic communications service" [ECS][150] provider[151]. By these means, he is able to use the software (as a service) provided by the SNS provider. He clicks on the relevant buttons and writes messages or selects files in the

relevant fields to make the application work and do what it is expected to do (send a message, join a group, chat, share a video, modify a birth date, change privacy settings, etc.). For instance, he writes a message in a specific field, selects the names of the contact (or friend) he wants to write to, and then clicks on "send." According to the terminology of the Working Party 29, the SNS provider would be its own Internet Service Provider[152] when it hosts the social network (the application and its web interface – the website) and users' data (there profile, what they share, etc.), and replies to users' requests (WP37, 2001, p. 24). It provides content: the application and its web interface connected to a giant database. The content broadcasted in the relevant fields of the Website constantly changes according to users' wishes, these latter being able to share and access to others' information through a framework designed by the SNS provider. Design which is more or less modifiable by members depending on the SNS[153], and can therefore also change. Finally, we assume that the SNS provider most probably subscribes to an Internet access service which enables him to connect to and make available its website on the Internet.

However, could *the SNS provider himself* be considered as the provider of an ECS (the SNS)? Or, even as a PCN provider (the technical infrastructure necessary for the working of the SNS)?

What is central in regards to the qualification as an ECS is "the *conveyance* of signals on *electronic communications network* [CN[154]]" (emphasis added by author). This is, for instance, clearly done by an Internet access provider [IAP] (the one of the SNS provider, and the one of the user at stake). The definition is neutral from a technological viewpoint[155], and the IAP is the archetype of the ECS provider in the context of Internet. An SNS provider should most probably operate an electronic communications network [CN] in the sense of directive 2002/21/CE – which provides a large definition[156]. Indeed, it should have (or at least rent[157]) computers, computers servers, switches and routers linked with cables, maybe at one place in the world or maybe at different interconnected via the Internet locations in the world. As private companies, for instance, have sometimes their own private network. These facilities are used to provide the SNS website, to answer users' requests, to store users' data and make them available, etc. However, it is true that the "computers" used by the SNS providers to offer its service could be deemed not to constitute a CN under the definition of Directive 2002/21/EC. It would only be considered as equipment[158]. In such a case, it would then be clear that the SNS provider could not be a PCN provider, since it would even not operate a CN. And hearing that the network at stake would then be the Internet, the IAPes would be the only ECS providers, because they would be the only ones to *convey* data on the PCN at stake. The exchange of information between users permitted by the SNS provider on its own computers and database would then happen outside any CN.

If it is taken as premise that the SNS provider operates his own CN, which seems correct in technique, it conveys signals on this particular network to answer users' requests and give them the web pages with content they asked. These web pages are the visible lay out of the SNS and its functionalities. In this perspective, the SNS provider would seem to provide an ECS. However, services providing, or exercising editorial control over, *content* transmitted using CN – *e.g.* Internet – and ECS – *e.g.* Internet access – are explicitly excluded from the definition of ECS; Information society services which do not consist *wholly or mainly* in the conveyance of signals on CN are not ECS (Article 2, c), of directive 2002/21/EC). In other words, directive 2002/21/EC "does not cover services such as broadcast content, or electronic commerce services" (Proposal for a Directive on a common regulatory framework for electronic communications networks and service, 2000). The recital 10 of Directive 2002/21/EC specifies that the "provision of web-based content" is not

covered by this Directive. And in our view, it can be considered that the SNS provider mainly provides *content*: an application giving access to a wide database through a website with different functionalities. Therefore, the SNS provider is not an ECS provider. And the SNS is not an ECS. The *conveyance* evoked above is nothing else than an *incidental* activity necessary to deliver the content asked by users of the SNS. With other words, the service provided by the SNS provider do not consist mainly in the conveyance of signals, which processing operations are only incidental due to the fact that the SNS provider hosts and operate himself its website[159]. A web hosting service provider could to the contrary be an ECS because its main activity would consist in the conveyance of signals. Its task is to answer and send the right pages requested by users, not to provide any specific content of his own. Taking as a premise that the SNS is not an ECS, the CN of the SNS provider could neither be considered as a PCN because it would not be mainly used for the provision of ECSes. And the only one ECS-PCN layer that exists in the context of SNSes is the IAPes-Internet one.

However, the Working Party 29 (WP148, p. 12) has already considered that "publicly accessible email service" is an electronic communication service, and Recital 10 of Directive 2002/21/EC underlined that "voice telephony and electronic mail *conveyance* services are covered by this Directive" (emphasis added by author), while the provision of "web-based content" is not. In our view, this reasoning cannot apply to webmail or "webmail-like" services such as the "send a message" functionality that SNSes, such as Facebook, could offer, or such as different forums over the Web. Indeed, in the same sense as above, a Webmail service would not constitute an ECS because what is provided is mainly content: an application offering people the possibility to communicate through mails and back up these latter. It is clear that both services, Webmail and SNS, permit the exchange of information between their users, but technically, data packets are in principle conveyed on the Internet by the IAPes, and that is on this conveyance that directive 2002/21/EC focus. The fact that the provided service has an *interpersonal communicative ambit* (webmails and even SNSes and Forums) does not prevent that content is offered, relying on the IAPes conveyance services to finally deliver webpages to users. In this respect, it does not matter that an application can retrieve data from the databases at stake[160].

To sum up, in our view, the SNS provider is considered not to operate a CN, and then only the IAPes provide a conveyance service over the Internet. Or, the SNS is considered to operate a CN; however, does not offer an ECS because the offered service consists mainly in offering content. And the reasoning is coherent despite the interpersonal communicative ambit of SNSes which will be nonetheless taken into account as regards the protected communications. Not to consider SNSes provider as ECS and/or PCN providers is not without consequences as regards, of course, telecom regulation, but also, data retention duties[161]. As regards the SNS context and directive 2002/58/EC, the publicly available ECS and CN at stake are Internet access services and the Internet. To some extent, this view reflects the reasoning held by the Austrian Regulatory Authority for Broadcasting and Telecommunications ([ARABT], 2005, p. 5) as regards voice over IP[162]. The protected communications have now to be identified.

Protected Communications under Directive 2002/58/EC

Directive 2002/58/EC provides that Member States "shall prohibit listening, tapping, storage or other kinds of interception or surveillance of *communications and the related traffic data* by persons other than users, without the consent of the users concerned" (Article 5.1 of directive 2002/58/EC) (emphasis added by author). A communication is "any information *exchanged or*

conveyed between a *finite number of parties* by means of a *publicly available electronic communications service*" (Article 2, al. 2, d) of directive 2002/58/EC) (emphasis added by author). Such a communication (its content and its traffic data) is protected to ensure the respect of fundamental rights as recalled by Recitals 2 and 3 of directive 2002/58/EC[163]. In this respect, the interpersonal communicative ambit or function of the service provided by the SNSes is relevant, contrary to what has been suggested as regards the qualification as an ECS.

To identify which pieces of information are protected and in the context of SNSes; it is taken as a point of departure that a user wants to share data (text, image, sound or video) with other users of the SNS. To be protected, a communication needs to satisfy a technical criterion – the means by which it is exchanged –, and an "audience" one – who are pieces of information intended to? In our view, the appreciation of these criterions can vary according to the fact that the communication is in transmission or is, after the transmission, in storage in the SNS. Any piece of information exchanged between SNS users is conveyed through the Internet *and* subsequently, via the SNS provider through its own facilities[164].

During a first stage, as already noted, information users want to share on SNSes are conveyed by IAPes, through the Internet, to the SNS provider. Any communication arising in this first *transmission* stage between the SNS provider and the SNS user is exchanged between those two parties and protected against any interference of a third party. But data are not directly conveyed *between users* by their IAPes, since the SNS is always a necessary intermediary mean to access such data[165]. The other user who is addressee has also to use his own IA service to be able to connect to Facebook and retrieve data. In other words, when data are exchanged between users of an SNS, the above-mentioned first stage of communication occurs for each user: then sender and the recipient both use their IA to connect to the SNS an use its functionalities.

Data are, during a second stage, *stored* by the SNS provider who makes them available according to the privacy settings or the functionality of the SNS chosen by users[166]. Here, it is not clear if the protection afforded by Article 5 of directive 2002/58/EC goes further than the first *transmission* stage identified above. It neither provides that it doesn't apply *after* the transmission of the communication. In our view, some communications should remain protected after their transmission through the Internet. Specifically, users who first conveyed to the SNS provider are intended *to a finite number of users of the SNS* and stored on the SNS provider servers. In regards to these communications, the SNS works as a "technical storage" necessary to the conveyance of data between SNS users. Without the SNS provider, there is no communication. So, if during a first stage data are transmitted to the SNS, it usually occurs for a "technical storage" purpose. Information is generally not intended to SNSes provider[167]. And in our view, even when communications are conserved as back up by their parties, they could nonetheless remain protected under Directive 2002/58/EC. Even if it is true that the prohibition of hacking will protect stored information, the confidentiality of communications affords to users' protection of their communications vis-à-vis the SNSes providers and, as the case may be, vis-à-vis application developers and other users who are authorized to access the computers at stake[168]. Users usually let their communications stored somewhere, either for their ongoing transmission, either for pure convenience as backup. For example, in regards to web mail, users may wish to save their mails as backup on the servers of the webmail (which usually is a default option): Even if users bring them back to their computers using web mail software (i.e., Microsoft Outlook or Apple Mail). Users also sometimes act this way to be able to consult these mails everywhere in the world. Not to protect such stored communication

would risk ruining the confidentiality of electronic communications, limiting this latter to a very short first transmission stage.

Taking Facebook as an example, the purpose can be illustrated and some nuances can be brought. The electronic communications involved by the use of the "send a message" (to one or more friends) functionality of the SNS are clearly protected. Even after messages are not deleted by users having received and saw them, they should also remain protected. Indeed, either they are kept for back up reason, either for ongoing discussion because it works as a kind of "recording chat." Instant messaging conversations are also protected (they can be made between two friends). As it would also be the case of the chat (or "video chat") communications on "Chatroulette" for instance[169]. Invitations to events sent to a limited number of friends are also protected. The list of webpages *visited* by a Facebook user, would these pages be profiles, Facebook pages or groups, is also generally protected. Indeed, the subjacent communications only occur between the user at stake and Facebook[170] – the requests are only intended to Facebook. In all these instances, the addressee of the pieces of information are limited and do not fluctuate.

To the contrary, wall posts and data shared on the SNS with all the users of the SNS – or even any web surfer when the relevant data are publicly available from the web –, are not protected communications[171]. Admittedly, strictly speaking, the number of members of an SNS is *finite*. Nonetheless, if *anybody can join* an SNS (just as in the case of Facebook), data which are available to the whole community are clearly public. It would then be excessive to consider that such a sharing involve protected electronic communications. The audience of the network is *fluctuating* between an unrealistic minimum of two users (if we take as a premise that a communication occurs) and a maximum of nearly the whole world...

But what about information exchanged through private groups, and restricted access profiles or parts of such profiles (*e.g.* Walls)? For example, on Facebook, a group can be "open", "closed" or "secret." Open, a group is public. Anybody can join and consult the discussion board, the group's Wall, etc. In such a case, to join a group doesn't involve a protected electronic communication, as it is the case of posting text, images, etc. However, the pure information resulting in the *consultation* of the group's wall, discussion board, etc., remains a protected communication because it is only exchanged with Facebook. If a group is closed, only members approved by the administrators of the group can see the discussion board and the wall and join it. However, the group description is visible by non members, while what is shared through the pages of the group is not. Finally, if the group is secret, it doesn't appear in the members' profiles, or in the search results of the SNS. An invitation has to be sent to the potential future member. As regards profiles, the accessibility to data can also be limited, when the wall of a user is restricted to his friends or to a particular list of friends. In such context, communications seems to appear between a finite number of parties, and *a priori,* it could arguably be considered that the confidentiality of electronic communications applies.

However, how to take into account the fact that a group, a part of a profile, or any other part of the network, can be restricted to *selected* members but nonetheless *numerous* members *and of different contexts* (work, sport, education, sexuality, etc.) and whose number is *fluctuating*? In our view, if in fact, access to the particular part of the profile, to the group, etc., at stake is systematically given to the general public on the same basis[172], or given to a lot of people from really different contexts[173] or, more generally, fluctuating, it can then be argued that the communications at stake are not protected. Indeed, in these cases, the communication has an *indeterminate* or *irrelevant* audience which composition is *fluctuating*. Even if this audience, at a certain times share pieces of information, it is a *finite* sharing, which parties can be numbered. Pieces of information are posted and their ac-

cessibility can vary. To deem it otherwise could threaten the Freedom of expression[174], notably ensured by the ECHR which, as already noted, can have a diagonal indirect effect. Therefore, such communications would be protected during the first transmission stage – still occurring between two parties. But not during the second technical storage stage where they are intended to an indeterminate or irrelevant audience which composition is fluctuating.

It has now to be evaluated if such reasoning can be transposed as regards the implementation of directive 2002/58/EC, taking Belgium as an example.

Protected Communications under Belgian Implementation of Directive 2002/58/EC

If the above-mentioned reasoning seems defendable as regards Article 5 of Directive 2002/58/EC, how it is implemented in Belgian law and does this reasoning remain valid? The confidentiality of electronic communications is protected through both rules that existed before directive 2002/58/EC: one is enshrined in the Belgian Penal Code [PC][175] and the other one is in the Law on Electronic Communications [LEC] (Article 124). According to the LEC, *no one* can, if he is not authorized by *all* the persons *directly or indirectly* involved in the electronic communication, intentionally acquaint himself with the *existence* of this electronically transmitted and not sent to him communication, intentionally identify the persons concerned by the transmission of the information and its content, or still use in anyway the identification or the data obtained (intentionally or not). To break this rule is criminally punished[176]. According to Article 314bis of the Belgian PC, shall notably be punished the one who, with any apparatus, intentionally listen (or make listen), acquaint himself or tape *private*[177] *communications* to which he is not a participant, *during their transmission*, without the consent of each participant to the communication. In this respect, communications are private when they are not intended to "every man jack" ("*tout un chacun*") (Proposition of Data Privacy Act, Belgium, 1992, p. 7).

Some scholars argue that the protection afforded by the LEC goes further the pure transmission of the communication (de Terwangne, Herveg, & Van Gyseghem, 2005, pp. 50 and 91; Lambert, 1999, pp. 203-204). Indeed, this transmission condition is not required under the LEC while it is explicitly needed in Article 314 bis of the Belgian PC[178]. Nonetheless, other scholars argue that the LEC only applies during the transmission of the communication (Docquir, 2008, pp. 81-82; de Corte, 2000, p. 12)[179]. As regards Article 314 bis of the Belgian PC, its aim is not to protect communications when they are "at destination", for instance as shown by the *travaux parlementaires*, when mails are stored on the computer of the addressee (LEC, preparatory act, 1992, p. 6), but during their transmission. In this respect, it has been judged, by the Leuven Court of first instance (N.V. G.P.G. v. C.P., 2007), that an e-mail not already read or downloaded from the server is still in transmission and therefore still protected by the PC.

How to apply both dispositions? For instance, it has been argued that the PC protected the content of the communication, while the LEC protected other pieces of information such as the existence of the communication and its parties – traffic data. However, to acquaint oneself with the content of a communication also implies to acquaint oneself of the existence of the communication. In our view, P. De Hert's reasoning related to e-mails gives a good solution and permits the interpretation above mentioned related to Article 5 of directive 2002/58/EC and the context of SNSes. According to the author, the protection of PC lasts until the emails are taken in and until the addressee has knowledge of the emails, which is to say during their transmission[180]. And then the LEC can still apply after the transmission of the e-mail (De Hert, 2001, pp. 124-125 and footnote no. 86).

Conclusion

Finally, the fate of the protected communications and their traffic data is under the control of the qualified consents of the parties to these communications, even when they are stored. This means that to acquaint himself of protected communications, a third party needs the consent, as defined by directive 1995/46/EC[181] and exposed in the first part of this chapter, of each party to the communication. And such a third-party could be an advertiser, an application developer, the SNS provider[182], etc. We suggested that this qualified consent protect whole the communications occurring between a user and the SNS provider, during a first transmission stage. Then, during the second technical storage stage, are only protected those communications which are intended to a finite number of parties and when such parties do not constitute an indeterminate or irrelevant audience whose composition is fluctuating.

AMERICAN LAW

In the United States, the Electronic Communications Privacy Act [ECPA] ensures the confidentiality of the electronic communications. "Title I of the ECPA, known as the Wiretap Act [(18 USC §§ 2701-2712)], protects wire, oral, and electronic communications while *in transit*. Title II, also known as the Stored Communications Act (SCA) [(18 USC §§ 2701-2712)], protects data while held *in storage*" (Kane & Delange, 2009, p. 324)[183] (emphasis added by author). And the definitions of the terms of the Wiretap Act also apply to the Stored communications Act (18 USC § 2711 (1)).

In both Acts, what is protected is an electronic communication. Electronic communication is a wide concept. It means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" (18 USC § 2510 (12))[184]. For example, the First Circuit held that an email and the "[t]ransmission of completed online forms [...]" (Pharmatrak, Privacy Litigation, 2003) constitute such communications. In the case of SNSes, messages sent from one profile to another one or more, or instantaneously sent via Chat functionalities should be considered as electronic communications. Even if such a definition seems to show that the spectrum of the protected communications is broader than according to directive 2002/58/EC, the next developments will show that restrictions related to the audience of the communications at stake also exist.

The Wiretap Act is first very briefly discussed, because it will reveal less relevant as regards SNSes. The Stored Communications Act requires more developments. Then, the consent of the user of the SNS is studied as a potential exception to the application of both acts.

Wiretap Act

According to the Wiretap Act[185], it is notably forbidden to intentionally intercept any wire, oral, or electronic communication (18 USC § 2511 (1) (a)). Hearing that "a contemporaneous interception – *i.e.*, an acquisition during "flight" – is required to implicate [this Act]" (USA v. Steiger, 2003)[186]. Therefore, as regards the context of SNSes, the Wiretap Act will only apply to the first transmission stage we identified – communications occurring between the SNS user and the SNS provider. And the Stored Communications Act directly focuses on communications that are stored for short or long term – once data are on the SNS servers, they are stored.

Stored Communications Act

The Stored Communications Act "provides privacy protection to communications held by two types of providers": The provider of public elec-

tronic communication services[187] [ECS] and the ones of public remote computing services [RCS][188] (Kerr, 2004, p. 7). The principle is that they cannot knowingly divulge to any person or entity the content[189] of the users' electronic communications (18 USC § 2702 (a) (1) (2)). However, they can divulge non-content information to private entities (but not to a governmental entity) (18 USC § 2702 (a) (1) (3))[190]. If the services they provide are not public[191] – which is generally not the case of SNSes –, the Stored Communications Act does not apply. The Act also provides that, except in some cases, nobody can "intentionally [access] without authorization a facility through which an electronic communication service is provided" or "intentionally [exceed] an authorization to access that facility" when the electronic communication is "in electronic storage in such system" (18 USC § 2701 (a) (1) and (2)).

As O.S. Kerr (2004, p. 9) points out, the "classifications of ECS and RCS are context sensitive: The key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract." In this respect, O.S. Kerr (2004, p. 10) writes that "files held in intermediate "electronic storage"[192] are protected under the ECS rules", while files held for "long-term storage by that same provider are protected by the RCS rules." So, the "traditional view" is that an email, not opened – or not retrieved from the webmail server – falls under the ECS rules, while an opened one – or a retrieved from the webmail server one – falls under the RCS rules (Kerr, 2004, pp. 10-11).

But it has to be underlined in this respect that, according to the Court of Appeals for the Ninth Circuit (Theofel v. Farey-Jones, 2003), such non-retrieved mails can be deemed to be stored for backup purposes and then still falling under the ECS rules. It has to be recalled that the Ninth Circuit rules California where numerous SNS are established (*e.g.* Facebook and Twitter). The Ninth Circuit decided the following:

> *An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again – if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition. (Theofel v. Farey-Jones, 2003)*

The regimes related to both types of stored communications substantially differ as regards the access to the communications by the Government[193]. For our purpose, as regards the disclosure of information to private entities, one discrepancy has to be pointed out. Indeed, it could reveal important in the context of SNSes. As regards the RCS, the communications are protected "if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing" (18 USC § 2702 (a) (2) (b)). It is therefore still useful to qualify the SNS provider.

The traditional ECS provider is an Internet service provider, a phone company or even a webmail provider. But Courts have already deemed that an electronic bulletin board fits the definition of an ECS (Kaufman v. Nest Seekers, 2006)[194]. In addition, it has been the case of a "web-based forum where parties could communicate" (Inventory Locator v. Partsbase, 2005). Therefore, SNSes groups, profiles, etc., could be at stake. In this respect, not all electronic bulletin boards or forums would be protected. Indeed, as it was stated by the Eleventh Circuit in Snow v. DirectTV (2006), in "order to be protected by the [Stored Communications Act]; an Internet website must be configured in some way so as to limit ready access by the general public"[195]. And according to the Court's judgment referring to Konop v. Hawaiian Airlines (2002), the simple

need of a registration *without any screening* could be insufficient for the application of the Stored Communication Act. The Court underlined that:

[A] short simple statement that the plaintiff screens the registrants before granting access may have been sufficient to infer that the website was not configured to be readily accessible to the general public. However, Snow failed to make this or any remotely similar allegation. Instead, Snow's allegations describe, in essence, a self-screening methodology by which those who are not the website's intended users would voluntarily excuse themselves. Because this is insufficient to draw an inference that the website is not readily accessible to the general public, Snow's complaint fails to state a cause of action and it was proper to dismiss it. (Snow v. DirectTV, 2006)

And in Konop v. Hawaiian Airlines (2002):

"Konop controlled access to his website by requiring visitors to log in with a user name and password. Konop provided user names to certain Hawaiian employees, but not to managers or union representatives. To obtain a password and view the site, an eligible employee had to register and consent to an agreement not to disclose the site's contents."

Since "Anyone can join" Facebook and also other SNSes, a user's content available to any member of the network (e.g. Wall posts of "public" profile but nonetheless restricted to the members of the SNS) will not be protected under the Stored Communications Act and the ECS rules. To the contrary, the content which will only be disclosed to the user's friends ("private" profile), who have been screened because they have been individually accepted by the user at stake, could be protected. The suggested reasoning above as regards communications occurring between a finite number of parties could be transposed here. Of course and *a fortiori,* the public parts of the profile that are accessible from the Web without subscribing to the SNS will not be protected. Of course, the present reasoning would only apply insofar as Courts accept to make an analogy between an SNS and a Forum or a webmail depending on the communications at stake.

The RCS rules target longer storage of data – beyond the backup storage. It requires processing services, and these services originally concerned an "outsourcing function" needed, originally, where companies do not have the technological resources to have their own IT infrastructure to process data themselves (Kerr, 2004, pp. 26-27). Clearly, SNSes permit their users to store data for a long term, as they also provide data storage as a service. For instance, YouTube has already been deemed to constitute a RCS (Viacom v. YouTube, 2008). Of course, the same considerations as above mentioned related to the public or private character of the service will apply. Most probably, and putting aside Theofel v. Farey-Jones (2003), SNS will usually be considered as RCS because users outsource the processing of their data and store them on the SNS provider's servers for an indeterminate period of time.

Therefore the following question arises: If Theofel v. Farey-Jones (2003) does not apply, SNS provider being considered as RCS providers and not ECS providers, how far the access, to provide other services, to the data claimed by the SNS provider in the privacy policy and terms of use affects the protection afforded to its users by the Stored Communications Act? For instance as regards Facebook, Facebook Inc. can access the data to deliver targeted advertisements, how does this have to be taken into consideration? In other words, when and how far is an access "in connection" with the provision of the service? For example in Viacom v. Youtube (2008), the Court decided that the authorization of YouTube to "access and delete potentially infringing private videos is granted *in connection with*" YouTube's provision of storage services (emphasis added by author). It is impossible here to answer that

question which seems close to the question of the users' consents that can lead to an exception to the Stored Communications Act and the Wiretap Act. This question can be addressed now.

Consent and Stored Communications Act and Wiretap Act

The consent to terms of service and privacy policy of SNSes websites could lead to an exception to the prohibitions set in the Stored Communications Act[196] and in the Wiretap Act[197]. To this respect, there is a substantial difference between American law and European law. In other words, communications can be intercepted when they are transmitted or disclosed when they are stored with the consent, to sum up, of *one of the parties* to the communication. For "example, the sender (originator) of an e-mail as well as any intended recipients may give consent to disclose the communication" (Ackermann, 2009, p. 43). Under the Stored Communication Act, according to the federal rules protecting electronic communications, a "one party consent" is then only required (Schwartz & Reidenberg, 1996, p. 226).

Some States, such as California, have however adopted a "two-party consent rule" (Schwartz & Reidenberg, 1996, p. 227) requiring the consent of each party to the communication at stake. But for instance, the relevant Californian rule, related to the eavesdropping or recording of communications, is of little help here. Indeed it does not lead to the same result we could plead for under directive 2002/58/EC. In the case of communications realized through the Internet, the Californian Penal Code § 632 (a) would apply. According to this disposition:

"[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished..."

Therefore, only the confidential communications are protected, that is to say the communications "carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." And in any case, such a communication is not "a communication made in [...] any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded" (California Penal Code § 632 (c)). Moreover, the "person" targeted by the offence "excludes an individual known by all parties to a confidential communication to be overhearing or recording the communication" (California Penal Code § 632 (b)).

The lawfulness of the collection of clickstream data through cookies has been discussed in regards to the Stored Communications Act and the Wiretap Act. These Acts illustrate the consequences of a "one party consent" rule. In DoubleClick Privacy Litigation (2001)[198], the Court applied the same reasoning as regards the consent in the Stored Communications Act and in the Wiretap Act. It noted that contracts existed between DoubleClick and the websites involved in the use of cookies for the DoubleClick's advertisement program. Due to these contracts, electronic communications between these websites and their web surfers – their clickstream – could lawfully be communicated to DoubleClick[199]; "because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access under § 2701 (c)(2)." As regards the identification number of the cookie, that is not communicated to the Web sites at stake, the Court considered that, even if it were protected – *quod non* according to the Court –, DoubleClick's access is authorized because:

In every practical sense, the cookies' identification numbers are internal DoubleClick communications – both "of" and "intended for" DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs' hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. In contrast, virtually all plaintiffs are unaware that the cookies exist, that these cookies have identification numbers, that DoubleClick accesses these identification numbers and that these numbers are critical to DoubleClick's operations. (DoubleClick Privacy Litigation, 2001) (emphasis added by author)[200]

While an application of directive 2002/58/EC would have required, in addition, the consent of the web surfers.

As regards the consent itself and the Wiretap Act, if a party has knowledge or notification of the interception, her consent does not need to be express and can only be "inferred from the surrounding circumstances" (Garrie & Wong, 2009, p. 146, footnote no. 88). A *qualified* consent as what is required under directive 95/46/EC is not needed. The First Circuit Court of Appeals considered, still as regards the Wiretap Act, that,

Consent may be explicit or implied, but it must be actual consent rather than constructive consent"; it requires an "actual notice" or that "the surrounding circumstances convincingly show that the party knew about and consented to the interception. (Pharmatrak, Privacy Litigation, 2003)

Finally, in Viacom v. YouTube (2008), where the YouTube RCS and the Stored Communications Act were at stake, the Court addressed, in some extent, the question of the scope of the user consent to the terms of use and privacy policy of the website. It had been argued that users of YouTube have consented to the disclosure of data *by assenting to the YouTube website's Terms of Use and Privacy Policy, which contain provisions licensing YouTube to distribute user submissions (such as videos) in connection with its website and business, disclaiming liability for disclosure of user submissions, and notifying users that videos they divulge online in the public areas of the website may be viewed by the public (Viacom v. YouTube, 2008)*

And the Court answered that,

[N]one of those clauses [could] fairly be construed as a grant of permission from users to reveal to plaintiffs [(notably Viacom, claiming that it owned copyrights in television programs, etc., broadcasted by YouTube users)] the videos that they have designated as private and chosen to share only with specified recipients (Viacom v. YouTube, 2008) (emphasis added by author)

It is interesting to see that the Court directly takes into account the fact that the users at stake have defined privacy settings.

Conclusion

The protection of the confidentiality of communications seems more elaborated in the United States than in Belgium where the transposition of directive 2002/58/EC as regards this topic is relatively brief. But directive 2002/58/EC gives Member States enough margin to establish a well balanced framework. The ECPA and, more precisely, the Stored Communications Act should offer the SNSes users a mean to control, by their consents, the protected communications. However and some interpretation concerns put aside, only the consent of one party to the communication at stake is required. And such consent does not need to be qualified as it has to be as regards directive 2002/58/EC. This shows two substantial

differences between the American and European regimes of confidentiality of electronic communications.

PROTECTION OF COMPUTERS

Judge Kleinfeld, who dissented in USA v. Micah Gourde (2006), underlined that:

[F]or most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests — including perfect strangers — are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation. There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications [...] a married mother of three may be carrying on a steamy email correspondence with an old high school boyfriend. Or an otherwise respectable, middle-aged gentleman may be looking at dirty pictures. (USA. v. Micah Gourde, 2006)

Without any doubt, the web surfer's terminal – computer or mobile phone, etc. – is a very private space. So much that Y. Poullet (2008, pp. 62-65) has already suggested that it should be at the core of a third generation of data protection rules, making it closer to a "private electronic space", a "virtual domicile" (Y. Poullet, 2010). The author also refers to Germany that knows a new fundamental right to the confidentiality and the integrity of the technological information systems, based on the general right to personality[201]. In our view, the user should have the complete ownership of its terminal, controlling to which other terminals this latter "speaks" and what it "tells" them. For instance, everybody should have a *user-friendly* mean to monitor (and, need be, to block) the electronic communications coming from its computer terminal to the Internet and coming from this latter, to the former. It should be pointed out that, particularly as regards SNSes, the user's computer terminal is more than a *place* where personal information is stored[202] and life happens. It is also, and above all, a *mean to behave*, a necessary extension of the individual to "e-socialize" with others and, more generally, to "e-act."

Whatever can be the links between privacy, data protection and the computer terminal, the purpose focuses on the prohibition of hacking (III.3.1). It then underlines the consequences that directive 2002/58/CE could have as regards the use of cookies. Indeed, cookies imply the access to the computer of a web surfer (III.3.2). In this context, the user's consent is still a key mean of control.

HACKING AND SNSES

Hacking is internationally prohibited, like it is in Belgian and American law. The unauthorized access to a computer is forbidden. As regards SNSes, it seems particularly interesting to determine if a breach of a contract (terms of use), concluded between the user and the SNS provider as regards the use of the website, could lead to a hacking. Indeed, the access to the provider's servers would then occur contrary to what is authorized to users.

The Prohibition of Hacking

Thanks to the prohibition of hacking, the SNS user is empowered to control the access to his personal computer, the writing of data on it and the extraction of data from it. As the SNS provider is empowered to do the same as regards his own servers. In the Internet, the use of cookies, for instance, involves accessing to and writing data on the web surfer's personal computer. As the use of a SNS implies writing on the computers of the SNS provider. The Council of Europe's Covenant on Cybercrime (Budapest Convention,

2001) compels its Member States[203] to establish a criminal offence forbidding hacking[204]. It targets the intentional access, "without right", to computer systems (Article 2 of the Budapest Convention, 2001). A scholar emphasized that since "in order to be considered an offence, the conduct must be committed intentionally and unlawfully, i.e. "without right"", "there are acts which, if duly [...] *accepted as lawful commercial practices*, will not be considered a criminal offence under the Convention" (Csonka, 2006, p. 483) (emphasis added by author). Indeed, according to the Explanatory Report of the Budapest Convention (no. 38): "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized."

For instance as regards cookies, the explanatory report follows:

The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial installment or not removing it (no. 48)

Therefore, it seems implicitly that to define the parameters of a browser or to let the default rules play is enough to authorize access to a computer. Although the actual widespread browsers – Safari, Internet Explorer and Firefox – do not integrate a really user-friendly tool to easily and practically manage the cookies coming from the different websites. And although numerous websites – like SNSes, e.g. Facebook – technically compel web surfers to accept cookies to access the website.

The Belgian PC protects everyone against an unauthorized access to his computer (Article 550 bis CP)[205]. In the Code's words, will be punished anyone who, *knowing* that he is *not authorized*, *access* to a computer system or remains in such a system – external hacking –, a *malicious intent* being an aggravating circumstance (Article 550 bis, § 1, CP). Will also be punished anyone who, with a fraudulent intent, *exceeds his power to access* to such a computer system – internal hacking (Article 550 bis, § 1, CP). Therefore, the *mens rea* varies depending on the qualification as an "external hacking" (to access without authorization) or an "internal hacking" (to exceed rights of access). The internal hacking requires a fraudulent or malicious intent. That is to say the lure of illegal profit or malice (*Projet de Loi*, 2000, p. 16). In each case, the breaking of a protection system is not a constitutive element of the offence (*Projet de Loi*, 2000, p. 17)[206]. Of course, if such protection systems have been broken or by-passed, it is then impossible, for the individual at stake, to argue that he ignored he was not authorized to access to the computer at stake[207].

In American federal law[208], the Computer Fraud and Abuse Act (18 USC § 1030 [CFAA])[209] forbids hacking. Who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains" (18 USC § 1030, (a) 2°) "information from any protected computer[210]" will be punished (18 USC § 1030 (a), 2° (C)). Like in the Belgian PC, the breaking of a protection system is not required. But contrary to this Code, the *mens rea* is the same in both cases of hacking (internal or external). Coming back to the example of cookies, in the aforementioned matter DoubleClick Privacy Litigation (2001), the Court applied this statute. However, the lessons it provides are limited for the purpose, since DoubleClick did not question that it had not had the authorization to access web surfers' computers. The debate focused on the kind of damage at stake and the threshold victims had to demonstrate for the success of their suit. This is precisely what they failed to do, leading them to the failure of their lawsuit[211]. This case nonetheless shows that the use of cookies could lead to hacking.

American case law provides some answers to an interesting question that could be decisive in

the SNSes context and that needs now to be addressed: Could a breach of a contract – if there is actually a contract between an SNS provider and its users[212] – amount to an unauthorized access to a computer, constituting therefore a criminal offence?

Hacking and Breach of a Contract

In the United States, different cases show that "[t]he extent of authorization may turn upon the contents of an employment agreement or similar document, a terms of service notice, or a log-on banner outlining the permissible purposes for accessing a computer or computer network" (Computer Crime and Intellectual Property Section, Criminal Division ([CCIPS], 2007, pp. 6-10). Courts have had to decide if the knowingly breach of a website's terms of service (AOL) (AOL v. LCGM, 1998), and even those of an SNS (MySpace) (USA v. Lori Drew, 2009) could lead to hacking. Indeed, the access to an SNS necessarily implies the access to the computer systems of its provider (or of the provider's subs contractors). As regards internal hacking and the CFAA, a conscious behavior, without any malicious intent, suffices to be punished as it has been noted. In AOL v. LCGM (1998), where unsolicited bulk emails were at stake, the defendant was deemed guilty of hacking[213]. The Court decided that,

Defendants have admitted to maintaining an AOL membership and using that membership to harvest the e-mail addresses of AOL members. Defendants have stated that they acquired these e-mail addresses by using extractor software programs. Defendants' actions violated AOL's Terms of Service, and as such were unauthorized. (AOL v. LCGM, 1998)

Whereas, in the matter of USA v. Lori Drew, the defendant was found not guilty (2009). In this latter case, the defendant was a mother who harassed a young girl using MySpace. To this aim, she falsely represented herself as a young boy (with a photo). She knowingly violated MySpace terms of use compelling users to provide real information. The American government, suing her, pleaded that such a behavior constituted a hacking – without specifying if it was an internal or an external one – of MySpace's servers[214].

Judge Wu concluded that the government wrongly charged her because of the "void-for-vagueness doctrine"[215]. Although he specified that "within the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of services/use will render the access unauthorized and/or cause it to exceed authorization"[216]. As stated by Judge Wu, "[t]o avoid contravening the void-for-vagueness doctrine, the criminal statute must contain "relatively clear guidelines as to prohibited conduct" and provide "objective criteria" to evaluate whether a crime has been committed" (USA v. Lori Drew, 2009). He deemed in particular that if any breach of terms of use constituted a criminal offense of hacking, the "fair warning requirement" would not be satisfied[217]. Which means that an average individual would not be able to identify what is forbidden and what is not. Not to follow Judge Wu's point of view in the context of SNSes would lead to potentially sentence for internal hacking anyone who, breaching – without any bad intent – the terms of use requiring its identification, would act under a pseudonym. Such "an interpretation that criminalizes routine computer use would give the government the power to arrest any typical computer user" (Kerr, 2010, p. 17). Terms of use are potentially really vague and "[v]iolating the [terms of service] is the norm; complying with them the exception" (Kerr, 2010, 21). Terms of use can be so vague that any illegal *intent* – from a civil or a penal viewpoint – in the use of the website – or service – at stake would lead to a breach of these terms[218]. This would therefore make the web surfer guilty of hacking. The reasoning can be pushed to an absurd result taking an IAP as an example. If an

IAP contractually forbids that his customer pursues any illegal purpose using the Internet access services provided[219], any use of the Internet with an illegal intent would then imply an unauthorized access to the IAP's computer infrastructure, and would therefore constitute a hacking. This is clearly an unpredictable result.

Transposed in Belgian law, the reasoning of Judge Wu would lead to consider that the proposed interpretation is contrary to the "legality principle" ("*prinicpe de légalité*") of criminal law[220]. It has to be recalled that, according to the Belgian PC and contrary to the CFAA, an internal hacking requires a fraudulent or malicious intent (*Projet de Loi*, 2000, p. 16). If the defendant, in USA v. Lori Drew (2009), had such a malicious intent since she wanted to harass a young user of the social network[221], would she be for all that guilty of hacking according to Belgian law? Clearly, the considerations evoked above can be recalled here, *mutatis mutandis*. She shouldn't have been sentenced for hacking. Moreover, focusing on the classification made by the Belgian legislator, computers are here only a mean to commit another offence (harassment), a *modus operandi*, and not the aim of the criminality as it is normally the case as regards hacking (*Projet de Loi*, 2000, pp. 6-7). In this second category of offences, where computers are the target of the criminality, the legislator focused on behaviors infringing the confidentiality, the integrity and the availability of computers or of data stored in them or processed or transferred through them (*Projet de Loi*, 2000, pp. 6-7). In USA v. Lori Drew (2009), to harass by means of a simulated flirt and under a false identity is something else.

Maybe the conclusion would be different if the harasser mother had wished to obtain access to the private profile of the MySpace user to retrieve data from this profile, knowing that the young girl would never have given access to her profile if the harasser didn't act under a false name. In this case, it could be argued that the mother would have tried to by-pass the technical protections that ensure the private character of the profile at stake, by deceiving the holder of the profile, exploiting her credulity.

However that may be, the disputed reasoning in U.S.A. v. Drew (2009) could prove to be a very powerful legal mean to protect SNS users against the wrongful transfer and use of personal information relating to them. This would be particularly true as regards the application programming interfaces [API] provided by SNSes and the applications developed by third-party developers. For instance on Facebook, as explained, an application can access personal data through the Facebook platform. If technical measures are not carried out by the SNS provider, and if the applications developers breach the terms of use related to the processing of users' personal data, would they become hackers? Facebook constitutes a case in point, as one looks at what the assistant to the Canadian Privacy Commissioner wrote in her report:

In the absence of any evidence of technological safeguards, I can only assume that, when Facebook speaks of limits on access to users' information, it speaks of contractual limits. In other words, as means of limiting access, it is relying mainly upon certain prohibitions stated in policy documents, and upon trust in the application developers' acknowledged agreement to abide by those prohibitions. (Denham, 2009, no. 199)

However Facebook contested this statement (Denham, 2009, no. 197). The security measures taken by Twitter have also been criticized when Twitter has been hacked by hacker taking administrative control of the website and accessing to (private) personal data. This finally led to a settlement between Twitter and the FTC (In the Matter of Twitter Inc., FTC, 2010).

The same question would arise if SNSes providers gave their users the possibility to define their own rules of diffusion of personal data in a privacy policy they could transform into a binding

contract, as suggested above. In this latter case, the "authorization" to access to the SNS servers would be directly defined by the users.

Therefore, the question is: When could a contractually forbidden access to the servers of an SNS provider, not prevented by technical measures, – the developer at stake only having reasonable notice of the additional developer terms of use – lead to an internal hacking under Belgium Penal Code and/or CFAA[222]? In particular, *quid* if this behavior would have constituted such a hacking if the contractual terms had been technically concretized? In our view, the precedent developments related to USA v. Lori Drew (2009) are still relevant in such a case. But some elements could moderate the previous conclusions. Indeed, on the one hand, a specific vigilance is waited from the application developer. He controls the development of his application and knows the working of the API on which he grafts his product if he wants that this latter works. And on the other hand, the developer would infringe the confidentiality of the SNS's systems in the extent that he would access and retrieve data he can not access or retrieve. Contrary to what happened as regards MySpace. Anyway, the potential responsibility – or irresponsibility – of the application developer would not prevent in any manner the responsibility of the SNS provider himself who would not provide the users adequate protection measures to protect their profiles and personal data.

Conclusion

The American and Belgian prohibitions of hacking are close[223]. This is logical hearing that both States ratified the Budapest Convention. They diverge nonetheless to some extent, for instance as regards the *mens rea* required for an internal hacking: no malicious intent is required according to American law. Anyway, the CFAA and the Belgian PC empower users to control the access to their computer, and SNSes providers to control the access to their servers. In our view, the pure breach of a contract (terms of service) concluded with a SNS provider, if such a contract is valid, should generally not lead to hacking. Even if it could be argued for the contrary as regards applications developers as suggested. Therefore, where no technical protection measures are put in place, the confidentiality of electronic communications remains an important guardrail.

DIRECTIVE 2002/58/ EC AND COOKIES

Directive 2002/58 could have a specific role to play as regards cookies which are, as already noted, written on users' computers. Its former Article 5.3[224] provided for that "the use of electronic communications networks to store information or to gain access to *information stored in the terminal equipment* of a subscriber or user" was "only allowed on condition that the subscriber or user concerned is provided with" due *information according to Directive 95/46* "and is offered *the right to refuse* such processing by the data controller" (emphasis added by author). A purely technical storage or access was nonetheless permitted to facilitate the transmission of electronic communications or if it was necessary, in order to provide an information society service explicitly requested by the subscriber or user (Article 5.3 of directive 2002/58/EC)[225]. In this respect, the user of cookies or web beacons – e.g. a SNS provider – can comply with its duties at once and for their future use during the user's next connections (Recital 25 of directive 2002/58/EC).

Since the recent modification of directive 2002/58/EC, for the use of cookies in the context of the processing of personal data to be permitted, the user (or subscriber) has henceforth to give his or her "consent" as defined according to directive 95/46/EC (Article 2, al. 2, f) of directive 2002/58/EC). The old opt-out[226] process becomes on opt-in one. In other words, the use of cookies requires what was previously named a qualified

consent. However, the French version of Directive 2009/136/EC modifying Directive 2002/58/EC requires that the user or the subscriber has given his or her "*accord*" –not defined by these directives – in place of "*consentement*" – referring to Directive 95/46/EC. The use of the word "*accord*" is most probably a simple formal mistake.

But the study of the legislative history of the Directive 2009/136/EC and the policy that could be behind recital 25 of Directive 2002/58/EC could show that it would not be the case. On the one hand, in his first lecture, the European Parliament proposed to modify Article 5.3 in such a way that the prior consent of the user or the subscriber would be first and foremost required to use cookies, "taking into account that *browser settings constitute prior consent*", and that then, this user or subscriber was offered "the right to refuse such processing by the data controller" (Article 2.5 of European Parliament legislative resolution, 2008) (emphasis added by author). This would mean that, following the European Parliament, defining the browser settings – or letting the default rules play – constitutes a "qualified" consent under directive 95/46/EC despite what has been noted about the widespread browsers[227] – lobbyism[228]? For the record, the Working Party 29 (WP171, 2010, pp. 13-15) recently considered that browser settings generally do not raise to the expression of valid consent[229]. And it declared itself in favor of a prior opt in consent mechanism (WP171, 2010, pp. 16-17). However that may be, this amendment has been rejected by the Commission that was then followed by the common position of the Council.

On the other hand, the consent required as regards cookies does not seem to have to be "as free" as the "qualified" consent, since recital 25 of directive 2002/58/EC, *in fine*, reads as follows: "Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose." Admittedly, directive 95/46/EC does not necessarily forbid a website provider – e.g. an SNS provider – to make the access to his service depending on the consent of the web surfer to the processing of personal data related to him[230], basing his processing operation on such consent.

Anyway, if one of the objectives of the Commission was to "[ensure] a high level of protection of consumers' and users' rights, including the right to privacy and data protection in electronic communications", to "[enhance] the protection of individuals' privacy and personal data in the electronic communications sector, in particular through strengthened security-related provisions" (COM/2007/0698 final, no. 1), and if the Parliament wanted "[s]trengthened provisions on protection against spyware and placing of cookies on users' devices" (COM/2009/0421 final, no. 3.1), having regard to the actual state of the art concerning basic and widespread browsers, the simple settings of such a browser cannot constitute the "assent" or "*accord*" needed by the data controller to use cookies or other tracking web beacons[231].

To sum up, if an SNS provider chooses to use cookies, he can only act under the control of the user's qualified consent he has to obtain before the placement of the cookie (e.g. by checking a specific box authorizing this processing). Except if he uses cookies for a purely technical purpose.

WHICH LAW AND WHICH JUDGE ARE IN CONTROL?

Given the differences identified above, between American and European rules related to privacy, data protection, confidentiality of electronic communications and hacking, it is interesting to discuss, admittedly briefly and without any in depth analysis, the question of the applicable law (prescriptive jurisdiction). As a premise, the question of the competent judge (adjudicative jurisdiction) has to be sketched. Without any doubt, these concerns need further assessment. They are only evoked from the European – if required, Belgian – perspective.

First and foremost, it has to be noted that a contractual choice of law made by the SNS provider – California law being often chosen[232] –, and of a jurisdiction – California jurisdiction as regards Facebook – is probable. In this respect, the SNS provider does not necessarily pursue the goal of avoiding the user's empowerment to control what happens. Although excessive limitations on liability clauses are a clue of the contrary... For instance, California law, in the United States, is one of the most developed as regards privacy[233]: "California [...] has the most comprehensive approach to data protection", and "[a]s a result of a series of important judicial opinions, California has the strongest constitutional scheme of data protection in the United States" (Schwartz & Reidenberg, 1996, pp. 132 and 135). To choose Californian jurisdictions is therefore not to try to avoid privacy. Although it has been noticed that privacy and data protection suffer significant limitations in the United States in general. However that may be, European law limits the autonomy of the parties as regards conflict of laws, for instance when consumers – concerning applicable law and jurisdiction[234] – or distance contracts – concerning applicable law[235] – are at stake. The rest of the purpose takes as a premise that there is no choice of law and no choice of judge.

If a user of the SNS suffers harm due to the violation of data protection or privacy rules, the extra-contractual liability of SNSes providers – need be, other users – could be staked. The "courts for the place where the harmful event occurred or may occur" would then have jurisdiction (Article 5.3 of regulation 44/2001/EC). However as regards applicable law, data protection and privacy have their own legal regimes. Courts of a Member State should normally apply the data protection rules of this State if the data controller is therein established, and if the processing operation occurs in the context of the activities of this establishment. Or, if the data controller, not established within the territory of the European Union, uses equipment[236] on the territory of this Member State, to the purpose of the processing operation at stake. Admittedly, the debate is here simplified[237].

According to Belgian private international law[238], the obligation resulting from a threat to privacy would be governed by the law of the State where the harmful behavior took place *or* where the harm occurred or *may occur*, unless that the person responsible demonstrate that she could not foreseen that the harm would occur in this State (Article 99, §2, 1 of the Belgian Private International Law Code). When a Belgian user of an SNS is at stake, it is reasonable to foresee that the harm he could suffer through the SNS can occur in Belgium, where he usually lives.

In addition, Article 8 ECHR could influence conflict of laws, *in concreto*, in a particular case. Indeed, insomuch as a foreign law would be to apply according to the national conflicts of law rules of a Court, the judge could have to discard the application of this foreign law – e.g. via a public order exception – if such an application thereof would create a situation conflicting with Article 8 ECHR, in the particular matter brought before him[239]. For the record, Article 8 ECHR includes, to some extent – but which precisely? –, data protection rules. In this respect, it still has to be determined when Article 8 ECHR could have to prevail over a foreign law in international cases. That is to say: which link with the territories of the contracting States would have to be satisfied as regards Internet in general, and which rights – if not all – enshrined in Article 8 ECHR cannot be tempered by the international characteristics of the situation at stake.

Concerning contracts concluded by consumers and contractual litigations, the Courts of the State where the SNS user is domiciled could have jurisdiction in cases where the SNS provider *directs its activities* notably *to* that Member State (Article 15 of regulation 44/2001/EC). And then even if there is a choice of law provision in the contract at stake, the consumer could not be deprived "of the protection afforded to him by provisions that

cannot be derogated from by agreement by virtue of the law" of the concerned Member State. Given that absent this choice of law, the whole law of this Member State would apply (Article 6 of regulation 593/2008/EC)[240]. Facebook, for instance, indisputably directs its activities to the UK, to France, Belgium, etc., in general, to the territory of the European Community[241], just as Hi5 precisely targeted international markets (OPCC, 2009, p. 15). Another example could be the website "Chatroulette" that began locally and is now worldwide used and, most probably, targeted[242]. To the contrary, MySpace originally excluded users located outside the United States, screening them by means of their IP addresses (OPCC, 2009, p. 15).

Still as regards consumer protection, directive 93/13/EC forbids unfair terms in consumer contracts notwithstanding a choice of law electing a foreign State law if the contract has a close connection with the territory of the Member States[243]. Which should be the case, for instance, when a user of an SNS has its habitual residence in a Member State, usually uses the SNS on its personal computer located in this Member State – the SNS being put on its market –, when cookies are placed on his personal computer and when this user is a data subject whose personal data are processed after transborder data flows from the Community territory.

Concerning Belgian criminal law, the adjudicative and prescriptive jurisdictions depend, as a rule, on the place where the offence has been committed. Criminal law is territorial, although it could exceptionally be extraterritorial[244]. To apply Belgian law and bring a criminal case before a Belgian court, it suffices that one of the constitutive elements of the offence occurred, in whole or in part, in Belgium (Kuty, 2009, p. 365). Which refers to the "subjective and objective territorial principles" (Hayashi, 2006, p. 286). Hacking can be taken as an example. In a case admittedly limited to the Belgian territory, a Court of first instance (OM v. P.K., 2008) find itself competent while the responsible of the hacking realized his unlawful behavior from its domicile, in a place were this Court was not competent. An unlawful access to an MSN account was notably at stake, and the Court decided that the victim, who was domiciled in the area of its jurisdiction, could bring her case before it. It was the Court of the place where the victim couldn't access her Hotmail account.

As regards the confidentiality of electronic communications, the Belgian LEC could apply to the unlawful use of cookies by SNSes providers who could be sued in Belgium. In such case, the acquaint of the communications at stake happens through the cookies located on the computer terminal of the concerned individual, thus, as the case may be, in Belgium. Given that the LEC does not define its territorial scope[245], the general above mentioned rule of Belgian criminal law should apply to determine the applicable law (Article 100 CP). Concerning the adjudicative jurisdiction, a criminal prosecution would occur according to the same rules of criminal law. And a civil claim for damages could be introduced before the "courts for the place where the harmful event occurred or may occur" (Article 5.3 of regulation 44/2001/EC), or before the court seized for the criminal prosecution (to the extent that that court has jurisdiction under its own law to entertain civil proceedings) (Article 5.4 of regulation 44/2001/EC)[246].

Finally without going into details, even European competition law could apply to SNS providers established outside the territory of the Community according to the effects doctrine. This doctrine has been applied in the United States and, in some extent, in European competition law[247]. In this respect, the global character of the market at stake will be particularly relevant in the analysis. For the record, European competition law has been evoked in the context of SNSes notably as regards the potential refusal of an SNS provider to access his platform of application. And it has been asked if providing a SNS free of charge in exchange of targeted advertising could not constitute a predatory pricing practice.

Now, which conclusion taking out of this brief outline of private international law? A kind of convergence arises as regards the possible applicability of European – Belgian – law as regards many legal concerns – consumer protection, privacy, hacking, confidentiality of electronic communications, competition – to a same SNS provider who would be established outside the territory of the European Union. Aside from data protection, that seems to follow an own regime leading to another conclusion. Put aside the Facebook's offices established in Europe[248] – given that their activities could be deemed distinct from those of Facebook, Inc. in California –, as Facebook Inc. processes personal data, it is a data controller established in the United States. A complicated and questionable interpretation of data protection rules seemed required to subject Facebook to the integrality of European data protection law – i.e. not only the transborder data flows regime[249]. Now, the discussion is probably more straightforward. Indeed, the clause 18.1 of the last version of the Statement of Rights and Responsibilities (October 4, 2010) specifies that "[i]f you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and *Facebook Ireland Limited*" (emphasis added by author). But the question remains subjected to the determination of the activities of the Irish office of Facebook.

Anyway, put aside the clause and the role of the Irish company, a Facebook-like SNS presents a lot of connections with the European Union as it was shown. Wouldn't it be useful to think again conflicts of law rules as regards data protection in this context, giving these rules, if it were deemed opportune – and we think it is – another territoriality[250]? Data protection could take profit of rapprochement with consumer contracts conflicts of law rules. After all, a software as a service is offered to European web surfers – final consumers –, free of charge hearing that their personal data can be used by the SNS provider. The criteria of applicability of data protection rules could take into account the data protection obligations at stake, the habitual residence of the individual concerned, the fact that the service provider directs its activities to the territory of the European Union, the fact that the Foreign State where the data controller is established only ensures an adequate protection[251] – or no adequate protection –, the place of establishment of this data controller, etc. Given that the localization of the equipments could not be relevant in the context of SNSes[252]. Article 4 of directive 95/46/EC has to be improved[253] to ensure better legal certainty. And the previous considerations should matter to this end.

As the case may be, the territoriality of the data protection rules could vary depending on what they impose to the data controllers or, *if an evolution of the is this sense is desirable and happens*, depending on the fact that they impose duties to the data controller *or to "data processors"* (SNS providers and, more generally, cloud computing service providers). Of course, in this respect, the question would be to determine if it is desirable and useful, or even required, to impose specific duties to cloud computing service providers when they are not data controllers. These rules could be useful, for instance, when the user of the service falls outside of the scope of Directive 95/46/EC (e.g. domestic use exemption) but nonetheless process personal data.

However that may be, nowadays, the international character of SNS and more generally cloud computing and Internet services requires an international discussion[254], at the end of which, on the one hand, data subject's rights must not be sacrificed to the profit of emergent technologies and on the other hand, this emergence must not be suffocated to death due to an unrealistic and unworkable conception of data protection.

CONCLUSION

In the context of cloud based SNSes, users claim more control over personal information. In fact, users lose some control. Principally, on the one hand, as regards the creation of personal data related to them and, on the other hand, concerning their spread and secondary use. It has been shown clearly that European and American law empower them, to a certain extent, to recover ownership over such data. Even if these laws differ and are not easy to apply to the SNSes environment.

Privacy, defined as "information self-determination" in European law, and as "contextual integrity" or "informational privacy" in the United States constitutes a first users' mean of control over information related to them. However, we noted that American privacy suffers weaknesses in SNSes due to its subordination to reasonable expectation of privacy. Admittedly, from a theoretical point of view, the interpretation of this requirement can evolve and compensate for the present weaknesses. Anyway, it has been suggested that contracts between users could help to solve the problem. European privacy is generally not subordinated to reasonable expectation of privacy. At the present time, European and American law diverge. But American law offers a conceptual framework permitting an evolution that would make both laws closer.

European privacy is "horizontalized" through data protection rules. While, at the present time, American law does not offer a general data protection framework. As regards European law, the purpose firstly brought into focus the interconnections between contract law and the qualified consent of the data subject. In this respect, it underlined that when using SNSes, the consent of users often does not satisfy the conditions required by data protection rule. Yet, SNSes providers usually rely on such consent. Even if no general conclusion can be proposed, users generally lack information as regards the processing of personal data. Their consents usually are not specific and only implied by the global assent to terms and conditions. And, finally, they are not often free insofar as the SNSes market is characterized by strong network effects – even if the market is dynamic –, and as they have no other choice that consenting to subsequent modifications of the service and the relevant terms if they want to remain on the social network. As far as the American Safe Harbor Principles are concerned, these do not require such a qualified consent. We also noted that the European individuals' right of access gives user a powerful mean to follow the spread of personal data and, as the case may be, stamp it out. While the right of access enshrined in the Safe Harbor Principles depends on the American privacy conception.

The confidentiality of electronic communications and the prohibition of hacking have been identified as two other means to control information. Concerning both these sets of rules, American law and European law are still different to some extent. For instance, the confidentiality of electronic communications is protected by a two-party consent rule in Europe. While in the United States, a one-party consent rule is established. And concerning hacking, both laws diverge concerning the *mens rea* required for internal hacking. Both laws also suffer interpretation concerns. As regards the confidentiality of electronic communications, it revealed difficult to identify which "actors" are concerned and which communications are protected. An interpretation ensuring users the protection of numerous communications occurring, on the one hand, between them and the SNS provider and, on the other hand, between themselves through the Internet and the network of the SNS provider himself has been suggested. Anyway, law appears difficult to apply in the SNSes context. As regards hacking, things seem less complicated at first sight. But they become more difficult when it has to be decided if the breach of a contract (terms of use)

can lead to hacking. It has been concluded that it should not be the case, even if, as regards application platform interfaces, it could be argued to the contrary.

The discrepancies between American and European laws lead us to a brief discussion related to adjudicative and prescriptive jurisdictions rules. These latter should bring legal certainty where SNSes involve inevitably and permanently both regulatory framework. The supply of popular SNSes comes from the United States (Facebook, LinkedIn, Twitter, etc.), and a significant part of the demand lies in Europe. We pointed out that European – as the case may be, Belgian – consumer protection law, privacy law, criminal law and competition law could apply to American based SNSes providers such as Facebook, when European judges are competent to give a ruling on a case. However, this is less evident as regards data protection rules whose territoriality could be thought again depending on the services at stake.

In any case, our purpose was not to eclipse the individual's responsibility. As B. Kane and B.T. Delange (2009, p. 345) wrote: "the ultimate guardian of privacy is the individual." The SNS user lies amongst the first people accountable of what becomes of personal data related to him. Nonetheless, when he is urged to get into a storm cloud where he thinks he is on cloud nine, he can then fall again on the grim reality, lacking control; in the "SNS-cloud", not everybody is a weather forecaster. Then, the legal means we presented come on stage.

NOTE

Jean-Philippe Moiny is a Research fellow FRS-FNRS in the *Research Centre on IT and Law (CRID) at the University of Namur, Belgium.*

REFERENCES

Ackermann, T. G. (2009). Consent and discovery under the Stored Communications Act. *The Federal Lawyer, 200,* 43–46.

Ahlborn, C., Evans, D. S., & Padilla, A. J. (2001). Competition policy in the new economy: Is European competition law up to the challenge?. *European Competition Law Review, 22.*

Antitrust Modernization Commission. (April, 2007). *Report and recommendations*. Retrieved on January 30, 2010, from http: //govinfo.library. unt. edu/amc/

Austrian Regulatory Authority for Broadcasting and Telecommunications. (April, 2005). *Guidelines for VoIP service providers*. Consultation Document. Retrieved on January 30, 2010, from http: //www.eadp. org/main7/position / VoIP_Guidelines_2005 _AUSTRIA.pdf.

Berman, G. A. (2006). *The constitution, international treaties, and contracts*. In Convergence in legal systems in the 21st century, General Reports delivered at the XVIth International Congress of Comparative Law, Brisbane, 2002. Brussels, Belgium: Bruylant.

Boyd, D. M., & Ellison, N. B. (October, 2007). *Social network sites: Definition, history, and scholarship*. Retrieved January 30, 2010, from http://www.danah.org/papers/

Bucklin, R. E., & Sismeiro, C. (2008). *Click here for Internet insight: Advances in clickstream data analysis in marketing*. Retrieved on January 30, 2010, from http://www.ssrn.com

Buya, R., Yeo, C. S., & Venugopal, S. (2008). *Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities*. Retrieved on January 30, 2010, from http://arxiv.org/pdf/0808.3558

Byrnside, I. (2008). Six clicks of separation: The legal ramifications of employers using social networking sites to research applicants. *Vanderbilt Journal of Entertainment and Technology Law, 10.*

Ciocchetti, C. A. (2007). E-commerce and information privacy: Privacy policies as personal information protectors. *American Business Law Journal*, 44.

Clayton, R., & Tomlinson, H. (2001). *The law of human rights*. Oxford, United Kingdom: Oxford University Press.

Cohen, J. E. (2000). Cyberspace and privacy: A new legal paradigm? *Stanford Law Review*, 52.

Computer Crime and Intellectual Property Section. Criminal Division, & Eltringham, S. (principal ed.), (2007). *Prosecuting computer crimes*. United States of America: Office of Legal Education, Executive Office For United States Attorneys. Retrieved on January 30, 2010, from http: // www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf

Couillard, D. A. (2009). Defogging the cloud: Applying fourth amendment principles to evolving privacy expectations in cloud computing. *Minnesota Law Review*, 93.

Csonka, P. (2006). The council of Europe's convention on cyber-crime and other European initiatives. *International Review of Penal Law*, 77, 3–4.

Dalsen, W. (2009). Civil remedies for invasions of privacy: A perspective on software vendors and intrusion upon seclusion. *Wisconsin Law Review*, 1059–1091.

de Corte, R. (2000). E-mails taboe voor de werkgever of niet. *Juristenkrant, 7.*

De Hert, P. (2001). Internetrechten in het bedrijf. Controle op e-mail en Internetgebruik in Belgisch en Europees perspectief. *Auteurs & Média,* 1.

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In Claes, E., Duff, A., & Gutwirth, S. (Eds.), *Privacy and the criminal law. Antwerpen, Belgium & Oxford.* United Kingdom: Intersentia.

De Hert, P., de Vries, K., & Gutwirth, S. (2009). Note d'observation sous Cour constitutionnelle fédérale allemande, 27 February 2008. *Revue du Droit des Technologies de l'Information, 34.*

Denham, E. (Assistant Privacy Commissioner of Canada). (July 16, 2009). *Report of findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act.* Retrieved on January 30, 2010, from http: //www.priv.gc. ca/cf-dc/2009/ 2009_008_0716_e.pdf

De Schutter, O. (2005). La renonciation aux droits fondamentaux, La libre disposition du soi et la règne de l'échange. In Dumont, H., Ost, F., & Van Drooghenbroeck, S. (Eds.), *La responsabilité, face cachée des droits de l'homme.* Brussels, Belgium: Bruylant.

de Terwangne, C., Herveg, J., & Van Gyseghem, J.-M. (2005). *Le divorce et les technologies de l'information et de la communication. Introduction à la protection des données dans la preuve des causes de divorce.* Brussels, Belgium: Kluwer.

de Villenfagne, F., & Dusollier, S. (2001). La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique. *Auteurs & Média, 1.*

Dhont, J., & Pérez Asinari, M. V. (2003). New physics and the law. A comparative approach to the EU and US privacy and data protection regulation. In *Usage of methodology in European law.* Namur, Belgium: Presses Universitaires de Namur.

Dhont, J., & Rosier, K. (2003). Directive vie privée et communications électroniques: Premiers commentaries. *Revue Ubiquité – Droit des technologies de l'information, 15.*

Dickson, B. (1999). The horizontal application of human rights law. In Hegarty, A., & Leonard, S. (Eds.), *Human rights, an agenda for the 21st century*. London, United Kingdom & Sydney, Australia: Cavendish Publishing.

Dinant, J.-M. (2000). Les traitements invisibles sur Internet. In Montero, E. (Ed.), *Droit des technologies de l'information, Regards prosepctifs: à l'occasion des vingt ans du C.R.I.D. Cahiers du C.R.I.D. Brussels*. Belgium: Bruylant.

Docquir, B. (2008). *Le droit de la vie privée*. Brussels, Belgium: Larcier.

Dreier, T. (2010). Opt in and opt out mechanisms in the Internet era – Towards a common theory. *Computer Law and Security Review, 26.*

Dumortier, F. (2009). *Facebook and risks of decontextualization of information*. Retrieved on January 2010, from http://works.bepress.com/franck_dumortier/1

Dunne, R. (2009). *Computers and the law, an introduction to basic legal principles and their application in cyberspace*. Cambridge, United Kingdom: Cambridge University Press.

Economic and Social Committee. (2000). *Opinion on the proposal for a directive of the European Parliament and of the Council on a common regulatory frame work for electronic communications networks and services*. COM(2000) 393 final – 2000/0184 COD.

Edwards, L. (2009). Consumer privacy law: Online direct marketing. In Edwards, L., & Waelde, C. (Eds.), *Law and the Internet*. Oxford, United Kingdom & Portland, OR: Hart.

Eisenmann, T., Parker, G., & Van Alstyne, M. (July 30, 2009). *Platform envelopment*. Retrieved on January 30, 2010, from http://www.ssrn.com

European Commission. (1997). Commission notice on the definition of relevant market for the purposes of community competition law. *Official Journal, C*, 372.

European Commission. (1998). Communication, status of voice communications on Internet under community law and, in particular, pursuant to directive 90/388/EEC. *Official Journal, C*, 6.

European Commission. (2000). *Proposal for a Directive of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services*. Explanatory memorandum. COM/2000/0393 final - COD 2000/0184.

European Commission staff working document. (June 14, 2004). *The treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework* (information and consultation document). Retrieved on January 30, 2010, from http://ec.europa.eu/information_society/policy/ecomm/doc/library/working_docs/406_14_voip_consult_paper_v2_1.pdf

European Commission. DG Competition. (December, 2005). *DG Competition discussion paper on the application of Article 82 of the Treaty to exclusionary abuses*. Retrieved on January 30, 2010, from http: //ec.europa. eu/competition/antitrust/art82/ discpaper2005.pdf

European Network and Information Security Agency, & Hogben, G. (Ed.). (October, 2007). *Position paper no. 1 - Security issues and recommendations for online social networks*. Retrieved on January 30, 2010, from http://www.enisa.europa.eu

European Network and Information Security Agency. Catteddu, D., & Hogben, G. (Eds.). (November, 2009). Cloud computing, benefits, risks and recommendations for information security. Retrieved on February 20, 2010, from http: // www.enisa.europa. eu/act/rm/files/deliverables/ cloud-computing-risk-assessment

European Regulators Group. (December, 2007). *ERG common position on VoIP.* Retrieved on January 30, 2010, from http: //www.irg. eu/streaming/ erg_07_56rev2_cp_ voip_final.pdf?contentId= 543022&field=ATTACHED_FILE

Evans, D. S. (2008). Antitrust issues raised by the emerging global internet economy. *Northwestern University Law Review*, 102.

Gardbaum, S. (2003). The horizontal effect of constitutional rights. *Michigan Law Review*, 102.

Gardbaum, S. (2006). Where the (state) action is, a review essay on the Constitution in private relations: Expanding Constitutionalism. In Sajó, A., & Uitz, R. (Eds.), *International Journal of Constitutional Law, 4*. Eleven International Publishing.

Garrie, D. B., Armstrong, M. J., & Harris, D. P. (2005). Voice over Internet Protocol and the Wiretap Act: Is your conversation protected? *Seattle University Law Review*, 29.

Garrie, D. B., & Wong, R. (2006). Demystifying clickstream data: A European and U.S. perspective. *Emory International Law Review*, 20.

Garrie, D. B., & Wong, R. (2009). Privacy in electronic communications: The regulation of VoIP in the EU and the United States. *Computer Telecommunications Law Review, 6.*

Gindin, S. E. (2009). Nobody reads your privacy policy or online contract? Lessons learned and questions raised by the FTC's action against Sears. *Northwestern Journal of Technology and Intellectual Property, 8.*

Grimmelmann, J. (2009). Saving Facebook. *Iowa Law Review*, 94.

Hammje, P. (1997). Droits fondamentaux et ordre public. *Revue Critique de Droit International Privé*, 1.

Hayashi, M. (2006). Objective territorial principle or effects doctrine? Jurisdiction and cyberspace. *In Law*, 6.

Herveg, J., & Gayrel, C. (2009). Décisions de la Cour européenne des droits de l'homme relative à l'article 8 de la Convention européenne des droits de l'homme. In de Terwangne, C., & Dussollier, S. (Eds.), *Chronique de jurisprudence en droit des technologies de l'information (2002-2008), Revue du Droit des Technologies de l'Information, 35.* Brussels, Belgium: Larcier.

Hillman, R. A., & Rachlinski, J. J. (2001). *Standard-form contracting in the electronic age.* Retrieved on January 30, 2010, from http://www/ ssrn.com

International Working Group on Data Protection in Telecommunications (Berlin Working Group). (March 4, 2008). Report and guidance on privacy in social network services. Rome Memorandum. Retrieved January 30, 2010, from www. datenschutz-berlin.de

Jefferey, K., & Neidecker-Lutz, B. (Eds.). (2010). *The future of cloud computing, opportunities for European cloud computing beyond 2010.* Report written for the European Commission, Information Society and Media, public version 1.0. Retrieved on February 10, 2010, from http://cordis.europa. eu/fp7/ict/ssai/docs/cloud-report-final.pdf

Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer Law & Security Review, 25.*

Jones, A., & Sufrin, B. (2008). *EC competition law.* Oxford, United Kingdom: Oxford University Press.

Kane, B., & Delange, B. T. (2009). A tale of two Internets: Web 2.0 slices, dices, and is privacy resistant. *Idaho Law Review, 45*, 2009.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, 50.

Kang, J., & Buchner, B. (2004). Privacy in Atlantis. *Harvard Journal of Law & Technology*, 18.

Katz, M. L., & Shapiro, C. (1994). Systems competition and network effects. Retrieved on January 30, 2010, from http://www.utdallas.edu/~liebowit/knowledge_goods/k&sjel94/jel94.html.

Kéfer, F., & Cornelis, S. (2009). L'arrêt *Copland* ou l'espérance légitime du travailleur quant au caractère privé de ses communications. *Revue Trimestrielle des Droits de l'Homme, 79.*

Kerr, O. S. (2004). A user's guide to the Stored Communications Act, and a legislator's guide to amending it. *The George Washington Law Review, 72.*

Kerr, O. S. (2010). (forthcoming). Vagueness challenges to the Computer Fraud and Abuse Act. [from http://www.ssrn.com]. *Minnesota Law Review*. Retrieved on March 20, 2010.

Keustermans, J., & Mols, F. (2001-2002). De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht. *Rechtskundig Weekblad, 21.*

Killingsworth, S. (1999). Minding your own business: Privacy policies in principle and in practice. *Journal of Intellectual Property Law, 7.*

King, N. J. (2008). Fundamental human right principle inspires U.S. data privacy law, but protections are less than fundamental. In Pérez Asinari, M. V., & Palazzi, P. (Eds.), *Défis du droit à la protection de la vie privée: perspectives du droit européen et nord-américain. Cahiers du C.R.I.D. (no. 31)*. Brussels, Belgium: Bruylant.

Korff, D., Brown, I., et al. (2010). *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*. Final report delivered in the framework of contract JLS/2008/C4/011, European Commission, Directorate-General Justice, Freedom and Security, 20 January 2010. Retrieved on September 15, 2010, from http: // ec.europa. eu/justice/policies/ privacy/docs/studies/ new_privacy_challenges/ final_report_en.pdf

Kuner, C. (2010). Data protection law and international jurisdiction on the Internet (Part 1 & 2). *International Journal of Law and Information Technology, 2 & 3.*

Kuty, F. (2009). Principes généraux du droit pénal belge: *Vol. I. La loi pénale*. Brussels, Belgium: De Boeck & Larcier.

Labrusse, C. (1974). Droit constitutionnel et droit international privé en Allemagne fédérale. *Revue Critique de Droit International Privé*, 1-46.

Lambert, P. (1999). Bescherming van prive-(tele) communicatie. In J. Dumortier (Ed.), *Recente ontwikkelingen in informatica- en telecommunicatierecht*. Brugge, Belgium: die Keure.

Leberton, G. (2009). *Libertés publiques et droits de l'Homme*. Paris, France: Dalloz.

Le Métayer, D., & Monteleone, S. (2009). Automated consent through privacy agents: Legal requirements and technical architecture. *Computer Law & Security Review, 25.*

Léonard, T. (2001). *E-commerce* et protection des données à caractère personnel, quelques considérations sur la licéité des pratiques nouvelles de *marketing* sur *internet*. In Byttebier, K., Feltkamp, R., & Janssens, E. (Eds.), *Internet en Recht*. Antwerpen, Belgium: Maklu.

Levin, A., & Sánchez Abril, P. (2009). Two notions of privacy online. *Vanderbilt J. of Ent. And Tech. Law, 11*, 1017.

Levinet, L. (2008). *Théorie générale des droits et libertés*. Brussels, Belgium: Bruylant, Nemesis.

Lind, R. C., & Muysert, P. (2003). Innovation and competition policy: Challenges for the new millennium. *European Competition Law Review, 24.*

Lobe, B., & Staksrud, E. (Eds.). (2010). *Evaluation of the implementation of the safer social networking principles for the EU part ii: testing of 20 providers of social networking service in Europe*. Report written for the European Commission under the Safer Internet Programme. Luxembourg, January 2010, (p. 24). Retrieved January 30, 2010, from http: //ec.europa. eu/information_society/activities/social_networking/eu_action/implementation_princip/index_en.htm

Louveaux, S., & Pérez Asinari, M. V. (2008). Introduction. Directive 2002/58: The Need of Specific Legislation. In Pérez Asinari, M. V., & Palazzi, P. (Eds.), *Défis du droit à la protection de la vie privée: perspectives du droit européen et nord-américain. Cahiers du C.R.I.D. (no. 31)*. Brussels, Belgium: Bruylant.

Madrid Resolution. (November 5, 2009). *Joint proposal for a draft of international standards on the protection of privacy with regard to the processing of personal data.* 31st International Conference of Data Protection and Privacy Commissioners. Retrieved on October 15, 2010, from http: //www.privacyconference2009. org/media/Publicaciones/common/ estandares_resolucion_madrid_en.pdf

Manny, C. H. (2003). Personal privacy-transatlantic perspectives, European and American privacy: commerce, rights and justice – part I. *Computer Law & Security Report*, 19.

Mantouvalou, V. (2008). Human rights and unfair dismissal: Private acts in public spaces. *The Modern Law Review*, 71.

Mayer, P. (1991). La Convention européenne des droits de l'homme et l'application des normes étrangères. *Revue Critique de Droit International Privé, 4.*

Mercado Kierkegaard, S. (2005). Lobbyism and the opt in/opt out cookie controversy: How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Report*, 21.

Meron, T. (April 26, 2000). *The implications of the European Convention on Human Rights for the development of public international law.* Ad Hoc Committee of Legal Advisers on the International Public Law (CAHDI). Retrieved on January 30, 2010, from https: //wcd.coe.int/ViewDoc.jsp?id=348429 &Site=COE&BackColorInternet=DBDCF2 &BackColorIntranet=FDC864&BackColorLogged=FDC864

Moine, I. (1997). *Les choses hors commerce: Une approche de la personne humaine juridique.* Paris, France: Librairie Génrale de Droit et de Jurisprudence.

Moiny, J.-P., & De Groote, B. (2009). Cyberconsommation et droit international privé. *Revue du Droit des Technologies de l'Information, 37.*

Moiny, J. P. (2010). Facebook au regard des règles européennes de protection des données. *European Journal of Consumer Law, 2.*

Moiny, J.-P. (2010/1). Contracter dans les réseaux sociaux: Un geste inadéquat pour contracter sa vie privée. *Revue de la Faculté de Droit de l'Université de Liège, 2.*

Moreno, O., & Van Koekenbeek, S. (2008). Les enjeux de la vie privée au travail et sa dynamique dans l'entreprise. In Docquir, B., & Puttemans, A. (Eds.), *Actualités du droit de la vie privée.* Brussels, Belgium: Bruylant.

National Institute of Standards and Technology. Information Technology Laboratory, Mell, P., & Grance, T. (July 10, 2009). *The NIST definition of cloud computing*, version 15. Retrieved on February 10, 2010, from http: //csrc.nist. gov/ groups/SNS/ cloud-computing/

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review (Seattle, Wash.)*, 79.

Nowak, M. (2003). *Introduction to the international human rights regime*. Leiden, The Netherlands & Boston, MA: Martinus Nijhoff.

Office of Privacy Commissionner of Canada, & Barrigar, J. (February, 2009). *Social network site privacy: A comparative analysis of six sites*. Retrieved on January 30, 2010, from http: //www.priv. gc.ca/information/pub/sub_comp_200901_e.pdf

Phillipson, G. (1999). The Human Rights Act, horizontal effect and the common law: A bang or a whimper. *The Modern Law Review*, 62.

Polański, P. P. (2007). *Customary law of the Internet: In the search for a supranational cyberspace law*. La Haye, The Netherlands: T.M.C. Asser Press.

Posner, R. A. (November, 2000). *Antitrust in the new economy*. Retrieved on January 30, 2010, from http://www.ssrn.com

Poullet, Y. (2008). Pour une troisième génération de réglementation de protection des données. In Pérez Asinari, M. V., & Palazzi, P. (Eds.), *Défis du droit à la protection de la vie privée: perspectives du droit européen et nord-américain. Cahiers du C.R.I.D. (no. 31)*. Brussels, Belgium: Bruylant.

Poullet, Y., & Rouvroy, A. (2009). Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. In *Etat de droit et virtualité*. Montréal, Canada: Thémis.

Poullet, Y., & Rouvroy, A.(2009/1). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., & Nouwt, S. (Eds.), *Reinventing data protection*. Springer Verlag.

Poullet, Y. (2010). About the e-privacy directive: Towards a third generation of data protection legislation. In Gutwirth, S., Poullet, Y., & de Hert, P. (Eds.), *Data protection in a profiled world*. Springer. doi:10.1007/978-90-481-8865-9_1

Purtova, N. (2009). Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review, 25*.

Richards, N. M., & Solove, D. J. (2007). Privacy's other path: Recovering the law of confidentiality. *The Georgetown Law Journal*, 96.

Rigaux, F. (1980). La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel. *Revue Critique de Droit International Privé*, 444-478.

Rigaux, F. (1998). *La protection de la vie privée et des autres biens de la personnalité*. Brussels, Belgium: Bruylant.

Rosier, K. (2008). La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative au traitement des données à caractère personnel: comment les (ré) concilier? In Pérez Asinari, M. V., & Palazzi, P. (Eds.), *Défis du droit à la protection de la vie privée – Perspectives du droit européen et Nord-américain, coll. Cahiers du C.R.I.D. (no. 31)*. Brussels, Belgium: Bruylant.

Samuelson, P. (2000). Privacy as intellectual property? *Stanford Law Review*, 52.

Schwartz, P. M., & Reidenberg, J. R. (1996). *Data privacy law. United States of America*. Virginia: Michie.

Schwartz, P. M. (2004). Property, privacy, and personal data. *Harvard Law Review*, 117.

Scolnik, A. (2009). Protections for electronic communications: The Stored Communications Act and the Fourth Amendment. *Fordham Law Review*, 78.

Shin, D., & Lopes, R. (2009). *Enabling interoperable and selective data sharing among social networking sites*. In CollaborateCom 2008, The 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing. Springer.

Simmons, J. L. (2009). Buying you: The government's use of fourth-parties to launder data about the people. *Columbia Business Law Review, 3.*

Soghoian, C. (August, 2009). Caught in the cloud: Privacy, encryption, and government back doors in the Web 2.0 era. Retrieved on February 20, 2010, from www.ssrn.com

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 90.

Solove, D. J., & Hoofnagle, C. J. (2006). A model regime of privacy protection. *University of Illinois Law Review*, 2.

Sorosky, S. B. (2008). United States v. Forrester: An unwarranted narrowing of the fourth amendment. *Loyola of Los Angeles Law Review*, 41.

Sprague, R. (2008). Orwell was an optimist: The evolution of privacy in the United States and its de-evolution for American employees. *The John Marshall Law Review*, 42.

Spulber, D. F. (2008). Consumer coordination in the small and in the large: Implications for antitrust in markets with network effects. Retrieved on January 30, 2010, from http://www.ssrn.com

Strahilevitz, L. J. (December, 2004). *A social networks theory of privacy*. Retrieved on January 30, 2010, from http://www.ssrn.com

Sudre, F. (2008). *Droit Européen et international des droits de l'homme*. Paris, France: Presses Universitaires de France.

Sudre, F. (2009). *Les grands arrêts de la Cour européenne des Droits de l'homme*. Paris, France: Presses Universitaires de France.

Berkeley, U. C. School of Information, Gomez, J., Pinnick, T., & Soltani, A. (June 1st, 2009). *KnowPrivacy*. Retrieved January 30, 2010, from http://knowprivacy.org/

Vandermeersch, D. (1997). Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs). In H. Bartholomeeusen, e.a. (Eds.), *Internet sous le regard du droit.* Brussels, Belgium: Editions du jeune barreau de Bruxelles.

van der Plancke, V., & Van Leuven, N. (2008). La privatization du respect de la convention européenne des droits de l'homme: faut-il reconnaître un effet horizontal generalisé? In *Entre ombres et lumières: cinquante ans d'application de la convention européenne des droits de l'homme en Belgique* (pp. x–x). Brussels, Belgium: Bruylant.

Van Linthout, P., & Kerkhofs, J. (2008). Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel. *Tijdschrift voor Strafrecht,* 2.

Van Overstraeten, T., Bruyndonckx, B., Szafran, E., & Rousseau, S. (2005). Belgium finally adopted the Electronic Communications Act transposing the EU telecom Package. *Computer and Telecommunication Law Review, 11.*

Vaquero, L. M., Rodero Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. *Computer Communication Review*, 50. Retrieved on February 20, 2010, from http: //ccr.sigcomm. org/drupal/files/p50-v39n1l-vaqueroA.pdf

Veljanovski, C. (2001). E.C. antitrust in the new European economy: Is the European Commission's view of the network economy right?. *European Competition Law Review, 22.*

Volokh, E. (2000). Freedom of speech, information privacy, and the troubling implications of a right to stop people from speaking about you. *Stanford Law Review*, 52.

W3C. (2009). *Workshop on the Future of Social Networking*. Final report, Barcelona, 15-16 January 2009. Retrieved on January 15, 2010, from http: //www.w3. org/2008/09/ msnws/report.

Walden, I. (2007). Privacy and data protection. In Reed, C., & Angel, J. (Eds.), *Computer law, the law and regulation of Information Technology*. Oxford, United Kingdom: Oxford University Press.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4.

Wong, R. (October, 2008). *Social networking: Anybody is a data controller!* Retrieved on January 30, 2010, from http://papers.ssrn.com/

Working Party 29. (November 21, 2000). *Privacy on the Internet – An integrated EU approach to online data protection*. WP37. Retrieved on January 30, 2010, from http: //ec.europa. eu/justice/ policies/ privacy/workinggroup/ index_en.htm

Working Party 29. (November 25, 2005). *Opinion on the use of location data with a view to providing value-added services*. WP 115. Retrieved on January 30, 2010, from http: //ec.europa. eu/justice/ policies/ privacy/workinggroup/ index_en.htm

Working Party 29. (April 4, 2008). *Opinion 1/2008 on data protection issues related to search engines.* WP148. Retrieved on January 30, 2010, from http: //ec.europa. eu/justice/policies/ privacy/ workinggroup /index_en.htm

Working Party 29. (June 12, 2009). *Opinion 5/2009 on online social networking*. WP163. Retrieved on January 30, 2010, from http: // ec.europa. eu/justice/policies/ privacy/working-group/ index_en.htm

Working Party 29. (December 1st, 2009). *The future of privacy*. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Retrieved on January 30, 2010, from http: //ec.europa. eu/justice/policies/ privacy/working-group /index_en.htm

Working Party 29. (February 16, 2010). *Opinion 1/2010 on the concepts of controller and processor*. WP169. Retrieved on May 20, 2010, from http: //ec.europa. eu/justice/policies/ privacy/ workinggroup /index_en.htm

Working Party 29. (June 22, 2010). *Opinion 2/2010 on online behavioural advertising*. WP171. Retrieved on September 3, 2010, from http: // ec.europa. eu/justice/policies/ privacy/docs/wp-docs/ 2010/wp171_en.pdf

Working Party 29. (December 16, 2010). *Opinion 8/2010 on applicable law*. WP179. Retrieved on January 5, 2010, from http: //ec.europa. eu/ justice/policies /privacy/docs/wpdocs/ 2010/ wp179_en.pdf.

Youseff, L., & Butrico Dilma Da Silva, M. (2009). *Toward a unified ontology of cloud computing*. Retrieved on February 20, 2010, from http: // www.cs.ucsb.edu/~lyouseff/CCOntology/ Cloud-Ontology.pdf

Zwaak, L. (2006). General survey of the European Convention. In P. van Dijk, F. van Hoof, A. van Rijn & L. Zwaak (Eds.), *Theory and practice of the European Convention on Human Rights*. Antwerpen, Belgium & Oxford, United Kingdom: Intersentia.

ENDNOTES

1 *See also* no. 105. This complaint has been supplemented, *see* EPIC v. Facebook 2 (2010).

2 *See also* Lobe & Staksrud, 2010, p. 24. Here Facebook's declaration to adhere to the Safer Social Networking Principles for the EU has been deemed partially compliant, notably with, principle 3 ("empower users through tools and technology"), and so are the measures implemented on the SNS as regards the self-declaration.

3 The present paper does not study conflicts that could exist between, on the one hand, privacy and data protection and, on the other hand, the freedom of expression or other fundamental rights or liberties.

4 As regards the analysis of consumer complaints, the *KnowPrivacy* study concludes that "[t]he biggest concern among the complaints we coded was the *lack of control*" (UCBSI, 2009, p. 32).

5 As regards the concepts of prescriptive and adjudicative jurisdictions, *see* Kuner, 2010, p. 185.

6 For a more complete definition, *see* Boyd & Ellison, 2007, p. 2. *See also* Working Party 29, WP163, pp. 4-5).

7 The purpose principally takes Facebook into consideration–and therefore, any "Facebook like" SNS –, sometimes approaching other SNSes. *See infra* for considerations related to the SNS market.

8 "Web 2.0 capitalizes on advances made in the ability to share information through the Internet" (Kane & Delange, 2009, p. 322).

9 As a rule, Facebook only hosts its own applications.

10 As regards common characteristics of SNS, *see* European Network and Information Security Agency [ENISA], 2007, p. 5.

11 About "cloud computing", *see* Buya, Yeo & Venugopal, 2008; Jefferey & Neidecker-Lutz, 2010, pp. 9-10; National Institute of Standards and Technology, 2009; ENISA, 2009, pp. 14-15; Soghoian, 2009, pp. 5-12; Vaquero, Rodero Merino, Caceres & Lindner, 2009, p. 50; Youssef & Butrico Dilma Da Silva, 2009.

12 *See e.g.* http://www.datacenterknowledge.com/archives/2009/04/17/a-look-inside-facebooks-data-center/, last visited on January 10, 2010.

13 These applications can be hosted on the servers of the developer of the application (or, of course, its subcontractor's servers). An application constitutes software as a service.

14 *See* Article 1, 2), a) Directive 98/48/EC, and Article 14 Directive 2000/31/EC. Later in the paper, the potential qualification of SNSes as electronic communication services, at least as regards some services, will shortly be discussed.

15 Whether they are directly remunerated or not by users, *see* Recital 18 Directive 2000/31/EC.

16 "Advertising is key to the business model of most SNS", Office of Privacy Commissioner of Canada [OPCC], 2009, p. 41.

17 *See* http://www.facebook.com/advertising/?src=awgl01&v=ntl1, http://www.insidefacebook.com/2008/10/30/facebook-advertising-resources-the-6-types-of-ads-on-the-new-home-page/; http://www.insidefacebook.com/2009/01/27/facebook-relaunches-polls-as-new-home-page-engagement-ad/, http://www.insidefacebook.com/2009/09/23/facebooks-new-sampling-engagement-ads-now-available-for-brands/, last visited on January 10, 2010.

18 E.g. "you grant [Facebook] a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook

("IP License")", notably stipulates the Statement of Rights and Responsibilities – formerly called "Terms of Use."

19 *See supra* the introduction.

20 *See* Article 102 of the Treaty on the Functioning of the European Union. The prohibition provided for in this Article applies when five elements are established: one or more undertakings, a dominant position, the dominant position being held within the common market or a substantial part of it, an abuse (the acts detailed in the Article only being examples) and an effect on inter-State trade (Jones & Sufrin, 2008, p. 298).

21 If tomorrow I leave Facebook, will my friends follow me? I don't think so. Maybe if their friends (our common friends and their exclusive friends) follow them. Then what about the friends of these friends? Which critical mass of "friends" will I have to convince?

22 *See* Nederlandsche Banden Industrie Michelin v. Commission of the European Communities (1983), no.37: "The possibilities of competition must be judged in the context of the market comprising the totality of the products which, with respect to their characteristics, are particularly suitable for satisfying constant needs and are only to a limited extent *interchangeable* with other products" (emphasis added by author). *See also* EC Commission, 1997, no.7, for instance recently quoted by the Court of First Instance in Microsoft Corp. v. Commission (2007), no.484. The question of the relevant geographic market is put aside taking as a premise that SNS such as Facebook are targeted to the whole Community market. However, an SNS could be limited to a Country, *see infra*. Also, a SNS could *de facto* be geographically limited by the use of particular languages (such as Japanese, *see* http://mixi.jp). Furthermore, it can be underlined that the "Small but Significant and Non-Transitory Increase in Price" test for the market definition (as regards this concept, *see* DG Competition discussion paper nos. 14-17.) can be less relevant "when competition is based on drastic innovations leading to the replacement of the current dominant firm, not on price competition between competitors" (Lind & Muysert, 2003, p. 88). As regards SNS, usually, users do not have to directly pay any price in coin money. As previously explained, in the context of multi-sided platforms like Facebook, the functionalities of Facebook for which we have to pay will lead to the providing of free users profiles. Therefore, it will generally make no sense for an SNS provider to charge its average users. Except sometimes (*e.g. see infra* as regards Hi5), when the SNS provider proposes to pay a fee in place of publishing advertisements on the website, or some SNS could usually be paying (dating SNS, etc.). If the SSNIP-Test is applied to Facebook, the website then becoming paying, most probably, users will move, for instance, to MySpace or Netlog. Most probably also, if other Facebook-like SNS didn't exist, web surfers would stop using the SNS, coming back to traditional instant messaging networks (such as MSN Messenger, Yahoo Chat, etc.), which would lead to the "cellophane fallacy." In this respect, if Facebook, with Facebook Chat, is arguably also on the market of instant messaging, MSN Messenger doesn't pertain to the market of Facebook-like SNS.

23 But we could wonder if, as regards the Marketplace application coupled to the Facebook network through the API platform, Facebook would not be on the same relevant market than eBay.

24 Another viewpoint could be taken, for instance as regards the market of e-advertising or even the one of targeted advertising.

25 As regards this concept, *see* Jones & Sufrin, 2008, pp. 65-78.

[26] *See also* Katz & Shapiro, 1994. Network effects are also called network externalities or economies of scale in consumption, *see* (Posner, 2000, p. 2).

[27] The switching costs would still be higher if users, relying on cloud computing technologies (SNS providers generally providing data storage as a service), deleted their data from their own personal computers and then had to bring them back from the cloud provider.

[28] Admittedly, according to what has been suggested, this could also lead to the creation of a new market.

[29] The authors "define platform envelopment as entry by one platform provider into another's market, combining its own platform's functionality with the target's in a multi-platform bundle that leverages shared user relationships and common components" (Eisenmann, Parker, & Van Alstyne, 2009, p. 1).

[30] *See*http://kara.allthingsd.com/20081124/when-twitter-met-facebook-the-acquisition-deal-that-fail-whaled/, last consulted the May 7, 2010.

[31] "Given the growing number and maturity of data interoperability formats and protocols, there is a significant opportunity for social networks to reduce the detrimental effects of architectural silos by opening their closed communities for the benefit of users. Totally distributed social networking is a possible future scenario" (W3C Workshop, 2009, p. 5). The report however underlined that the "difficulty of sharing users' assets (i.e. the user generated content posted on a given social network) across social networks was mentioned as a potential area where further work would be beneficial" (p. 7). *See for instance* Shin & Lopes, 2009, pp. 439-450. *See also* the Webpage of the W3C Social Web Incubator Group whose mission "is to understand the systems and technologies that permit the description and identification of people, groups, organizations, and user-generated content in extensible and privacy-respecting ways" (http://www.w3.org/2005/Incubator/socialweb/, last visited on September 3, 2010).

[32] The author emphasized that, "[a]s social-network-site data becomes more portable, it also becomes less secure – and thus less private. The supposedly privacy-promoting solution so badly misunderstands the social nature of relationships on social network sites that it destroys the privacy it means to save" (Grimmelmann, 2009, pp. 1194-1195). It could be imagined that the migration of data to another SNS is depending on the redefining of the privacy settings on the new SNS. Given that before any choice of privacy settings, data would be totally inaccessible by defaults.

[33] "Market power is the power to influence market prices, output, innovation, the variety or quality of goods and services, or other parameters of competition on the market for a significant period of time" (EC DG Competition, 2005, no.24).

[34] "The dominant position thus referred to relates to a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by affording it *the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of the consumers*" (emphasis added by author) (Hoffmann-La Roche & Co. AG v Commission of the European Communities (1979), no.38).

[35] EPIC Before the FTC supp., 2010, no.1. For October 2009 statistics, *see* for instance http://www.hitwise.com/index.php/us/press-center/press-releases/2009/social-networking-sept-09/, last visited August 15, 2010. This reference puts Facebook, MySpace and Twitter in the same market.

[36] Which "has become almost synonymous with the information technology industries including computer software, hardware, internet-based businesses and associated technologies such as wireless communications", but "also includes biotechnology, medical devices, pharmaceuticals, aerospace and others" (Lind & Muysert, 2003, p. 87).

[37] The authors underline that "market contestability" would be a better indicator of market power. As regards Facebook-like SNS, it could be argued that Facebook does not enjoy a "position of dominance because potential entry imposes an effective competitive constraint on its conduct." Putting into perspective the impact of network effect, C. Veljanovski (2001, p. 117) writes that "[p]arts of the new economy, even though subject to a process of "serial monopolization", do not inflict the harmful effects attributed to static monopolies."

[38] Posner underlines that "the prospect of a network monopoly should thus induce not only a high rate of innovation but also a low-price strategy that induces early joining and compensates the early joiners for the fact that eventually the network entrepreneur may be able to charge a monopoly price."

[39] About the Facebook iPhone application, *see* EPIC et al. before the FTC, 2009, nos 26-44. In this case, the contacts list of an iPhone user (identities and phone number) are communicated to Facebook, while "[s]ome Facebook users and non-Facebook users have consciously chosen *not* to provide Facebook with their contact information" (EPIC et al. before the FTC, 2009, no.39).

[40] This application makes it possible to inform user's friends of what the latter did on other websites insofar as these websites subscribe to the Facebook Beacon application). This is at present litigated in the United States, Facebook having proposed (*see*http://www.beaconclasssettlement.com/, last visited on October 10, 2010), which has been approved in March 2010 (*see*http://www.wired.com/threatlevel/2010/03/facebook-beacon-2, last visited on October 21, 2010).

[41] *See*http://www.facebook.com/policy.php, last visited on January 10, 2010; EPIC v. Facebook 3, 2010, no.89.

[42] For instance, the terms of use of Facebook, LinkedIn and MySpace notably compel users to provide their real names during the subscribing process.

[43] As regards "tracking cookies" and "flash cookies", *see* WP171, 2010, pp. 6-7.

[44] About this case, *see notably* Edwards, 2009, pp. 512-515 and 528-531.

[45] *See also* Dinant, 2000, pp. 278-282; Mercado Kierkegaard, 2005, pp. 314 and ff.; Working Party 29, WP37, 2000, p. 16.

[46] This hypothesis makes sense when the social network can be publicly consulted (*e.g.* MySpace, some parts of profiles on Facebook and LinkedIn, YouTube, etc.).

[47] Users can read, in the second title of the Privacy Policy (last revised on December 22, 2010), what follows:

Information we collect when you interact with Facebook: Site activity information. We keep track of *some of the actions you take on Facebook, such as* adding connections (including joining a group or adding a friend), creating a photo album, sending a gift, poking another user, indicating you "like" a post, attending an event, or connecting with an application. In some cases you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content you uploaded, we might log the fact that you shared it. Access Device and Browser Information. When you access Facebook from a computer, mobile phone, or other device, we may collect information from that device about your browser type,

location, and IP address, as well as *the pages you visit.*" (Emphasis added by author).

48 *Clickstream* data consists of information about the Internet activity of a web surfer due to his browsing through a website. *See* Garrie & Wong, 2006, pp. 565-567; Bucklin & Sismeiro, 2008.

49 In this case, it is necessary for Facebook to store which group a user has joined. If this were not the case the user would have systematically join each group he wants to consult again, etc.

50 Facebook modifies the service it offers, on its servers (or those of its subcontractors) and the user does not have any control over such evolutions and they *have to* consent if they want to continue to use the website.

51 It can be noted that, in the United States, a "data security breach incident" is typically one that draws the U.S. Federal Trade Commission's [FTC] attention (Ciocchetti, 2007, pp. 94-95). The Twitter case recently illustrated it (In the matter of Twitter Inc., 2010).

52 The use of applications however requires greater disclosures of information.

53 Formerly, a user could join a Region network. Users can no longer join such networks but they can specify a location in their profile.

54 Most probably due to the EPIC complaint before the FTC and the users' opposition.

55 *See supra.*

56 To this respect, the website has been last tested on October 15, 2010.

57 *See* OPCC, 2009, p. 17.

58 "To request that we close your account and remove your information from the LinkedIn website, please send your request to customer_service@linkedin.com. Please send your request using an email account that you have registered with LinkedIn under your name. You will receive a response to requests sent to customer_service@linkedin.com within five business days of its receipt" (http://www.linkedin.com/static?key=privacy_policy, last visited on January 15, 2010). It has to be noted that according to the new privacy policy (last consulted on October 15, 2010), the deletion of the account seems easier.

59 *See* OPCC, 2009, p. 29.

60 *See also* at the European level, Article 7 (privacy) and 8 (data protection) Charter of Fundamental Rights of the European Union, 12 December 2007, which has now the same legal value as the Treaties, *see* Article 6.1 of the Treaty on European Union; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg, 28 January, 1981, hereinafter referred to as "ETS 108", and its Additional Protocol regarding supervisory authorities and transborder data flows, adopted in Strasbourg, 8 November 2001. At an international level, *see* Article 17, International Covenant on Civil and Political Rights, adopted by General Assembly resolution 2200A (XXI) of 16 December 1966; O.E.C.D. Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data, 23 September 1980. And at the Belgian level, *see* Article 22 of the *Constitution coordonnée*, 17 February 1994 and the Belgian Privacy Act hereinafter referred to as "LVP."

61 The concept of privacy is "*contingent au contexte sociétaire dans lequel nos capacités autonomiques en tant qu'individus doivent être protégées*" (Poullet & Rouvroy, 2009, p. 190).

62 D.J. Solove identifies six conceptions of privacy: "The Right to Be Let Alone", "Limited Access to the Self", "Secrecy", "Control Over Personal Information", "Personhood", "Intimacy" (Solove, 2002, pp. 1099-1124). As regards privacy, *see generally and notably*

Docquir, 2008; Poullet, 2008, pp. 35-38; Rigaux, 1998.

63 I.e. it is, to some extent, a shield against discrimination.

64 *See* Herveg & Gayrel, 2009, pp. 104-105.

65 Article 6.1, b) Directive 95/46/EC.

66 Article 6.1, b) and c) Directive 95/46/EC.

67 As regards Article 8 ECHR specifically, *see* Zwaak, 2006, pp. 729 and 743; Sudre, 2008, pp. 191-204 and 245-258; Moreno & Van Koekenbeek, 2008, pp. 44-47 and 49-52.

68 *See notably* Berman, 2006, pp. 1080-1085; Zwaak, 2006, pp. 28-32; Levinet, 2008, p. 61; Nowak, 2003, p. 53. L. Zwaak (2006, p.29) writes that two views of the *Drittwirkung* can be identified, one stating that human rights "*apply*" to the legal relation between private parties, and another one enabling the individual to *enforce* the rights against another individual.

69 As an example of direct horizontal effect, R. Clayton and H. Tomlinson (2001, pp. 217-218) write that "in Ireland it is well established that constitutional guarantees have direct horizontal application to litigation between private individuals", the Irish constitution itself directly imposing obligations on private individuals. But in the UK, G. Phillipson (1999, pp. 824 and ff.) and V. Mantouvalou (2008, pp. 916-917) state that the Human Rights Act (1998) – and privacy in particular – does not have a direct horizontal effect because it does not create a cause of action between private parties.

70 *See* van der Plancke & Van Leuven, 2008; Gardbaum, 2003, pp. 394-411.

71 *See* van der Plancke & Van Leuven, p. 205, for examples as regards Belgium. As regards France and a possible direct horizontal effect of the ECHR, *see* Sudre, 2009, pp. 31-32. F. Sudre underlines that before a national Court, the question of the direct horizontal effect coincides with that of the "direct effect" or "self-executing", which originally is not the same since it refers to ability of a Covenant to have effects in domestic law – and the differences between monism and dualism. As regards the direct applicability of treaties, *see notably* Berman, 2006, pp. 1093-1095.

72 For instance in the UK, the Human Rights Act (1998) explicitly stipulates that "it is unlawful for a public authority to act in a way which is incompatible with a Convention right" (s.6 (1)), understood that the concept of public authority includes a court or a tribunal (s.6 (3)(a)).

73 The measures that a State could be obliged to take due to the positive obligations it has can not be disproportionate as regards the individual interests to protect.

74 *See* van der Plancke & Van Leuven, 2008, p. 212, who borrow the words from B. Dickson (1999, pp. 59 and ff.).

75 And of course, if this violation also results from its *actions or encouragements*. "This accountability on the one hand depends on the type of human right concerned, and on the other, what measures the state has taken to protect against violations by private persons in general, and in individual cases" (Nowak, 2003, p. 53). *See* van der Plancke & Van Leuven, 2008, pp. 215-218).

76 Of course, it is impossible for any individual to introduce a recourse before the European Court of Human Rights *against another individual*. This would be contrary to the *ratione personae* competence of the Court, *see notably* Article 34 ECHR.

77 *See infra* footnotes nos. 135 and 136.

78 About U.S. privacy law, *see generally* Purtova, 2009, pp. 508-514.

79 As regards these torts, *see notably* Dunne, 2009, pp. 195-197.

80 For a summary about the Constitutional Right to Privacy, *see* Sprague, 2008, pp. 103-110; Purtova, 2009, pp. 512-513; Dunne, 2009, pp. 197-237.

[81] S. Gardbaum (2003, p. 415) wrote that the American Constitution has a "strong indirect horizontal effect", referring to the conceptualization of the indirect horizontal effect suggested by Phillipson (1999). According to S. Gardbaum, this means that "all law – including, of course, all private law – is directly and fully subject to constitutional rights and may be challenged in private litigation. This, in turn, means that constitutional rights fully protect the individual whether it is another individual or the government that seeks to rely on an unconstitutional law", (Gardbaum, 2006, p. 766). The indirect effect results from the hierarchy of the norms and from the fact that the government, the courts (adjudicating litigations), etc., are subject to the Constitution. As regards UK, *see* footnote nr 72.

[82] Referring to the common law (privacy tort) and the Californian Constitution, the Supreme Court of California, in Hernandez v. Hillsides (2009), recently underlined that these "two sources of privacy protection 'are not unrelated' under California law." Citing another decision, the Court recalled that the right to privacy in the California Constitution "creates at least a limited *right of action* against *both private and government* entities" (emphasis added by the author). In the case submitted to the Court, both the common law and the Constitution were invoked. Therefore, it seems that the Californian right to privacy could even have a *limited* direct horizontal effect. Admittedly as regards this Californian constitutional right to privacy, the Court stated that the individual must possess a "legally protected privacy interest" [...] "determined by established social norms *derived from such sources as the common law and statutory enactment*" (emphasis added by the author). But the Court nevertheless refers to two causes of action.

[83] Regarding other weaknesses, *see* Richards & Solove, 2007, pp. 175-176; Sprague, 2008, pp. 101-102; King, 2008, p. 97; Strahilevitz, 2004, pp. 9-10; N. Purtova, 2009. As regards the intrusion upon seclusion tort, *see* Dalsen, 2009, pp. 1071-1075.

[84] The European Court of Human Rights has already taken into account the reasonable expectations of privacy of the individual who claims a violation of his privacy, for instance, in the work context, *see* Kéfer & Cornelis, 2009, p. 784.

[85] *See also* Poullet & Rouvroy, 2009/1, p. 48.

[86] As regards the monitoring of the activity of Internet users, *see* Sorosky, 2008, p. 1137.

[87] It has to be pointed out that reasonable expectation of privacy is only subjective as far as torts are concerned, but should be objective (i.e. that society will accept them) as regards constitutional rights (Strahilevitz, 2004, p. 13, footnote no.29; Sprague, 2008, p. 106). W. Dalsen (2009, pp. 1071-1075) however also refers to an objective expectation for privacy as regards the intrusion upon seclusion tort. *See* Hernandez v. Hillsides.

[88] The Supreme Court (City of Ontario v. Quon, 2010, pp. 10-12) decided that: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." "At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve." "A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds."

[89] R. Sprague (2008, p. 125) writes: "[u]nder the *Florida v. Riley* plurality's approach, the expectation of privacy is defeated if a single member of the public could conceivably position herself to see into the area in question without doing anything illegal."

"According to Webster's initial definition, information may be classified as 'private' if it is 'intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public'" (U.S. Dep. of Justice v. Reporters Committee, 1989).

90 For a criticism, *see* Sorosky, 2008, pp. 1121-1142. This case is an application of the "third-party doctrine." While the author correctly points out that "individuals have no viable choice but to reveal information to a third party"; "the third-party argument should not apply when a defendant relies on a mode of communication and has no choice but to continue using that mode, despite the existence of a third-party intermediary", (Sorosky, 2008, pp. 1133-1134). For a discussion related to the Fourth Amendment and cloud computing, *see* Couillard, 2009, pp. 2205 and ff.

91 J. Kang (1998) identifies, under the word "privacy", three "clusters" of ideas, functionally interconnected and often concomitantly involved in a same situation: "space, decision and information." He focuses on the third concept.

92 *See notably* the Privacy Act (1974), the Fair Credit Reporting Act (1970), the Cable TV Privacy Act (1984), the Children's Online Privacy Protection Act (1998) and the Video Privacy Protection Act (1988). About these acts, *see* Solove & Hoofnagle, 2006, pp. 359-368. As regards the Video Privacy Protection Act, *see* Viacom v. YouTube (2008), where the District Court for the Southern District of New York refused to extend its scope to videos watched through YouTube.

93 "An entire industry devoted primarily to processing and disseminating personal information", (Solove & Hoofnagle, 2006, p. 359.

94 *See* Gindin, 2009, pp. 28-35.

95 Nonetheless our purpose is not to ignore or diminish the potential huge benefits to which self-regulation can lead.

96 For a comparison between U.E. and U.S. perspectives, *see* Dhont & Pérez Asinari, 2003, pp. 79-96.

97 *See*http://www.export.gov/safeharbor.

98 *See for example,* in California, the Online Privacy Protection Act of 2003 – Business and Professions Code sections 22575-22579.

99 As regards Facebook, LinkedIn, LiveJournal, MySpace, Hi5 and Skyrock (skyblogs), *see* OPCC, 2009, p. 43.

100 In this respect, "the policies are often vague about actual practices, and contain statements that are contradictory or misleading" (UCBSI, 2010, p. 33, *see also* pp. 11-12).

101 *See* FTC Policy Statement on Unfairness, December 17, 1980, and FTC Policy Statement on Deception, October, 14, 1983.

102 For an overview of documents published by the FTC, *see* Gindin, 2009, pp. 1-36.

103 *See* as regards English law, Walden, 2007, pp. 462-463.

104 Contractual limitations would satisfy those who protest against rules about data protection due to free speech protection considerations, *see* Volokh, 2000, pp. 7-11.

105 Once information is produced, it is in a context linked with "informational norms", i.e.: "norms of appropriateness" and "norms of flow or distribution." If later these rules are not respected by the individuals involved by the production of the information at stake, there is a violation of privacy, regardless of this violation is or not justified (and then, lawful). For instance, in the friendship context – word for word targeted on Facebook (where you have "friends"), but in practical terms distorted –, H. Nissenbaum (2004) explains that the norms of appropriateness are loose – we tell ourselves a lot –, while norms of flow are much more strict – zip it, lock it, put it in your pocket. For an ap-

plication of this theory in the SNS context, *see*Dumortier (2009).

106 "Privacy is built around a few key ideas: You should have control over what you share. It should be easy to find and connect with friends. Your privacy settings should be simple and easy to understand" (http://www.facebook.com/privacy/explanation.php?ref=pf, last visited on February 13, 2010).

107 *See* Moiny, 2010, pp. 247-250; Wong, 2008; Working Party 29, WP163, pp. 5-7; Working Party 29, WP169, pp. 21 and 23.

108 *See* Moiny, 2010/1. In this paper, we discussed the contract formation in the context of SNS as regards American and Belgian laws.

109 In the United States, choice of law clauses generally electing California law, *see notably*, as regards SecondLife, True.com and MySpace where a contract has already been considered concluded: Bragg v. Linden Research (2007); Cohn v. Truebeginnings (2007); as an obiter dictum, in a footnote, USA v. Lori Drew (2009).

110 Even if consent is not always necessary to the lawfulness of a processing operation (*see notably* Article 7, f) Directive 95/46), the SNS provider generally relies on such a basis (which is normal as regards Safe Harbor Principles). In this respect, consent is supposed to be expressed at the moment of the subscription (the user agreeing to the terms of use and privacy policy) and later by defining privacy settings and spontaneously communicating data.

111 In some extent, it has to be noted that Facebook was originally not so far from this doomsday scenario. Users could not permanently delete their accounts and the privacy policy was (and is still to some extent) unclear about the purposes of the processing operations Facebook could realize. Moreover, a terms of use modification seemed – but has been challenged by users and finally avoided – to give Facebook extensive rights as regards the conservation of users' data, *see*http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html, last visited on March 15, 2010.

112 P. Polański (2007, pp. 305-306 and 323) aims at "signal[ing] the emergence of potential customary norms in global Internet-based commerce" and identifies "the most important Internet common practices." He cites as an "Internet-specific custom", the "Right to explore user's behaviour", and underlines that "[i]t is also a global practice of website operators to employ cookies or web beacons for the purpose of tracking user behaviour or storing important personal data to personalise a website. The whole online advertising industry relies on the legal permissibility of this practice."

113 *See also* nos. 130 and ff.

114 In Belgium, *see for instance* a judgment of the Tribunal du commerce of Liège, Real de Madrid et al. v. Hilton Group Plc. et al. (2006).

115 Our societies admit the validity of the exploitation of the "goods of the personality" ("*biens de la personnalité*") (Léonard, 2001, p. 437 and the references cited in footnote no.55).

116 *See generally* about this topic Moine, 1997, pp. 352-366; Kang & Buchner, 2004, pp. 230 and ff; Samuelson, 2000, pp. 1125 and ff; Schwartz, 2004, pp. 2056 and ff.

117 Such as the selling of personal data to the American government, *see* Simmons, 2009, pp. 984-999.

118 *See supra* as regards privacy and data protection.

119 *See notably* as regards nullity due to violation of the public order, the decision of the Belgian Cour de cassation no. C980042F (1999). *See also* Rigaux, 1980, p. 473.

120 *See also* Article 8.1 of directive 95/46/EC.

121 As regards the servers of the cloud computing service provider: "The location of these servers can be spread all over the world, with the data changing and moving continuously between the provider's servers" (Joint, Baker, & Eccles, 2009, p. 271).

122 Facebook's privacy policy explicitly reveals that information is used for advertising purpose: "4. How We Use Your Information... To serve personalized advertising to you."

123 "[O]ne of the practical implications of cloud-sourcing is that its cost-efficiencies are driven by a freedom a provider has to move the data/application/operating system to the most efficient location for them" (Joint, Baker, & Eccles, 2009, p. 272).

124 Without prejudice to a latter real-time information.

125 And for instance, as regards Facebook, LinkedIn, MySpace, Twitter and SecondLife, these documents are not displayed, they are only accessible through hyperlinks.

126 It is here referred to about how consumers conclude (e-)contracts. " 'Blanket assent' is best understood to mean that, although consumers do not read standard terms, so long as their formal presentation and substance are reasonable, consumers comprehend the existence of the terms and agree to be bound to them." " 'Blanket assent' means only that, given the realities of mass-market contracting, the consumer chooses to enter a transaction that includes a package of reasonable, albeit mostly unfavorable to her, boilerplate terms" (Hillman & Rachlinski, 2001, pp. 33-34).

127 Following Working Party 29 (WP115, 2005, p. 5), as regards the use of location data with a view to providing value-added services, the definition of consent "explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered." *See* Le Métayer & Monteleone, 2009, pp. 137-138.

128 The F.T.C. compelled Sears to inform its users "[c]learly and prominently, and *prior to* the display of, *and on a separate screen from*, any final "end user license agreement," "privacy policy," "terms of use" page, or similar document" (In the Matter of Sears, 2009, p. 3). Concerning this particular case and what could be learned from it, *see* Gindin, 2009.

129 "LiveJournal offers six different types of accounts, with the extent of advertising, size of account, and access to services defined by the type of account selected" (OPCC, 2009, p. 25).

130 EPIC, in its recent complaint against Facebook (EPIC v. Facebook 3, 2010, no. 121) underlined that "Facebook Has a History of Changing Its Service in Ways that Harm Users' Privacy", and enumerated the different substantial revisions of the website's terms of use and privacy policy that occurred in spite of users protestations (nos. 121-132).

131 *See* footnote no. 130.

132 If the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

133 Facebook and LinkedIn also bear the TrustE label. Originally, MySpace did the same but doesn't bear this label anymore.

134 *See* Article 8, b) and c) ETS 108 and Article 8.2 Charter of Fundamental Rights of the European Union.

135 But a user who is a legal or natural person that has to comply with Directive 95/46/EC, and therefore do not fall (if natural person) within the domestic use exemption of Article 3.2, second dash Directive 95/46/EC.

[136] It could be argued that a user having a non-publicly accessible profile, only accessible to a definite number of contacts he accepted, fall outside the scope of Directive 95/46/EC. *See* as regards this question Working Party 29, WP163, 2010, pp. 5-7; Moiny, 2010, pp. 250-254. In this case, the data subject would suffer a lack of protection (e.g. how would he be protected against transborder data flows to countries lacking an adequate data protection law, how the security of the processing operations would be ensured, etc.). Another question is to know if he needs a specific protection in this case. We think so in the elusive context of cloud computing. The following questions arise if we wonder about an evolution of data protection rules. If a very strict interpretation of the domestic use exemption is adopted, it could be opportune to impose to a natural person data controller and using SNS or cloud computing services for a personal purpose, a "diet" data protection regime. In our view, the solution to intrusive data protection rules for an individual socializing over the Internet, lays in a lighter data protection regime, and not in an exclusion of the scope of the regulation.

[137] *See infra.*

[138] Legal persons could use SNS to promote their business (with a Page on Facebook or an account on LinkedIn that has a clearly professional purpose), and it leads to the question of a potential extension of data protection rules to such legal persons – but, if desirable, which ones (S.M.Es?) and when?

[139] College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer (2009), nos. 57-59.

[140] The limits Member States would fix have to result from

a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to rectification, erasure and blocking of the data in the event that the processing of the data does not comply with the Directive, and rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller. (College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer (2009), no.64)

[141] Compare with Article 13, §2 Directive 95/46/EC.

[142] *See supra.*

[143] More generally, the study underlined that "[o]ur review of the policies showed that only 23 of the top 50 affirmatively stated that users could have access to some portion of the information the website had collected about them. The remaining 27 policies lacked mention of access or their statements about access were unclear. However, none of the policies specified that a user could access *all* the data that had been gathered" (UCBSI, 2009, p. 30). The first recommendation of KnowPrivacy relates to the right of access, (UCBSI, 2009, p. 32).

[144] Some technical storage remains permitted (Article 5.1, *in fine,* of Directive 2002/58/EC), so does the "legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication" (Article 5.2 of Directive 2002/58/EC). Moreover, Member States can adopt some exceptions according to Article 15. Finally, Directive 2006/24/EC mustn't be forgotten.

[145] See Working Party 29, WP148, p. 14.

[146] Concerning this topic, *see* Working Party 29, WP37, 2000, pp. 22-23; Working Party 29, WP148, 2008, pp. 12-13; Rosier, 2008, p. 339.

[147] *See* Dhont & Rosier, 2003, pp. 10-12 and pp. 15-16; Rosier, 2008, pp. 327-354 and

pp. 339 and 341; Louveaux & Pérez Asinari, 2008, p. 323.

148 Public communications network "means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points", Article 2, d) of Directive 2002/21/EC. *See* the Belgian transposition of this disposition, Article 2, 3° *Loi relative aux communications électroniques* [LEC]. About this law, *see* Van Overstraeten, Bruyndonckx, Szafran, & Rousseau, 2005, pp. 203-208.

149 The use of an SNS from a mobile phone through the GSM network (not via Airport) is not taken into consideration. This case does not change the reasoning related to the SNS provider.

150 Electronic communications service "means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks" (Article 2, § 1 of Directive 2002/58 and Article 2, c) of Directive 2002/21). *See also* Article 2, 5° of LEC

151 "There is no doubt that connecting Internet users to an *ISP*, providing Internet services to Internet users and routing requests and replies from Internet users to website servers and back are telecommunications services. So, Directive 97/66/EC applies to telecommunications providers, *Internet Service Providers* and providers of *routers* and lines for Internet traffic", (Working Party 29, WP37, 2001, p. 23).

152 "The *Internet Service Provider (ISP)* provides services to individuals and companies on the Web. It owns or hires a permanent TCP/IP connection and uses servers permanently connected to the Internet. Classically, it will offer web hosting (web pages stored on its web server), access to newsgroups, access to an FTP server and electronic mail. This involves one or more servers using the HTTP, NNTP, FTP, SMTP and POP3 *protocols*" (Working Party 29, WP37, 2001, p. 12).

153 For instance, each Facebook profile, group and page are provided in a uniform presentation. While MySpace users can modify the presentation of their pages.

154 Which "means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed" (Article 2, (a) of Directive 2002/21).

155 Which has been underlined by the Economic and Social Committee which "particularly welcomed the commitment to base the proposed regulatory evolution on: *technology neutrality, including no Internet-specific measures. Technologically neutral regulation should not, however, lead to stronger regulation of new services, but rather to the roll back of existing specific regulation of*

traditional services", (Economic and Social Committee, 2000).

156 *See* footnote no. 154.

157 As an example, Facebook rents data centers and plan to have its own one, *see* http://gigaom.com/2010/01/21/facebook-matures-will-build-its-own-data-center/, last consulted on 3 June 2010.

158 This question would depend on the material facilities of the SNS provider at stake.

159 A web hosting service provider could to the contrary be an ECS because its main activity would consist in the conveyance of signals. Its task is to answer and send the right pages requested by users, not to provide any specific content of his own.

160 As regards webmails, applications like Microsoft Outlook, Mozilla Thunderbird or Apple Mail enable the user to retrieve his emails from the server and download them on its own computer. As regards SNSes, an application should be imagined to retrieve photos, videos, etc. from the website's database.

161 Indeed, Directive 2006/24/EC applies to "the obligations of the providers of *publicly available electronic communications services* or of *public communications networks* with respect to the retention of certain data which are generated or processed by them" (emphasis added by author), Article 1.1. Coming back to the example of the webmail, in our view, a webmail provider does not provides any ECS and therefore does not have to retain any data, even if the Directive 2006/24/EC targets Internet e-mail (Article 5.1 (a)(2°), (b)(2°), (c)(2°), (d)(2°) and (e)(3)). In this respect, the Directive imposes that data are retained "to the extent that those data are generated or processed *by providers of publicly available electronic communications services or of a public communications network* [...] *in the process of supplying the communication services concerned*" (Article 3.1). That is to say that, for instance, data must be retained as regards Internet e-mail provided by IAPes, because data related to the Internet e-mail are then processed by providers of ECS (Internet access) in the process of supplying this Internet access. In practical terms, the Internet e-mail is provided with the Internet access, both services being linked and provided at once. But as regards webmail providers, hearing that these latter do not provide ECS such as Internet access, no Internet e-mail data has to be retained under Directive 2006/24/EC. If the webmail provider offers an ECS such as hosting websites, the provision of Internet e-mail is another service and data generated in providing this latter do not appear to be generated in the process of supplying hosting. It could be deemed otherwise if specific e-mail accounts were provided to the ones who would subscribe to the hosting service.

162 The reasoning of the Austrian Regulatory Authority for Broadcasting and Telecommunications ([ARABT], 2005, p. 5) as regards voice over IPis the following:

The key Internet service enabling the global transport of data packets is Internet Connectivity. Internet Connectivity, as provided by Internet Backbone Providers (on wholesale level) and ISPs, (on retail level) undoubtedly is a classic ECS. On top of this basic ECS "Internet Connectivity" within the "Internet Access" product of ISPs numerous intelligent Internet services and applications are provided by third party providers, e.g. based on corresponding application servers. Both third party service provider and the end customer have to be connected to the Internet and be able to use the Internet Connectivity without restrictions. For classification of such an intelligent service (e.g. a server based VoIP service) as ECS or non-ECS it has to be investigated if the service offered to the end customer by a specific third party

service provider wholly or mainly comprises the ECS Internet Connectivity or not. In typical Internet-only VoIP applications (i.e. without access to the PSTN) the VoIP provider in essence provides to his subscriber the called party's IP-address only and has no function or responsibility with regard to the transport of the IP voice packets between VoIP users. Therefore it would not be reasonable if a VoIP subscriber complains to his VoIP provider in case of poor voice quality, as the transmission of IP voice packets (i.e. the ECS part of the combination of the two generally totally independent products used by the VoIP subscriber) is not part of the VoIP service. Transmission of voice packets is the technically and contractually independent service of the VoIP user's ISP on request of the user's terminal software. If therefore the transmission of IP voice packets between the calling party and the called party is not part of the VoIP service (no corresponding cost elements within the VoIP service price, no (re)selling of Internet Connectivity) it has to be recognized, that such a VoIP service does not mainly consist in the conveyance of electronic signals (i.e. IP voice packets in this case) which would be the necessary prerequisite for a classification as ECS according to the European framework and the TKG 2003.

However, again as regards voice over IP and more precisely, as regards voice over IP services where "E.164" telephone numbers are not provided and from which there is no access to or from the Public Switched Telephone Network, the European Regulators Group ([ERG], 2007, p. 4) noticed that this "case [...] includes different implementations: from pure peer-to-peer, based simply on a VoIP software which uses users' computers as nodes of the connection to more centralized architectures based on call management servers, data bases and routers provided by the VoIP operator." It then underlined in footnote that "different regulatory approaches are adopted by the Member States due to an uncertainty on the regulatory treatment of such services: it is not clear whether this case should be considered an electronic communication service." In this respect, it could be argued that if the SNS provider operates an CN, it provides such a "more centralized architecture", which could plead in the sense that it provides an ECS and a PCN

163 According to these recitals: "This Directive seeks to respect the fundamental rights and observes the principles recognized in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter", and "Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States."

164 Even if users not *only* use an ECS.

165 As regards instant messaging (chat), for instance, data could be however directly transmitted between users, without going through the SNS servers.

166 This second storage stage does not occur as regards chat, when communications are delivered immediately and in real time.

167 Some data are however *intended to* the SNS provider. That is for instance the case as regards pieces of information users have to give to the SNS provider when subscribing to the network (name, age, gender, etc.).

168 *See infra* as regards hacking.

169 Chatroulette (http://chatroulette.com/) is not really a social network, in the extent that users do not have profiles. It is what we would call a "video chat" website randomly

linking people through webcam, microphone and traditional chat. *See* http://www.spiegel.de/international/0,1518,681681,00.html, http://bits.blogs.nytimes.com/2010/02/13/chatroulettes-founder-17-introduces-himself/, last visited on March 20, 2010. Even if, generally, the user doesn't know with who he is going to be connected (this individual is indeterminate), the communication nonetheless happens between a finite number of parties, that is to say, two parties. At least, two computers are involved even if more individuals are behind the webcams. And these communications seem always in the first transmission stage identified above.

170 The "the Working Party thinks that surfing through different sites should be seen as a form of communication and as such should be covered by the scope of application of Article 5" of the old Directive 97/66 (Working Party 29, WP37, 2001, p. 50).

171 *See infra* where such communications would be considered to be intended to an "indeterminate" or "irrelevant" audience with fluctuating accessibility.

172 *E.g.* if a user or a group accept no matter who as a friend or member and, in fact, has really a lot of friends or members (e.g. 500 people).

173 As regards Facebook-like SNS for instance, lots of contexts intertwine through the profile of a user. *See* Moiny, 2010, p. 252.

174 If communications were deemed protected, another solution to safeguard the freedom of expression would be for Member States to provide for a "one-party consent rule" (*see infra*) as regards the second stage of transmission. The consent of one party to the communication would then be enough for the divulgation of the communications.

175 The knowingly use of an information obtained in such a way is also punished. *See* Article 314bis, §1, 1°, and §2 Belgium PC, *see also* Article 259 bis PC.

176 *See* Article 145, §1 LEC

177 Communications are private when they are not intended to "every man jack" ("*tout un chacun*"), *See* (Proposition of Data Privacy Act, Belgium, 1992, p. 7).

178 *See notably* Vandermeersch, 1997, pp. 247-255, discussing the condition of "during transmission" in the context of Internet.

179 R. de Corte (2000, p. 12), writing about the former Telecom Law, underlines that both Articles protect different kinds of information: one protects the content of the communication (Penal Code) and the other "telecommunication data" (Telecom Law). However, since the implementation of Directive 2002/58/EC, content is now protected under the LEC, according to the wording of its Article 125. Anyway, it could also be argued that to know the content of a communication implies to know its existence. Both disposition could and still can apply at the same time.

180 The interpretation of the transmission stage can be refined. From the Criminal point of view, as regards the requiring of "during transmission"(in the context of Article 90 ter of the Belgian Criminal Procedure Code), some scholars propose to presume that the transmission occurs between the sender and the "*a priori* expected terminus of the transmission" ("*geïndiceerd noodzakelijk eindstation*", the authors considering that "*geïndiceerd*" means what can reasonably be expected *a priori*). In this sense, on the one hand, they consider that the "terminus" of the transmission is the personal computer of a user when "popmail" (normally provided by the Internet Access Provider) are used (i.e. when the mails are retrieved through a software such as Safari or Thunderbird). Even if the IAP gives the possibility to use the "popmail" as a "webmail" through a

website. And on the other hand, the transmission ends as regards webmails, when the mails are in the "webmailbox." Even if the webmail can be used as a "popmail" (Van Linthout & Kerkhofs, 2008, pp. 86-88).

[181] *See* Article 2 Directive 2002/58.

[182] Of course, as it has been shown, the SNS provider can acquaint himself of each protected communication occurring through the SNS but strictly for the sole technical purpose of their transmission (including their backup).

[183] *See also* Killingsworth, 1999, pp. 75-76.

[184] However, the Act specifies that this concept does not include: "(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds."

[185] As regards the Wiretap Act, *see notably* Garrie, Armstrong, & Harris, 2005, pp. 115-117.

[186] The Court notably quotes Konop v. Hawaiian Airlines (2002).

[187] According to 18 USC § 2510 (15), ""electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications."

[188] According to 18 USC § 2711 (2), the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system."

[189] For example, the text of a message and the subject line, *see* § 2510 (8); Kerr, 2004, p. 24.

[190] "For example, a company can disclose records about how its customers used its services to a marketing company" (Kerr, 2004, p. 15).

[191] 18 USC § 2702 (a) (1) and (2) target services provided "to the public." The service will be public if the provider offers it to "the public at large", "for a fee or without cost", where "anyone can sign up and pay for an account", etc. The service is not public if it involves a special relationship between the provider and the user (e.g. a university and its students, an employer an his employees) (Kerr, 2004, pp. 22-23).

[192] Following 18 USC § 2510 (17), ""electronic storage" means— (A) any *temporary, intermediate storage* of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of *backup protection* of such communication" (emphasis added by author).

[193] For a summary of the difference, *see notably* Scolnik, 2009, pp. 376-377.

[194] *See also* USA v. Steiger, 2003.

[195] *See also* Kaufman v. Nest Seekers, 2006: only "electronic bulletin boards which are note readily accessible to the public are protected under the Act."

[196] According to 18 USC § 2702 (b) (3), "a provider described in subsection (a) may divulge the contents of a communication", "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." According to § 2701 (c) (2), § 2701 (a) does not apply if the access to the communication stored in a facility through which an ECS is provided is authorized "by a user of that service with respect to a communication of or intended for that user."

[197] 18 USC § 2511 (2) (d): "it shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communica-

tion or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."

198 *See in the same sense* Pharmatrak Privacy Litigation (2002), reversed by the First Circuit (Pharmatrak, Privacy Litigation, 2003), deeming that the clients of Pharmatrak did not consent to the collection of personal data; Chance v. Avenue (2001).

199 The Court considered that ""Internet Access" is the relevant electronic communications service", provided by the Internet Service provider, and that "Web Sites are "users" under the ECPA" (DoubleClick Privacy Litigation, 2001).

200 It has to be noted that other class action suits had been filed against DoubleClick for privacy violations and led to a settlement, *see* Mercado Kierkegaard, 2005, p. 315.

201 As regards the decision, *see* De Hert, de Vries, & Gutwirth, 2009, pp. 87-92.

202 In the context of SNSes, data can (and is) even be stored elsewhere, in data centers due to the use of cloud computing technologies.

203 Including the United States having signed and ratified this Convention.

204 *See also* Council Framework Decision 2005/222/JHA.

205 *See* concerning this rule, Keustermans & Mols, 2001-2002, pp. 725-728; De Villenfagne & Dusollier, 2001, pp. 69-71.

206 Article 2 of the Budapest Convention provides that "A Party may require that the offence be committed by infringing security measures." The Belgian legislator has not required this condition deeming that this would cause "complications" such as the need to identify the level of protection required and to reveal the protection systems for evidence considerations. It also considered that protection systems are standardized. The purpose will show that the absence of this condition causes interpretation difficulties to identify when access is authorized.

207 Except maybe if he is a student in computer science realizing an exercise in a teaching framework, and non-intentionally going further than what is required by his professor...

208 Hacking is also punished under States Law. For instance in California, and without going into the details of the California Penal Code, shall be punished who "[k]nowingly and without permission uses or causes to be used computer services" (California Penal Code § 502, (c), (3)), that is to say, notably, "computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network" (Californian Penal Code § 502, (a), (4)).

209 18 USC, § 1030.

210 "In a nutshell, "protected computer" covers computers used in interstate or foreign commerce (e.g., the Internet) and computers of the federal government and financial institutions" (Computer Crime and Intellectual Property Section, Criminal Division [CCIPS], 2007, p. 3).

211 Plaintiffs had to demonstrate that the harm they suffered corresponds to one of the categories included in the 18 USC, § 1030, (g) and (c) (4), (A), i), I to VI. In Doubleclick Privacy Litigation (2001), it was about demonstrating a "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value."

212 *See* Moiny, 2010/1, pp. 6-96.

213 "Defendants have admitted to maintaining an AOL membership and using that member-

ship to harvest the e-mail addresses of AOL members. Defendants have stated that they acquired these e-mail addresses by using extractor software programs. Defendants' actions violated AOL's Terms of Service, and as such was unauthorized" (AOL v. LCGM, 1998).

214 More exactly, it would be about exceeding access rights, in place of accessing without authorization, *see* in the same sense LVRC Holdings v. Christopher Brekka (2009).

215 This doctrine is made up of two tests: "fair notice" and "discriminatory enforcement." "The fair notice test asks whether the law is so vague and standardless that it leaves the public uncertain as to the conduct it prohibits." "If a law is so vague that a person cannot tell what is prohibited, it leaves judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case." The second test is focused on "how much discretion the law gives the police" (Kerr, 2010, p. 14).

216 As regards scholars and, for instance, the case of employers using SNSes to investigate jobs applicants, *see* Byrnside, 2008, p. 468.

217 Judge Wu also underlines that the SNS provider would not necessarily forbid the access to the website in the case of breach of the terms of use. Therefore, such a breach would not necessarily lead to an access without authorization.

218 The hypothesis is not insane. For instance, Article 5.2 of Gmail's terms of service (last visited on April 5, 2010) specifies that: "You agree to use the Services only for *purposes* that are permitted by (a) the Terms and (b) *any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions* (including any laws regarding the export of data or software to and from the United States or other relevant countries)" (emphasis added by author).

219 The Belgacom (a Belgian IAP) Acceptable Use Policy, as regards Internet services (including Internet access), prohibits, in its Article 2.1, "to use the Service for any purposes other than those which are legal", *see* http://www.belgacom.be/private/gallery/content/documents/conditions/aup_v1_fr.pdf, last visited on April 5, 2010.

220 *See* as regards this topic Kuty, 2009, pp. 70 and ff.

221 After having flirted under the avatar of a young boy, the defendant told the deceived young girl that the boy "no longer liked her", and that "the world would be a better place without her in it."

222 As regards Belgian law, the developer would act "fraudulently", pursuing an unlawful benefit resulting from an unlawful processing operation.

223 Hearing that we did not study the sentences, which is not relevant for the purpose.

224 Implemented in Belgium in the Article 129 of the LEC

225 *See also* Article 129, al. 1, 1° and 2° LEC

226 *See* Mercado Kierkegaard, 2005, p. 320, *see* pp. 315-316 as regards the concepts of opt-in and opt-out. Concerning these latter, *see also* Dreier, 2010, pp. 144 and ff.

227 *See supra.*

228 About the pressure from industry lobbyists as regards the adoption of the old version of Directive 2002/58/EC and cookies, *see* Kierkegaard, 2005, pp. 318-321.

229 It considered that: "Browsers or other applications which default reject 3rd party cookies and which require the data subject to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites may be able to deliver valid and effective consent" (WP171, 2010, p. 14).

230 *See supra.*

231 *See* Recital 24 of Directive 2002/58/EC as regards the concerned devices.

232 E.g. SecondLife, LinkedIn, Facebook, Twitter and YouTube (worldwide).

233 *See* Strahilevitz, 2004, p. 18.

234 *See* Moiny & De Groote, pp. 5 and ff. *See notably* Articles 15 to 17 of Regulation 44/2001/EC and Article 6 of Regulation 593/2008/EC.

235 *See* Article 12.2 of Directive 97/7/EC.

236 As regards cloud computing, the localization of equipments needed to the processing of personal data could be automatically assigned owing to the technical effectiveness of the offered service.

237 If the data controller is established in another Member State, this Member State has to apply its data protection rules. The Directive then does not precise what the Member State of the place of establishment has to do, given that the applicability of its data protection rules can not restrict the free flow of personal data. The applicable law to data protection will depend on the national implementation of Article 4 of directive 95/46/EC. *E.g. see* Article 3bis of the Belgian Data Protection Act (1992). For a brief discussion about conflicts of law and directive 95/46, especially in the context of SNSes, *see* Moiny, 2010. *See also* for more details Workin Party 29, WP179, 2010, and Kuner, 2010.

238 For the record, Regulation 864/2007/EC on the law applicable to non-contractual obligations does not apply to "non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation" (Article 1.2, g)). Therefore, it has to be referred to national conflicts of laws rules.

239 It still remains necessary to further identify in which cases the application of the foreign rule contrary to the ECHR is justified by the "foreignness" ("*extranéité*") of the situation, Mayer, 1991, p. 664; P. Hammje (1997, pp. 14-18) suggests a "public order exception" with the development of public order specific to the defense of fundamental rights. *See also* Labrusse, 1997.

240 Admittedly, this Article only applies if the consumer has its "habitual residence" in the concerned Member State. While the concept of "domicile", relevant as regards "Brussels I" Regulation, is something else. For the needs of the purpose, we consider that the consumer at stake has its domicile – which has to be determined according to the law of the State where the domicile is claimed to be – in the State where he has his habitual residence.

241 *See* Moiny, 2010. The only geographical exclusion is the following: "[i]f you are located in a country embargoed by the United States, or... you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website."

242 *See* footnote no. 169.

243 "Member States shall take the necessary measures to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-Member country as the law applicable to the contract if the latter has a close connection with the territory of the Member States", Article 6.2 of Directive.

244 *See*, Kuty, 2009, pp. 382 and ff.

245 It is not discussed here if Directives 95/46/EC and 2002/58/EC have the same territorial scope due to their connections. If it were the case, Belgian law having to be interpreted in accordance whit European law, the LEC, as far as it implements Directive 2002/58/EC, would have had to be territorially limited according to Articles 4 and 1 of Directive 95/46/EC.

246 Article 5.4 "Brussels 1" Regulation.

247 As regards this doctrine and the extraterritoriality of competition law, *See* Jones & Surfin, 2008, pp. 1356-1387.

248 An SNS provider directing its activities to the worldwide market does not necessarily has offices in Europe. For instance, does Twitter has any office in Europe? Anyway, lots of European citizens subscribed to Twitter.

249 *See* Moiny, 2010; WP148, 2010.

250 The Working Party 29 recently noted that "there are situations which fall outside the scope of application of the directive. This is the case where non-EU established controllers direct their activities to EU residents which result in the collection and further processing of personal data" ... "If they do so without using equipment in the EU, then Directive 95/46/EC does not apply" (WP168, 2009, no. 27).

251 As regards the Convention no. 108 of the Council of Europe, the processing of personal data for criminal purposes is involved in the adequacy assessment, while it is not as regards Directive 95/46/EC. Could it be tempered through conflicts of law rules? Or, according to Article 8 ECHR, *does it have to be* tempered in such a manner, or by a public order exception, etc.?

252 *See* footnotes nos. 121 and 123. For instance, an American Company, having processing facilities on the European territory, could use these facilities, due to technical effectiveness considerations, to process personal information related to American data subjects. It is tenable to consider that, as regards opportunity, European data protection law should not apply in such a case. But the place of these equipments could be a clue of the will of a company to direct its activities toward a specific market or toward the worldwide market. For instance, the creator of Chatroulette – a seventeen years old boy (does he know anything about data protection?) –, with the expansion of use of its website, seems now to use servers in Germany, *see* http://bits.blogs.nytimes.com/2010/02/13/chatroulettes-founder-17-introduces-himself/, last visited on March 15, 2010.

253 In the same sense and for suggestions, *see* Korff & Brown, 2010, pp. 24-26.

254 *See* for instance the Madrid Resolution (2009).