Agentschap voor Innovatie door Wetenschap en Technologie
IWT
SBO Security and Privacy for Online Social Networks

Document type	Report
Title	Rights and obligations of actors in social networking sites
Deliverable Number	D6.2
Authors	Brendan Van Alsenoy
Dissemination level	Internal
Preparation date	2 December 2014
Version	1.2

SPION

Contributors

	Name	Organisation
1	Brendan Van Alsenoy	ICRI, KU Leuven, iMinds
2	Willem De Groef	Distrinet, KU Leuven, iMinds
3	Alessandro Acquisti	CMU
4	Ero Balsa	COSIC, KU Leuven, iMinds
5	Bettina Berendt	DTAI, KU Leuven
6	Rula Sayaf	Distrinet, KU Leuven, iMinds
7	Rob Heyman	SMIT, VUB, iMinds
8	Seda Gürses	COSIC, KU Leuven, iMinds

Table of Contents

1. Introduction

One of the most significant developments in the online environment over the last few years has been the rise of social media.[1] More and more individuals are making use of Online Social Networks (OSNs) to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas. But users are not the only ones who are interested in OSNs. OSNs have come to attract a wide range of actors, which include application developers, web trackers, third-party websites, data brokers and other observers.

As the number of actors engaging with OSNs and OSN data increases, so does the risk for potential privacy infringements. One way to minimize this risk is to clearly define the rights and obligations of each actor. The objective of this deliverable is to analyze how the current data protection framework relates to the context of OSNs. To this end, we will begin by describing the various actors engaging with OSNs and the interactions between them. Next, we will identify the legal status of each of the actors in order to map their rights and obligations. This deliverable serves as a building block for a number of forthcoming SPION deliverables, namely (a) Liability and accountability of actors involved in online social networking services (SPION D6.3); (b) Evaluation of the applicable legal framework (SPION D9.6.3) and (c) Policy recommendations for privacy-friendly social networks (D9.6.6).

[1] O. Tene, 'Privacy: the new generations', *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 22.

2. "Who's who?" Mapping the relevant actors

The purpose of this section is to identify the main actors engaging with OSNs. Our inventory is based on a literature study of news articles, academic publications and regulatory guidance concerning security and privacy in OSNs. A common denominator among the selected entities is that they each process personal data resulting from (a) the usage of OSNs and/or the usage of other services which somehow interact with the OSN.

The following figure provides a -highly simplified- representation of the main actors engaging with OSNs and OSN-related data. It is intended to be conceptual rather than factual.

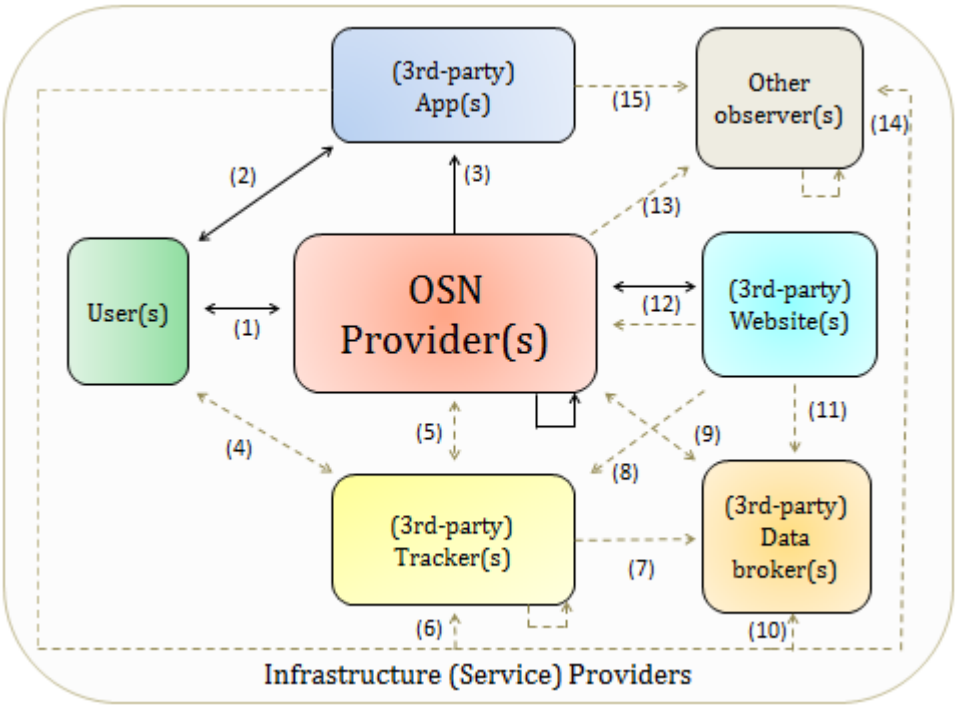

Figure 1 – Relevant OSN Actors

The arrows in Figure 1 indicate that an exchange of personal data is taking place. This exchange can be either uni- or bi-directional. Solid black arrows signify exchanges of personal data which occur primarily 'in the foreground', meaning that they can easily be observed or inferred by users. They typically imply some form of active involvement by users (e.g., granting a permission, manually entering data, use of an application).

Dashed grey arrows were used to signify data exchanges which are likely to be less obvious to OSN Users. Some of these exchanges may be detectable (e.g., by monitoring the activities of one's internet browser) or otherwise ascertainable (e.g., by reading the privacy

notice of an OSN provider).[2] Others may occur completely unnoticed. Over the following sections, we will briefly describe each of the actors and interactions displayed in Figure 1.

Note that the categories of actors identified in Figure 1 are not mutually exclusive. A given actor may combine multiple roles depending on the circumstances (e.g., an OSN provider might also deploy its own tracking mechanisms, or an application provider might also be the operator of a third-party website).

2.1 OSN user

People join OSNs for a variety of reasons. Most people do so to stay in touch with friends and family, to connect around shared interests or hobbies, or to make new friends.[3] Increasingly, however, OSNs are also used by companies and other organizations to advance commercial, political or humanitarian goals.[4]

The creation of an OSN account (or 'profile') involves disclosure of a number of attributes, which typically include name, date of birth and place of residence. Most OSNs also encourage its users to upload a picture of themselves.[5] Depending on the nature of the OSN, users might be encouraged to reveal additional information such as relationship status and interests (e.g., Facebook) or current employment (e.g., LinkedIn).

Once a user has signed up, he or she is essentially free to share any information they see fit. This information can range from mundane facts (e.g., "I'm at the mall"), to political views (e.g., "vote 'no' on prop 11"), to highly intimate personal details (e.g., "I'm dating Alice but I think I'm in love with Bob"). Even though the policies of an OSN may impose certain restrictions, OSN users are also in a position to disclose information about others.

It is worth noting that a significant amount of personal data disclosed via OSNs is *relational*. Social connections among OSN users can be used to create a 'social graph', whereby nodes represent users and connections or edges represent the relationships

[2] Even if users are notified of their existence at a certain point in time, they may not be consciously aware of them at a later stage, as these exchanges typically occur 'in the background' or do not require active User involvement.

[3] A. Smith, 'Why Americans use social media', *Pew Internet & American Life project*, 15 November 2011, available at http://pewinternet.org/Reports/2011/Why-Americans-Use-Social-Media.aspx (last accessed 17 December 2013).

[4] See e.g. J. Heidemann, M. Klier and F. Probst, 'Online social networks: A survey of a global phenomenon', *Computer Networks* 2012, vol. 56, p. 3871-3872 (discussing potential usage by businesses); R.D. Waters, E. Burnett, A. Lamm and J. Lucas, 'Engaging stakeholders through social networking: How nonprofit organizations are using Facebook', *Public Relations Review* 2009, Vol. 35, Issue 2, p. 102–106. See also Article 29 Working Party, 'Opinion 5/2009 on online social networking', WP163, p. 7, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (last accessed 17 December 2013).

[5] d.m. boyd and N.B. Ellison, 'Social Networking Sites: Definition, History and Scholarship', *Journal of Computer-Mediated Communication* 2008, vol. 13, p. 211-212.

between these users.[6] In addition, many OSN features have been designed to expose additional relational information (e.g., by promoting group formation).

At the end of the day, OSN users disclose considerable amounts of information about themselves. They also access significant amounts of information related to others. This flow of personal data is depicted in Figure 1 as bi-directional arrow (1).

2.2 OSN Provider

The central actor in Figure 1 is the OSN Provider. An OSN provider is an entity that operates the hard- and software necessary to deliver an OSN service.[7] According to boyd and Ellison, the key features of social network sites are that they allow individuals to

> '*(1)construct a public or semi-public profile within a bounded system,*
> *(2) articulate a list of other users with whom they share a connection, and*
> *(3) view and traverse their list of connections and those made by others within the system.'*[8]

While the display of profiles showing a list of connections may be considered the 'backbone'[9] of an OSN, many platforms offer an array of additional features and services. OSNs typically provide common messaging services (e.g., chat, email), as well as message board and commenting functions.[10] Other features encourage users to import information from outside the OSN domain, e.g. through 'share' or 'like' functions (see also *infra*; section 2.6).

OSN providers also operate the hard- and software which enables them to generate revenue from their service. For most OSN providers, the primary source of revenue is

---

[6] R. Sayaf and D. Clarke, 'Access control models for online social networks', in *Social Network Engineering for Secure Web Data and Services*, IGI, 2013, p. 2.; G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), 'Online Social Networks: Status and Trends', *New Directions in Web Data Management*, Studies in Computational Intelligence, Vol. 331, 2011, p. 215.

[7] A reference architecture of OSNs can be found in G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), 'Online Social Networks: Status and Trends', *New Directions in Web Data Management*, Studies in Computational Intelligence, Vol. 331, 2011, at p. 217.

[8] d.m. boyd and N.B. Ellison, 'Social Networking Sites: Definition, History and Scholarship', *l.c.*, p. 211. This definition has been criticized by Beer as being too broad: see D. Beer, 'Social network(ing) sites … revisiting the story so far: A response to danah boyd & Nicole Ellison', *Journal of Computer-Mediated Communication* 2008, Vol. 13, p. 516 et seq. See also J. Heidemann, M. Klier and F. Probst, 'Online social networks: A survey of a global phenomenon', *l.c.*, p. 3867. Like Heidemann, we use the term Online Social Networks to refer to 'user-oriented' (as opposed to 'content-oriented') social network sites; which emphasize social relationships and communities. The distinction between 'content-oriented' and 'user-oriented' social networks was proferred by G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), 'Online Social Networks: Status and Trends', *l.c.*, 2011, p. 220.

[9] d.m. boyd and N.B. Ellison, 'Social Networking Sites: Definition, History and Scholarship', *l.c.,* p. 211.

[10] J. Heidemann, M. Klier and F. Probst, 'Online social networks: A survey of a global phenomenon', *l.c.*, p. 3867.

derived from advertising.[11] These business models are based on the principle that 'free' services can attract large and diverse audiences, which in turn will attract advertisers.[12] Popular OSNs, which have a large number of active users, can develop rich sets of demographic and behavioral data.[13] The profile information of these users, together with information about their activities (e.g., web browsing, app usage, 'likes', current location, etc.), can be used to enhance audience segmentation and contextual awareness.[14] This ability is of great interest to advertisers, who are eager to see advertisements presented to users who are likely to be influenced by them. The data flows which facilitate behavioral targeting are represented in Figure 1 by arrows (4) through (10). Each of these data flows will be elaborated further over the following sections.

2.3 (Third-party) Application provider

Third-party applications (often referred to simply as 'apps') have become a popular feature on OSNs.[15] An app is a standardized piece of software that runs on a computing platform.[16] In principle, an app can provide just about any functionality: gaming, content

[11] For an early analysis of different revenue models for OSN see A. Enders, H. Hungenberg, 'The long tail of social networking. Revenue models of social networking sites', *European Management Journal* 2008, Vol. 26, p. 199– 211. For a more recent study see G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), 'Online Social Networks: Status and Trends', *l.c.*, 2011, pp 213-234. Alternative and/or additional revenue sources include subscription fees (e.g., for 'premium' accounts) and platform purchases (e.g., by charging a percentage on the purchase of apps or other products which were bought through the OSN platform).

[12] G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), 'Online Social Networks: Status and Trends', *l.c.*, p. 221.

[13] *Ibid*, p. 222.

[14] Facebook, for example, enables third parties to target advertisements to its users on the basis of location, gender, age, likes and interests, relationship status, workplace and education (see https://www.facebook.com/help/207847739273775). (See also R. Heyman and J. Pierson, 'An Explorative Mapping of the Belgian Social Media Value Network and its Usage of Personal Identifiable Information', paper presented at *IFIP Summerschool on Privacy & Identity Management* 2013, p.2.) In April of 2013, Facebook added 'partner categories' as an additional targeting feature, which enables advertisers to target individuals based on the basis of their purchase behavior outside the social network. See https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature (last accessed 17 December 2013). For a survey of different targeting methods using social networking information see A. Bagherjeiran, R.P. Bhatt, R. Parekh and V. Chaoji, 'Online Advertising in Social Networks', in B. Furht (ed), *Handbook of Social Network Technologies and Applications*, 2010, Springer, New York, p. 653 et seq.

[15] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *Proceedings of ACM Conference on Online Social Networks* (CSON) 2013, preprint version available at http://www.sba-research.org/wp-content/uploads/publications/AppInspect_peprint.pdf

[16] OECD, 'The App Economy', *OECD Digital Economy Papers* 2013, No. 230, OECD Publishing, available at http://dx.doi.org/10.1787/5k3ttftlv95k-en (last accessed 19 December 2013). Apps can be divided among two main categories: 'mobile' or 'web-based'. In case of mobile apps, the 'computing platform' that hosts the app is a mobile device, typically a smartphone or a tablet. In case of web-based apps, the app itself is hosted on a webserver which is controlled by the application provider. While mobile apps are stored on a smartphone rather than a webserver, many mobile apps still communicate with a webserver. For purposes of simplicity, we will approach our discussion of third-party applications under the assumption that they are web-based, except when explicitly indicated otherwise. For an in-depth discussion of mobile apps on smart

streaming, location sharing, crowd funding … the possibilities are endless. Several major OSN providers now allow third-party application developers to offer their apps through the OSN.[17] This in turn permits users to enhance their OSN experience with additional functions and features.

Some apps are 'socially aware', meaning that they consume OSN data (e.g., profile data, relationship information) to deliver their functionality. For example, a horoscope application might require the birthdates of you and your contacts in order to create a compatibility chart. Other apps do not require user data to function as such, but use them to incorporate other aspects of social networking.[18] For example, users might be encouraged to share gaming high scores or to display which music feeds they are listening to on their profile. The data collected by apps may also be used to facilitate behavioral targeting (cf. *infra*).

While an app may be accessible through an OSN website, the app itself typically runs on a third-party server (i.e., outside the OSN domain).[19] In order to make app usage an integral part of the user experience, the OSN provider can embed applications within the OSN website (e.g., as an iframe).[20] In this approach, the OSN provider effectively acts as a proxy between OSN users and third-party application providers.[21] Alternatively, the OSN provider can simply direct its users to the websites of the application providers.

App usage is generally predicated upon the granting of permissions. Most applications stipulate a number of permissions which must be granted before the app can be used. Such permissions typically concern access rights (e.g., the ability to access to profile information, photo's, etc.) and/or the ability to act on the user's behalf (e.g., to post on a message board or send an email on behalf of the user).[22]

---

devices see Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', WP202, 27 February 2013, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (last accessed 20 January 2014).

[17] W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and Privacy of Online Social Network Applications', in L. Caviglione, M. Coccoli and A. Merlo (eds.), *Social Network Engineering for Secure Web Data and Services*, IGI Global, 2013, p. 207 et seq.

[18] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 2.

[19] *Id.* In earlier implementation models, social applications were deployed on the infrastructure of the OSN itself (this model is sometimes referred to as the 'gadget paradigm'). Increasingly, however, a different model is followed, whereby applications are delivered through an Applications Programming Interface (API) (also referred to as the 'distributed' paradigm). (W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and Privacy of Online Social Network Applications', *l.c.*, p. 208.)

[20] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 2. See also W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and Privacy of Online Social Network Applications', *l.c.*, p. 211 et seq.

[21] *Ibid*, p. 1.

[22] In practice, the OSN user delegates one or more access rights to the application provider using a pre-determined protocol (e.g., OAuth). Once the permissions have been granted, the application provider will query the social network application programming interface (API) to make use the delegated privileges (e.g., access profile information, post to wall). (W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and

Once permissions have been granted, the application provider can use these privileges to collect personal data from the OSN provider. It can also collect additional information from users directly (e.g., by monitoring application usage). These data flows are depicted in Figure 1 as arrows (2) and (3). Arrow (2) is bi-directional because application providers may also send their users data about other users (e.g., music feeds or current location).

2.4 (Third-party) Tracker

Web tracking is pervasive. It has become practically impossible to navigate the web without multiple entities keeping tabs on which sites we visit, which pages we view or how much time you spend on a particular page. In the context of this deliverable, we use the term 'tracker' to refer to any entity that collects and/or analyzes data relating to the browsing activities of OSN users.[23]

There are many different ways of tracking individuals online.[24] The most well-known technique involves the use of 'cookies'.[25] Cookies are browser files deployed by website operators in order to keep track of their interactions with a particular visitor.[26] Very often, individuals also receive cookies emanating from third party domains ('third-party cookies'), which can be used to monitor their browsing behavior across different websites.[27] Other well-known tracking techniques involve use of javascripts and browser fingerprinting.[28]

By monitoring individuals' browsing activities over time, trackers are able to build rich behavioral profiles. These profiles can in turn be used for online behavioral advertising

---

Privacy of Online Social Network Applications', *l.c.*, p. 208). See also M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 1-2.

[23] We have bracketed the term 'third party' to indicate that several OSN provider deploy their own tracking technologies to monitor user behavior inside and outside the OSN.

[24] See C. Casteluccia, 'Behavioural Tracking on the Internet: A Technical perspective', S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, 2013, Springer Science+Business Media, p. 21 et seq. for an inventory of prevalent web tracking techniques.

[25] A cookie is an alphanumeric text file which is stored by a web browser. Cookies are typically set by web servers the first time a user visits a particular site. They are then sent back automatically by the browser each time it accesses the web server that placed them. (C. Casteluccia,'Behavioural Tracking on the Internet: A Technical perspective', *l.c.*, p. 23-24 and Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising', WP 171, 22 June 2010, p. 7, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed 3 January 2013).

[26] This technique may be particular useful for identifying returning visitors and recording user preferences (e.g. language preferences).

[27] For example, a web page may contain images, links, iframes or other components stored servers in other domains. When the user accesses the website, these components will be retrieved from the third-party domain, which allows for the placement of third-party cookies. This technique can be used to effectively track users across multiple sites (in particular across all pages where one has placed an advertising image or web bug) (C. Casteluccia,'Behavioural Tracking on the Internet: A Technical perspective', *l.c.*, p. 23-24.)

[28] See C. Casteluccia,'Behavioural Tracking on the Internet: A Technical perspective', *l.c.*, p. 21 et seq.

(OBA), which is an important source of revenue for trackers.[29] In many cases, third-party trackers work on behalf of an ad network, whose goal it is to target ads with the maximum effect possible.[30]

A 2008 study by Krishnamurthy and Wills showed that individuals' activities on OSN may be subject to third-party tracking. Specifically, they found that several user actions (e.g. logging in, viewing a profile page, leaving a message) on OSNs such as Facebook and Myspace resulted in the retrieval of objects from third-party domains.[31] The access of third-party domains in this context suggests that OSN users may be tracked by third parties even when they are engaged in social networking activities (in addition to being tracked during other browsing activities).[32] In a follow-up study, the same authors found that many OSNs also leak additional information about OSN users, such as name, gender or OSN unique ID.[33] This means that the browsing behavior of a particular OSN user – including his or her behavior outside of the OSN context - may be easily linked to his or her OSN identity.[34]

The data flows related to tracking of OSN users are depicted in Figure 1 by arrows (4) and (5). Arrow (4) represents tracking which occurs via the browsers of OSN users (arrow (4)). In this scenario, the OSN provider does not directly share information about the user with trackers. Instead, it is sufficient for the OSN provider to embed components

[29] The Article 29 Working Party defines behavioural advertising as advertising which is based on the observation of the behavior of individuals over time. By studying the characteristics of individuals' behavior over time (repeated site visits, interactions, keywords, etc), trackers can develop specific profiles on individuals, which in turn allows tailoring advertisements to the inferred interests of each individual concerned. (Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising', *l.c.*, p. 4).

[30] An ad network is an entity that connects website owners ('publishers') with advertisers. In this model, a website owner simply needs to reserve a certain amount of visual on its website that will serve to display ads and relinquish the rest of the process to one or more ad network providers. The ad network provider is then responsible for distributing advertisements to publishers (on behalf of companies seeking to advertise). (Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising', *l.c.*, p. 5.) As indicated earlier, many OSN providers offer targeting options which function independently of third-party trackers, using criteria derived from e.g. the profile information of their users. In this model, the OSN provider uses its own targeting technology and makes its own decisions about ad placement and distribution (in accordance with advertiser demands).

[31] B. Krishnamurthy and C.E. Wills, 'Characterizing Privacy in Online Social Networks', *WOSN* 2008, Proceedings of the 1st ACM workshop on Online social networks, 2008 p. 40.

[32] *Ibid*, p. 41.

[33] B. Krishnamurthy and C.E. Wills, 'On the Leakage of Personally Identifiable Information Via Online Social Networks', *WOSN 2009*, Proceedings of the 2nd ACM workshop on Online social networks, 2009, p. 7. See also C. Casteluccia, 'Behavioural Tracking on the Internet: A Technical perspective', *l.c.*, p. 28.

[34] *Id.* See also J. Cheng, 'Social networks make it easy for third parties to identify you', *Ars Technica*, 25 September 2009, available at http://arstechnica.com/security/2009/09/which-user-clicked-on-viagra-ads-ask-myspace-and-facebook (last accessed 7 January 2013).

which result in the retrieval of third-party objects.[35] As indicated above, however, this retrieval may also involve leakage of additional information from the OSN.

Arrow (5) depicts the data flows which take place in situations where an OSN provider actively collaborates with a tracker. This might occur, for example, in situations where the tracker is working on behalf of the OSN provider (e.g., if the OSN provider wishes to collect data about its users browsing activities).[36]

It is worth noting that application providers and third-party websites similarly embed components which facilitate third-party tracking and ad delivery. This is depicted in Figure 1 by arrows (6) and (8).[37]

Finally, we would like to mention that tracking of OSN users is not limited to their browsing activities. With the rise of mobile OSNs (e.g., Foursquare) and mobile apps more generally, location tracking is increasingly used supplement the behavioral profiles of OSN users.[38]

2.5 (Third-party) Data broker

Data brokers (also referred to as 'data aggregators' or 'information resellers') are entities which collect and sell information. To be more specific, a data broker is a company that collects data, including personal data, from a wide variety of sources with a view of turning these data into marketable commodities.[39] Among the products offered by data brokers are consumer profiles (which categorize individuals into pre-determined consumer segments) and scoring products (which score the likelihood for certain behaviors, based on inferences drawn from other data).[40]

Several data brokers also collect data about individuals from OSN sites.[41] For example, data broker Acxiom reportedly collects data regarding individuals' social media

---

[35] Arrow (4) is bi-directional arrow because every time a user accesses a webpage which links to the tracker's server, the cookie that is stored in the user's browser will be updated with data about the user's latest interactions.

[36] We have bracketed the term 'third party' to indicate that several OSN provider deploy their own tracking technologies to monitor user behavior inside and outside the OSN.

[37] Arrows (7) and (9) are misleading to the extent that tracking occurs via the browser or operating system of the user (in which case they would simply coincide with arrow (4). We deliberately chose this way of visual representation to make clear that users can be tracked across a wide range of activities, i.e., across web browsing, OSN usage and app usage.

[38] See C. Casteluccia, 'Behavioural Tracking on the Internet: A Technical perspective', *l.c.*, p. 29.

[39] Based on Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, March 2012, p. 68, available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[40] U.S. Senate Committee on Commerce, Science and Transportation, 'A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes', Staff Report for Chairman Rockefeller, 2013, p. 12 and 23 available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 (last accessed 6 January 2014).

[41] Other avenues include government records and other public data, purchase or license from other data collectors, cooperative agreements with other companies, self-reporting by consumers (e.g., through surveys

usage to predict whether he or she should be considered a 'heavy social media user', 'poster', 'video sharer', 'social influencer', or 'social influenced'.[42]. Several data brokers reportedly also use click-stream data (i.e. data relating to individuals' browsing behavior) in developing consumer profiles.[43]

Information collected by data brokers is put to a variety of uses. Prominent examples include identity verification, fraud prevention, marketing, credit risk assessments and background checks.[44] Some data brokers also offer products that enable marketers to use off-line data to target individuals online.[45] These products can also be put to use in an OSN context. Facebook, for example, has partnered with data brokers such as Acxiom, Datalogix and Epsilon so that advertisers can target OSN users on the basis of their purchasing behavior outside the social network.[46] Facebook has reportedly also partnered with data broker BlueKai to enable further targeting of OSN users on the basis of their browsing activities outside the OSN.[47]

Figure 1 visualizes the corresponding data flows as follows: arrow (9) represents the exchange of personal data that takes place between data brokers and social networks. It is important to note that the collection of personal data by data brokers does not necessarily involve 'active' disclosure by the OSN provider (e.g., the data might simply be collected from publicly available OSN sites). Arrow (9) is bi-directional as data brokers may also indirectly reveal data about OSN users to the OSN provider (e.g., regarding their inferred interests).[48]

---

or questionnaires). U.S. Senate Committee on Commerce, Science and Transportation, 'A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes', *l.c.*, p. 15.

[42] *Ibid*, p. 21.

[43] *Id.* See also OECD, "Exploring data-driven innovation as a new source of growth: Mapping the policy issues raised by "big data"", in OECD, Supporting Investment in Knowledge Capital, Growth and Innovation, 2013, OECD Publishing, doi: 10.1787/9789264193307-12-en, p. 328, available at http://www.oecd-ilibrary.org.

[44] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, March 2012, l.c., p. 68

[45] U.S. Senate Committee on Commerce, Science and Transportation, 'A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes', *l.c.*, p. 12.

[46] Specifically, Facebook has added 'partner categories' as an additional targeting feature, which enables advertisers to target individuals based on the basis of their purchase behavior outside the social network. See https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature (last accessed 17 December 2013). See also C. Dello, 'Facebook to Partner With Acxiom, Epsilon to Match Store Purchases with User Profiles – Can Facebook Ads Drive Offline Buying?', *Advertising Age*, 22 February 2013, available at http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-store-purchases-user-profiles/239967 (last accessed 7 January 2014).

[47] K. Opshal and R. Reitman, 'The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads', Electronic Frontier Foundation (EFF), 22 April 2013, available at https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads (last accessed 7 January 2014).

[48] In case of Facebook, user targeting is achieved through a matching function which has been explained as follows: a company contacts a data broker with a particular audience in mind (e.g., people interested in losing weight). The data broker then generates a list of email addresses of people it believes that belong to that audience. It then creates a cryptographic hash function for each of the email addresses of each person on the list and sends these hash functions to Facebook. Facebook then compares this list of hash functions to its own list of hash functions of email addresses belonging all Facebook users and then identifies the relevant users as

Arrows (7), (10) and (11) intend to illustrate that data brokers may also obtain information about individual OSN users from trackers (e.g., browsing history), application providers (e.g., app usage) or third-party website operators (e.g., purchase history).

2.6 (Third-Party) Website

Earlier, we discussed how several OSNs allow third-party application providers to gain access to social networking data. The ability to interact with social networking data is not reserved to app providers alone, however. Most OSNs offer a range of tools to support interaction between third-party websites and OSN data. For example, OSNs such Facebook and MySpace allow third parties to leverage their authentication services, so that individuals can make use of their OSN credentials when accessing these websites (and therefore do not need to create a separate username and password).[49]

'Social plug-ins' are another way in which third-party websites can interact with OSNs. A social plug-in is a website component designed to facilitate the sharing of third-party content within OSNs. Facebook's 'like button', for example, enables users to leave positive feedback for a web page and to share it with others.[50] Similar tools are offered by other OSNs such as Google+ ('+1'), Pinterest ('Pin it') and Linkedin ('in share').

Embedding social plug-ins can help increase the visibility of a webpage. It also enriches the data exchanged within OSNs, so these tools are generally considered beneficial for both website operators and OSN providers. For OSN users, the presence of social plug-ins offers convenience, as it enables them to share third-party content within their OSNs almost seamlessly.[51] Nevertheless, the increased presence of social plug-ins on third-party websites has also engendered some controversy. Specifically, it has been demonstrated that many social plug-ins enable the OSN provider to monitor the browsing activities of its users beyond the context of the OSN.[52] This tracking capability may exist even if the user

---

being part of the target group. (K. Opshal and R. Reitman, 'The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads', *l.c.*). In case of targeting based on browsing activity, mapping OSN users with the intended audience is done through a process referred to as 'cookie matching'. Even if data brokers do not directly share any data with Facebook other than the relevant hash functions, Facebook might still be able to glean information of the user based on what is being advertised (*Id.*).

[49] M.N. Ko, G.P. Cheek and M. Shebab, 'Social-Networks Connect Services', *Computer* 2010, Issue n° 8, IEEE Computer Society, p. 37. The Facebook platform (Facebook's API) also allows third-party sites to obtain authorization tokes from Facebook. This basically works as follows: the user first authenticates herself using Facebook as their identity provider. Next, Facebook issues a token that allows the third-party site to access the user's basic profile information. The third-party site can then request additional permissions, much in the same way as (other) application providers (*Ibid*, p. 38-39). See also *supra*; section 2.3.

[50] G. Kontaxis, M. Polychronakis, A.D. Keromytis and E.P. Markatos, 'Privacy-Preserving Social Plugins', *Proceedings of the 21st USENIX conference on Security symposium*, 2012, p. 30, available at https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final150.pdf (last accessed 8 January 2014).

[51] *Id.*

[52] *Id.* See also A.P.C. Roosendaal, "We Are All Connected to Facebook … by Facebook!", in S. Gutwirth et al. (eds), *European Data Protection: In Good Health?*, Springer, 2012, p. 3-19. An earlier version of this paper is

does not actually click on the plug-in at hand. It is sufficient that the plug-in has been embedded on the website in question.[53] Moreover, the tracking capability offered by plug-ins is not limited to OSN users. Even if an individual does not have an account with a particular OSN provider, the presence of its social plug-ins may allow it to uniquely identify this individual and to keep track of its visits to other pages in which the plug-in has been embedded.[54]

The data flows between OSN providers and third-party websites are depicted in Figure 1 by two arrows (12): the first is a solid bi-directional arrow which represents those flows which can be easily observed or inferred by OSN users. This is the case, for example, if an OSN user decides to use its OSN credential to log-in to a third-party website or to link third-party content to his or her profile. The second arrow is a dashed arrow which is meant to capture the leakage of browsing behavior through social-plug-ins.[55] We have bracketed the term 'third party' to indicate that an OSN provider may also operate websites outside the OSN context (e.g., Google owns Youtube in addition to Google+).

2.7 Other observers

The previous sections have introduced some of the main players interacting with OSN-related data on a regular basis. An additional category of actors worth identifying is what we refer to as 'other observers'. Other observers are entities who, regardless of

available on SSRN as A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', *Tilburg Law School Legal Studies Research Paper Series*, No. 03/2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563 (last accessed 8 January 2013).

[53] *Id.*

[54] *Id.* This happens much in the same way as third-party tracking: when a person visits a webpage in which a social plug-in is embedded, the user's browser will also query the domain of the OSN (plug-in) provider. When queried the OSN (plug-in) provider will also send along a cookie which uniquely identifies the website visitor (and links it to the OSN user's account if applicable). For more detailed information see M.N. Ko, G.P. Cheek and M. Shebab, 'Social-Networks Connect Services', *l.c.*, p. 38-39 and A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', *l.c.*, p. 4-8. This issue was investigated by the Irish Data Protection authority in 2011, who considered that the collection of these data by Facebook shall be considered lawful as long as Facebook retained only the minimum information necessary for a limited period of time, and does not use these data for profiling purposes: see Data Protection Commissioner, 'Report of Audit – Facebook Ireland Ltd.', 21 December 2011, p. 81-86, available at http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf (last accessed 12 February 2014). However, the French Data Protection Authority (CNIL) has taken the position that website operators should only activate social plug-ins once the visitor of the website expresses his or her consent with regards to the placement of the corresponding cookies. See Commission nationale de l'informatique et des libertés (CNIL), *Solutions pour les boutons sociaux*, http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/outils-et-codes-sources/les-boutons-sociaux/ (last accessed 3 December 2014). Tools such as « Social Share Privacy » enable website operators to de-active social plug-ins until the website visitor decides he or she wishes to make use of a particular plug-in. For more information see http://panzi.github.io/SocialSharePrivacy/.

[55] Dashed arrow (12) is misleading - in a way similar to arrows (7) and (9) - to the extent that tracking occurs via the browser or operating system of the user (in which case they would coincide simply with arrow (4). We deliberately chose this way of visual representation to make clear that users can be tracked by OSN providers across websites who have embedded their social plug-ins.

whether or not they have a formal relationship with an OSN or its users, access data that is processed in the context of an OSN. Such access takes place regularly, and for a plethora reasons: market research, student oversight, law enforcement, intelligence gathering, credit risk assessment, employee background checks, disability verification etc. Online news outlets are brimming with reports of how schools, employers, intelligence agencies and other entities are using social media to monitor individuals' activities.

For example, school administrators are often cited as reviewing social networking data for inappropriate student behavior, such as underage drinking.[56] Recently, a Californian high school even hired a firm to monitor public postings on social media to search for possible violence, drug use, bullying, truancy and suicidal threats.[57]

Employers are also known to consult OSNs when evaluating job applicants; or to take disciplinary action towards employees (even firing) after learning about unwanted behavior through social media data.[58]

Last, but definitely not least, recent revelations concerning intelligence operations have indicated that national security agencies also use social networking data to evaluate potential national security threats.[59]

Arrow (13) represents the data flows which take place in situations where observers access OSN-related data. It is important to note that an observer may also access these data indirectly, e.g. via a data broker or tracker (arrows (14) and (15)).[60] Finally, it is worth underlining that the observation of OSN data is not necessarily limited to data which

[56] See e.g., Associated Press, 'District to monitor students MySpace pages', NBC news, 23 May 2006, available at http://www.nbcnews.com/id/12937962/#.Us50c7R_tGM; N. Buczek, 'Schools discipline students of Internet content', 22 February 2006, http://thefire.org/index.php/article/6855.html (last accessed 9 January 2014).

[57] M. Martinez, 'California school district hires firm to monitor students' social media', CNN, 18 September 2013, available at http://edition.cnn.com/2013/09/14/us/california-schools-monitor-social-media (last accessed 8 January 2014).

[58] See e.g., C.A. Ciocchetti, 'The eavesdropping employer: a twenty-first century framework for employee monitoring', Future of Privacy Forum, 2010, p. 45 available at http://www.futureofprivacy.org/wp-content/uploads/2010/07/The_Eavesdropping_Employer_%20A_Twenty-First_Century_Framework.pdf (last accessed 9 January 2013). According to a 2009 study by Proofpoint, an internet security firm, 8 percent of companies with one thousand employees or more have terminated at least one employee for comments posted on a social networking site. See A. Ostrow, 'Facebook Fired: 8% of US Companies have Sacked Social Media Miscreants', Mashable, 10 August 2009, available at http://mashable.com/2009/08/10/social-media-misuse (last accessed 10 January 2013).

[59] See e.g., E. MacAskill, J. Borger, N. Hopkins, N. Davies and J. Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, Friday 21 June 2013, available at http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (last accessed 9 January 2013).

[60] For examples see K. Opshal and R. Reitman, 'The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads', *l.c.*

has been labelled as 'public' according to the user's privacy settings (e.g., in case of surreptitious eavesdropping or co-operation with law enforcement officials).[61]

2.8 Infrastructure (Service) Provider

A final category of actors which is worth mentioning are what we refer to as 'infrastructure (service) providers'. These are the entities that operate the technical infrastructure which is necessary for OSN providers to offer their services and for OSN users to make use of the OSN. are Examples include Internet Service Providers ('ISPs'), hosting service providers, device manufactures, the providers of operating systems, etc. While we will not discuss the role of these entities with great detail, it is nevertheless worth noting their important role in enabling OSN interactions.

[61] See Facebook, 'Global Government Requests Report' for an aggregate overview of the data requests received by Facebook from government officials during the first 6 months of 2013, available at https://www.facebook.com/about/government_requests (last accessed 9 January 2013).

3. Legal framework

Now that we have identified the main types of actors engaging with OSNs, we will proceed to analyze their legal status. It is impossible, within the context of a single deliverable, to provide an in-depth analysis for every single activity described in the previous chapter. Instead, our analysis will be focused on 3 central actors and 3 legal instruments. The actors we have chosen as focal points for our legal analysis in the context of the SPION project are the OSN provider, OSN users and third-party application providers. The three legal instruments are:

1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the 'Data Protection Directive')[62];
2. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the 'E-Privacy Directive')[63]; and
3. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market[64] (the 'E-Commerce Directive').

The first two instruments were selected because they contain the main rights and obligations of OSN users, OSN providers and third party application developers in relation to the processing of personal data. The third instrument, the E-Commerce Directive, was selected because it contains important liability exemptions which may be held applicable to the providers of OSNs or related applications. Only the first two instruments will be analyzed in the context of this deliverable. The third instrument, the E-Commerce Directive, will be analyzed in SPION deliverable D6.3 ('Liability and accountability of actors in social networking sites').

---

[62] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Official Journal of the European Union, n° L 281, 23 November 1995, p. 31–50. Hereafter also referred to as 'Directive 95/46/EC' or simply 'the Directive'.

[63] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L201, pp. 37-47 (31 July 2002). This Directive was amended in 2009 by the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, (OJ L 337, 18.12.2009).

[64] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *O.J.* 17 July 2000, L 178/1-16.

Other important sources of rights and obligations are the terms and conditions and privacy notices of both OSNs and application providers, as well as well as the OSN terms and conditions for developers. Where appropriate, reference shall also be made to the role and impact of these instruments.

3.1 Data protection

a. Scope

Ratione materiae

Directive 95/46/EC applies to the processing of personal data.[65] In order to assess its applicability vis-à-vis OSNs, one must first establish which types of data are involved. Schneier has developed a taxonomy of 'social networking data', which distinguishes among the following six categories of data[66]:

1. *Service data*: data provided to an OSN provider in order to make use the OSN (e.g., legal name, age)
2. *Disclosed data*: data that is posted by OSN users on their own profile pages (e.g., blog entry, picture, video)
3. *Entrusted data*: data that is posted by OSN users on the profile pages of other OSN users (e.g., a wall post, comment)
4. *Incidental data*: data about an OSN user which has been uploaded by another OSN user (e.g., a picture)
5. *Behavioral data*: data regarding the activities of OSN users within the OSN (e.g., who they interact with and how)
6. *Derived data*: data which is inferred from (other) OSN data (e.g., membership of group X implies attribute Y).

Each of these social networking data will qualify as personal data insofar as they relate to an identified or identifiable individual.[67] It is not required that the individual in question be identified by his or her full name. Even where individuals do not appear to be

[65] Specifically, article 3(1) provides that Directive 95/46 shall apply '*to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*'. This essentially includes any automated operation performed upon personal data. Two areas are excluded by art. 3(2) of the Directive: processing of personal data (a) in the course of an activity which falls outside the scope of Community law and (b) by a natural person in the course of a purely personal or household activity.

[66] B. Schneier, 'A Taxonomy of Social Networking Data', *Security & Privacy* 2009, IEEE, Vol. 8, Issue 4, p. 88. While overlap among the identified categories is possible, the taxonomy is helpful

[67] According to the Article 29 Working Party, data relates to an individual '*if it refers to the identity, characteristics or behavior of an individual, or if such information is used to determine or influence the way in which that person is treated or evaluated*' (Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP 136, 20 June 2007, p. 10.)

easily identifiable (e.g., when an alias is used), they may be indirectly identifiable through (a combination of) other data, such as the personal attributes listed in their profile (e.g., age, residence, etc.), their list of friends, traffic data (e.g., IP-addresses) or cookie data. As a result, much of the data processed in the context of OSNs will qualify as 'personal data' in the meaning of Directive 95/46/EC.

Ratione personae

Once it has been established that a certain activity falls within the material scope of Directive 95/46, one must determine which entity (or entities) is (are) responsible for ensuring compliance. Directive 95/46 assigns the responsibility for compliance to the 'controller', who is defined by article 2(d) as

> '*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data [...]* (emphasis added)'

The definition of a 'controller' contains two main components. First, there is a reference to the exercise of a determinative influence ('determines'), which is generally understood as an '*exercise of decision-making power*'.[68] The second component of the definition refers to the *object* of the controller's influence, namely the '*purposes and means of the processing of personal data*'. Commentators sometimes paraphrase art. 2(d) by saying that the controller is the entity deciding about the '*why and how*' of the processing[69]: given a particular processing operation, the controller is the entity who has determined *why* the processing is taking place (i.e., 'to what end'; or 'what for') and *how* this objective shall be reached (i.e., which means shall be employed to attain the objective). Classic examples include: an employer collecting data about job applicants as part of a recruitment process or a hospital using patient records for medical research purposes.[70]

Another important actor recognized by Directive 95/46/EC is the 'processor'. A 'processor' is defined as an entity who processes personal data *on behalf* of the data

---

[68] The ability to influence the processing may stem from a variety of circumstances. See Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP169, 16 February 2010, p. 10-12, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (last accessed 22 May 2013). See also B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46', *Computer, Law & Security Review* 2012, vol. 28, p. 30.

[69] See also Opinion 1/2010, *l.c.*, p. 13.

[70] Directive 95/46 recognizes that the purposes and means of the processing might be determined by more than one entity. Article 2 (d) alludes to this possibility by stating that the controller may determine the purposes and means of the processing '*alone or jointly with others*'. An example of joint control is the scenario where a travel agency, a hotel chain and an airline decide to create a common reservation portal, whereby they jointly decide which data will be stored, how reservations will be allocated and confirmed, who can have access to the information stored, etc. (Opinion 1/2010 *l.c.*, p. 22.)

controller (art. 2, (e)). This concept was introduced in light of the practice whereby one organization requests another organization to perform certain processing operations on its behalf. When an entity other than the controller (or its employee) carries out processing 'on behalf of' a controller, this organization shall be deemed a 'processor' rather than a 'controller'. This distinction is quite important seeing as processors shall, as a rule, only be indirectly accountable for compliance with Directive 95/46/EC.[71]

While the criteria set forth by articles 2(d) and (e) seem straight-forward in theory, their application in practice often is not. As the complexity of data processing increases, determining which entity - or entities - may be said to 'control' a particular processing operation can be quite challenging. This is especially the case when the data processing involves a range of different actors, who are each involved in the processing to a greater or lesser extent. Over the following sections, we will analyze to what extent OSN providers, OSN users and third-party application developers may be considered as 'controllers' within the meaning of article 2(d) of Directive 95/46.

b. OSN provider

OSN providers are generally considered to be 'controllers' within the meaning of Directive 95/46.[72] After all, they determine both the *purposes* and *means* of their own processing activities: their *purpose* is to provide a social networking service which generates revenue. They also determine the *means* of their own processing activities: they decide about the nature of the social networking service and how it will be provided – from user registration until account deletion. In addition to those operations that are strictly necessary to provide the OSN service, the provider also decides about a range of additional processing activities; including those designed to support targeted advertising.[73]

---

[71] B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46', *l.c.*, p. 25 et seq.

[72] See e.g. College Bescherming Persoonsgegevens, 'Publicatie van Persoonsgegevens op het Internet', *CBP Richtsnoeren*, December 2007, p. 7-8; ; B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *Identity in the Information Society* (IDIS) 2009, p. 70; Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', WP 163, 12 June 2009, p. 5; Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of controller and processor', *l.c.*, p. 21; P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *Computer Law & Security Review* 2010, Vol. 26, p. 537-538; E. Kosta, C. Kalloniatis, L. Mitrou and S. Gritzalis, 'Data protection issues pertaining to social networking under EU law', *Transforming Government: People, Process and Policy* 2010, Vol. 4, No. 2, p. 196; D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *International Law & Management Review* 2010, Vol. 6, p. 131; B.J. Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice', *Tilburg Law School Legal Studies Research Paper* Series No. 08/2012, p. 10 and Information Commissioner's Office (ICO), 'Social networking and online forums – when does the DPA apply?', 24 May 2013, Version 1.0, p. 10-11.

[73] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 70.

While most would agree that OSN providers should be considered as 'controllers', opinions vary as to the scope of their control. In certain cases, it is relatively clear whether or not an OSN provider acts is acting as a controller. For instance, few would dispute that an OSN provider acts as a controller in relation to:

- the collection of explicitly solicited data (e.g., information which OSN users are asked to provide when registering to the site, such as their name, age and place of residence) (cf. 'service data');
- their processing of user data for purposes of targeted advertising (e.g., analysis of 'behavioral data'); and
- their processing of user data designed to enhance the quality of the OSN service (e.g., use of facial recognition techniques to create 'tag suggests'[74]).

For other processing operations, however, the issue of whether or not an OSN provider is acting as a controller is less clear-cut. A particular contentious matter is whether or not an OSN provider should be considered as a (co-)controller in relation to content shared (spontaneously) by its users. For example, should an OSN provider be considered a 'controller' of the processing that takes place when its users share content with one and other (e.g., the sharing of a photograph among friends)? There are essentially four ways of approaching this issue.

First, several authors argue that web 2.0 service providers, such as OSN providers, should not be considered as controllers in relation to user-generated content at all.[75] After all, these entities exercise little or no control at the moment content is being uploaded. Moreover, requiring OSN providers to assume such control would have undesirable consequences, most notably for the freedom of expression of OSN users.[76] From this perspective, one could argue that only the OSN user who decides to upload certain content should be considered as a controller vis-à-vis this sharing activity.[77]

---

[74] See e.g. S. Curtis, 'Facebook defends using profile pictures for facial recognition' *The Telegraph*, 15 November 2013, available at http://www.telegraph.co.uk/technology/facebook/10452867/Facebook-defends-using-profile-pictures-for-facial-recognition.html.

[75] See e.g. G. Sartor, 'Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?', *International Data Privacy Law* 2013, Vol. 3, No. 1, p. 9-10.

[76] *Ibid*, p. 10.

[77] Certain authors have also argued that the OSN provider should instead be considered as a 'processor', which is defined by art. 2(e) as '*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*'. (see e.g. P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 537-538). This interpretation is at odds with 17(3) of Directive 95/46/EC, which implies a willingness, on the part of the processor, to only process personal data in accordance with the instructions issued by the controller. Moreover, this provision stipulates that this willingness must be expressed in the form of a legally binding instrument. Given that many OSN providers, in practice, reserve themselves the ability to modify the nature of their services at all times, often without prior consultation of their users, we would argue that they should not be considered as 'processors', but rather as separate controllers (whose 'control' extends to different aspects of the processing).

Other commentators argue that OSN providers should be considered as controllers in addition to OSN users. Specifically, they argue that the OSN provider should be considered a controller in relation to its social networking service 'as a whole'.[78] Once data have been uploaded, the OSN provider proceeds to perform operations upon them which enable the actual sharing of information (e.g., storage, analysis[79], dissemination, access control). And for these processing activities, the provider has determined the 'purposes and the means' in advance, independently of the OSN users.[80] Because the sharing of personal data among contacts is an essential component of its service, these commentators conclude that the OSN provider acts as a (co-)controller vis-à-vis the dissemination of content over its platform (even though the initiative to share this content originated from one of its users).[81]

A third approach, which combines elements of the previous two approaches, views both OSN users and OSN providers as controllers, but each 'for different combinations of data flows and purposes'.[82] In other words, both entities might act as controllers, but each for different aspects of the processing. They each exercise control, but 'at different stages' and 'to different degrees'.[83] While this approach allows for greater nuance and flexibility, its practical implications aren't always clear.

Finally, a fourth approach (which could also be viewed as an extension of the third approach) considers that the OSN provider may only be considered a 'controller' of personal data shared over its platform once it has obtained actual knowledge of its existence. Under this approach, it is the OSN user who shares the content which is seen as the 'primary' controller, while the OSN provider would only become a (secondary) controller once it has been notified of specific personal data processing.[84]

---

[78] See B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *Identity in the Information Society* (IDIS) 2009, p. 70.

[79] For example, algorithmic analysis carried out by the OSN provider may determine the degree of visibility given to a particular content item. In case of Facebook's 'Newsfeed', for instance, Facebook deploys an automated selection mechanism to establish relevancy of content posted by friends, which ultimately determines the degree of visibility a particular item receives. (see T. Bucher, 'Want to be on top? Algorithmic power and the threat of invisibility on Facebook', *New Media Society* 2012, Vol. 14, p. 1167 et seq.

[80] See B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 71.

[81] While this approach involves an expansive interpretation of the controller concept, these authors anticipate certain limitations as to the corresponding responsibilities and liabilities of OSN providers. For example, the indicate that OSN providers might be able to escape liability if they can demonstrate having continuously undertaken all reasonable measures to prevent the data protection violation from taking place, and to limit their effects once they have been manifested (see B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 71.)

[82] Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 537-538.

[83] Based on Opinion 1/2010, *l.c.*, p. 22. See also B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46', *l.c.*, p 32 et seq.

[84] This was essentially the reasoning of the Italian Supreme Court in its recent judgment concerning the *Google Video* case, see Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, sentenza n. 5107/14, at paragraph 7.2 ('*[…] as long as the offense is unknown to the service provider , it cannot be regarded as the controller of the processing, because it lacks any decision-making power on the data*

c. OSN Users

The users of an OSN may, in certain circumstances, also be considered as 'controllers' within the meaning of article 2(d), namely when processing data relating to other individuals.[85] In order to be qualified as a 'controller', the user must exercise decision-making power with regards to both the purposes and means of the processing operation (cf. *supra*). Generally speaking, the *purposes* for which OSNs are used vary according to two main parameters (1) the type of OSN, its technical features and its intended audience; and (2) whether the user is an individual or an organization. Private individuals typically use OSNs for purposes of social interaction, self-expression, career development, self-education, etc. Organizations, on the other hand, typically engage in OSN usage to further their organizational mission or corporate objectives (e.g., product promotion, membership recruitment, event planning).[86] In both cases, however, the OSN user can in fact freely determine why it processes personal data relating to others in the context of the OSN.

As to determining the technical *means* of the processing, OSN users generally do not have any real decision-making power. While they may have the ability to adapt some minor features or settings, they do not have any real power of negotiation as to the manner in which the processing is conducted. They either take it or leave it. But every OSN user does, as a rule, exercise the choice as to whether or not he wishes to share a particular piece of information and how to do so. In this sense OSN users still effectively determines the 'means' of their processing when entrusting data about others to an OSN.[87]

The control exercised by OSN users in principle extends to any content they choose to provide and any processing operations they undertake of their own accord (i.e., without

---

itself, and when, instead, the provider is aware of the illegal data and is not active for its immediate removal or makes it inaccessible, however, it takes a full qualification of the data controller') (unofficial translation based on Google translate). The full text of this opinion is available at http://www.dirittoegiustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html (last accessed 13 February 2014).

[85] An individual cannot act as a controller towards his or her own data. The regulatory scheme of Directive 95/46/EC is predicated on the notion that the data controller is an entity other than the data subject him- or herself. An individual person might act as a controller of personal data relating to others, but not of his or her own personal data. Accepting that the data subject could act as a controller of the processing of his own personal data would have rather absurd implications: the data subject would have to obtain consent from him- or herself, provide him- or herself with notice, etc.

[86] See also Information Commissioner's Office (ICO), 'Social networking and online forums – when does the DPA apply?', *l.c.*, p. 4

[87] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 70. One must, however, be careful not to exaggerate the decision-making power of the individual user. The controllership of the user does not extend to the SNS as a whole, but only to those processing operations for which he can actually determine the purposes and means.

solicitation).[88] For example, a company which uses an OSN for purposes of product promotion shall be considered a controller towards:

- any personal data that is included on the company's profile page (including its list of 'connections' or 'friends');
- any personal data which the company collects through the OSN (e.g., personal attributes of its connections);
- any information about individuals which the company disseminates through the OSN.[89]

For private individuals, the issue is less clear cut. The second indent of art. 3(2) provides that Directive 95/46 shall not apply to the processing of personal data '*by a natural person in the course of a purely personal or household activity*'. This exemption gives rise to the following question: to what extent can OSN usage be considered a 'purely personal or household activity'?

The European Court of Justice (ECJ) has provided further guidance regarding article 3(2), namely in the context of the *Lindqvist* case.[90] Here, the ECJ considered that the exception for personal use must

> '*be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*'.[91]

The Court thus put forward two elements to determine whether the personal use exception can be applied. In the first place the processing activity must be carried out '*in the course of private and family life'*. Secondly, the exception shall not apply where the data is published on the Internet and made accessible to an indefinite number of people.[92] The

---

[88] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 70.

[89] See also Information Commissioner's Office (ICO), 'Social networking and online forums – when does the DPA apply?', *l.c.*, p. 3.

[90] European Court of Justice , C-101/01, *Bodil Lindqvist*, 6 November 2003, available at http://curia.europa.eu. The facts of this case were as follows: Mrs. Lindqvist, who worked as a catechist in a local parish, had set up a number of web pages to provide information to fellow parishioners preparing for their confirmation. These pages also included information about several of her colleagues in the parish, who were referenced either by their full names or merely by their first names. In many cases telephone numbers were listed. The pages also described, 'in a mildly humorous manner' the jobs held by these colleagues and their hobbies. Other information was also mentioned, such as family circumstances; and of one colleague it was stated that she had injured her foot and was working half-time for medical reasons. Mrs. Lindqvist had not obtained the consent of the individuals referenced on her web pages, nor informed them of the fact that she was mentioning personal information about them. She also hadn't notified the data protection authority. She was subsequently prosecuted for violation of the Swedish law on personal data.

[91] European Court of Justice , *Bodil Lindqvist*, at paragraph 47 (emphasis added).

[92] The Belgian Privacy Commission, in a recommendation regarding the sharing of pictures by individuals, also touched upon the question of personal use. It considered that where images are processed for the sole purpose of distribution among a select ('definable') group of friends, family members or acquaintances, such

first criterion suggests that private OSN users, who make use of an OSN for purposes of social interaction, should in principle be able to avail themselves of the personal use exemption. After all, social interaction is an essential component of one's private or family life.[93] However, one must not lose track of the second element in the reasoning of the ECJ, namely that the exception shall not apply where the data is made accessible to an indefinite number of people. This implies that OSN users might not be able to invoke this exception once the data in question passes a certain threshold of accessibility.[94]

In its Opinion on social networking, the Article 29 Working Party indicated that the processing activities of private OSN users are generally covered by the personal use exception.[95] However, it also identified two situations in which the personal use exception will not apply. First, the exception will not apply if the individual is acting '*on behalf of a company or association, or uses the [OSN] mainly as a platform to advance commercial, political or charitable goals.*'[96] Second, the exception for personal use also will not apply if the individual '*takes an informed decision to extend access beyond self-selected "friends"*'.[97]

In conclusion, one can state that OSN users may be considered as 'controllers' within the meaning of article 2(d). Organizations and companies shall in principle be subject to the same set of responsibilities as those incumbent upon controllers in any other context. In case of private individuals, the applicability of Directive 95/46/EC depends on whether or not the OSN usage falls within the remit of the personal use exemption. The implications of this outcome will be discussed *infra*; section 4.3.a.

---

processing could fall under the exception of personal use. As examples it mentioned the transmission of pictures via email to the participants of a family event, or the posting of such pictures on a secured website, which is only accessible to the relevant family members; and which is protected against indexing by search engines. (Commissie voor de Bescherming van de Persoonlijke Levenssfeer, 'Aanbeveling uit eigen beweging inzake de verspreiding van beeldmateriaal' Aanbeveling nr. 02/2007, 28 november 2007, p. 21-22, available at www.privacycommision.be The Dutch Data Protection Authority adopted an almost identical approach shortly thereafter in its Guidance Report relating to the publication of personal data on the internet (See College Bescherming Persoonsgegevens, 'Publicatie van Persoonsgegevens op het Internet', *CBP Richtsnoeren*, December 2007, p. 12–13).

[93] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 74.

[94] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *Computer Law Review International (Cri)* 2010, Vol. 4, p. 103.

[95] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 5.

[96] *Id.*

[97] *Id.*

d. Application providers

Third-party application providers will typically also be considered as 'controllers' within the meaning of article 2(d).[98] Similar to OSN providers, the objective of most application providers is to provide a service which generates revenue. [99] The nature of this service will depend on the intended functionality of their application(s): gaming, content streaming, location sharing, crowd funding … .[100] In this sense, they determine the *purposes* of the processing of user data that takes place when they provide their services. Application providers also determine the *means* of their processing: they decide which data to collect regarding OSN users and how these data will be subsequently processed. In addition to deciding about those activities which are necessary to deliver the app's functionality, the provider may also decide about additional processing activities; including those designed to enable targeted advertising.

When collecting data related to OSN users, application providers are not entirely free in deciding how this collection shall be organized. As indicated before, many application providers obtain access to OSN data by soliciting permissions from OSN users. Once these permissions have been granted, the application provider will query the social network's Application Programming Interface (API) to make use the delegated privileges (e.g., access profile information, post to wall).[101] Using the API of an OSN is generally subject to a number of terms and conditions, which are stipulated by the OSN provider. As a result, application providers are in principle bound by the limitations and restrictions imposed by the API terms when soliciting, collecting and processing OSN data.[102]

---

[98] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 5.See also P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 540-541.

[99] As in the case of OSNs, many application providers derive (a portion of) their revenue from targeted advertising (so-called 'in-app advertising'). Application providers may also charge money for the downloads of their apps, for in-app purchases or for premium subscriptions. For an overview of the different revenue models of mobile apps see OECD, 'The App Economy', *l.c.*, p. 22-26.

[100] Cf. *supra*; section 2.3.

[101] W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and Privacy of Online Social Network Applications', l.c., p. 208. See also M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 1-2. A number of OSN providers, which include Google, Myspace and Yahoo united their efforts to develop a uniform social application programming interface, which is called '*OpenSocial*'. The goal of this initiative is to allow application developers to offer their applications to users from various OSNs and to enable their functionality across OSNs. See W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and Privacy of Online Social Network Applications', l.c., p. 210. See also F. Le Borgne-Bachschmidt et al., 'User-Created-Content: Supporting a participative Information Society', Final Report, 2008, p. 243, available at http://www.ivir.nl/publications/helberger/User_created_content.pdf (last accessed 28 January 2014).

[102] For more information regarding Terms & Conditions of OSN APIs see A. Kuczerawy, 'Legal and ethical analysis', *Exploiting Social Networks for Building the Future Internet of Services* (SocIoS), Deliverable D3.5, p. 21-29. While third-party application providers are bound by API terms, they in principle decide autonomously whether they wish to collect certain data via an OSN and how to use it. Although they too must 'take it or leave it', they exercise a choice when deciding to collect data about individuals through an OSN API. In this sense application providers still effectively determine the 'means' of their processing when collecting data about OSN users in this way.

The access rights of application providers may vary across platforms. In case of Facebook, for example, application providers are granted access to the user's 'basic information' by default.[103] This information includes user ID, name, picture, gender, locale and friend connections.[104] Additionally, application developers may also request access to several additional permission classes (e.g., 'email permissions', 'extended profile properties', 'extended permissions', etc.).[105] These permissions may, for example, enable the application provider to post information on behalf of users or to access private messages.[106] Other OSN platforms support different access control models; which may be either more granular or more coarse-grained.[107]

The control exercised by application providers in principle extends to any processing which takes place to support the application's functionality. It also extends to any processing undertaken by the application provider to enable targeted advertising (e.g., disclosure of a user's location to support contextual advertising).[108] Depending on the nature of the application, the application provider might also enable users to share content with others. If this is the case, the provider is likely to face uncertainties similar to those of OSN providers regarding their obligations vis-à-vis user-generated content (see also *infra*; section 4.3.b).

e. Other entities

In the previous section, we identified a range of additional actors interacting with OSN data, such as trackers, data brokers and other observers. Each of these entities will typically also be considered as 'controllers' in their own right, at least insofar as they pursue their own purposes in processing these data. In cases where they do not determine their own purposes, or have limited control over the means used, they may be considered as 'processors' rather than 'controllers'.[109]

---

[103] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 3. See also https://www.facebook.com/about/privacy/your-info-on-other (last accessed 27 January 2014).

[104] *Id.*

[105] *Id.* See also https://developers.facebook.com/docs/facebook-login/permissions (last accessed 27 January 2014).

[106] *Id.*

[107] See also W. De Groef, D. Devries, T. Reynaert and F. Piessens, 'Security and Privacy of Online Social Network Applications', l.c., p. 212-213. For example, 'OpenSocial' currently supports only one specific permission: allow or deny the application to access all of the user's data. However, implementers can always enhance this model in their own implementations. (*Id.*)

[108] See also Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', WP202, 27 February 2013, p. 12available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (last accessed 28 January 2014).

[109] For a more detailed discussion of the distinction between controllers and processors see Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169, 16 February 2010. See also B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46', *l.c.*, p. 30-33.

For example, a third-party tracker will in principle be considered a 'controller' for its collection and analysis of data related to the web browsing behavior of OSN users. However, it will only be considered a controller as long as it determines its own purposes and means of the processing. As indicated earlier, trackers often work on behalf of an ad network.[110] If a tracker is working on behalf of an ad network, and only processes personal data in accordance with the instructions issued by the ad network provider, the tracker will be considered a 'processor' rather than a controller. Another scenario in which a tracker might be considered a 'processor' is the scenario in which the tracker processes data on behalf of the OSN provider (e.g., if the OSN provider hires a tracker to learn more about how its users navigate the OSN).[111]

Data brokers generally act as controllers in their own right. They determine their own purposes when collecting data about individuals (e.g., collect data for purposes of profiling or predictive scoring). They also decide autonomously about how to organize this collection (e.g., which sources to consult, which technical methods to employ). While the product developed by a data broker will (eventually) be consumed by a third party, the data broker will have typically concluded its product development long before it is offered to clients.[112]

Other 'observers' of OSN data in principle also collect these data for their own purposes. For example, an employer who accesses the profile of a job applicant is likely to do so in order to assess the fitness of the candidate. Similarly, the intelligence agency mining OSN data in order to detect a potential threat to national security is likewise pursuing its own (statutory) objectives. In certain instances, observers may rely on the assistance of other entities to help achieve its objectives (e.g., a school may hire a private firm to monitor social network usage of its students). In these cases, the extent to which the service provider will be considered a 'processor' or a '(co-)controller' will depend largely on (1) how the service provider has defined the purpose(s) of its services up front and (2) the extent to which the service provider acts in accordance with the instructions issued by its customers.[113]

---

[110] Cf. *supra*; section 2.4

[111] See also Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', *l.c.*, p. 13 (indicating that a third party provides analytics services for an application owner, without processing the data for its own purposes or sharing it across developers, it is likely to be acting as a processor).

[112] The third party using the brokers service will typically also be a controller in its own right, separately from the data broker.

[113] See also B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46', *l.c.*, p. 36-37

3.2 E-Privacy

The second legal instrument relevant to OSNs is Directive 2002/58/EC, commonly referred to as the 'E-Privacy Directive'.[114] The E-Privacy Directive compliments the general rules of data protection provided by Directive 95/46/EC with specific rules for the processing of personal data in the context of electronic communications.[115] In addition, the E-Privacy Directive also contains several rules of general applicability, e.g. with regard to the use of location data or the storage of information on the devices of end-users.

a. Scope

According to article 3, the 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 EU, including public communications networks supporting data collection and identification devices*'.

The provisions of the E-Privacy are therefore in principle aimed at the providers of (publicly available) electronic communications services. However, several provisions have been drafted in such a way that their scope is not limited to such providers, but may also apply to other actors.[116] Over the following subsections, we will briefly elaborate upon those provisions which are of particular relevance in the context of OSNs.

b. Electronic communications services

The E-privacy Directive does not contain a formal definition of an 'electronic communications service'. This term is defined by Directive 2002/21/EC (the Framework Directive'), which defines an electronic communications service as

'*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including*

[114] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L201, pp. 37-47 (31 July 2002). This Directive was amended in 2009 by the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, (OJ L 337, 18.12.2009).

[115] See recitals (10) et seq.

[116] E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, Doctoral Thesis, K.U.Leuven, Facutly of Law, 1 June 2011, p. 304.

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 […] which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'.[117]

The concept of an 'electronic communication service' is intended to be technology-neutral.[118] It includes traditional telecommunications services such as fixed and mobile telephony, but also includes internet access services, such as (public) Wi-Fi hotspots.[119]

When considering the actors identified in section 2, it would appear as if the E-Privacy Directive is mainly relevant for 'infrastructure service providers'. Services offered by other entities, such as those offered by application providers or OSN providers, will generally not be considered as 'electronic communications services'.[120] While many of these services involve some form of electronic communication, they often do not consist 'wholly or mainly' in the conveyance of signals on an electronic communications network.[121] As a result, they shall in principle not be considered as providers of an 'electronic communications service'. There is, however, one notable exception to this rule, namely for the offering of electronic mail services.

Most OSN providers offer an e-mail service. According to the Article 29 Working Party, these electronic mail services may be considered as 'electronic communications services' within the meaning of Directive 2002/58/EC.[122] The Article 29 Working Party has therefore held that OSN providers who offer a publicly accessible email service will be

---

[117] Article 2(c) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ('Framework Directive'), O.J. L-108, 24 April 2002, p. 33 (emphasis added).

[118] E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, *o.c.*, p. 218-219.

[119] For more information on the concept of an 'electronic communications service' see also Article 29 Working Party, 'Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection', WP 37, 21 November 2000, p. 26, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf and E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, *o.c.*, p. 217 et seq.

[120] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 10.

[121] For a lucid explanation of the distinction between 'electronic communications services' and communications services which otherwise make use of electronic communications networks (such as certain VoIP services) see: Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH), 'Guidelines for VoIP Service Providers - Consultation Document', April 2005, p. 5, available at https://www.rtr.at/de/komp/KonsultationVoIP2005/VoIP_Guidelines_2005_Cons.pdf (last accessed 30 January 2014). See also D. Stevens, P. Valcke and E. Lievens, '"Voice over IP": law challenged by technology', *16th European Regional Conference, International Telecommunications Society*, September 2005; http://userpage.fu-berlin.de/~jmueller/its/conf/porto05/pages/papers.htm (last accessed 30 January 2014).

[122] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 10.

subject to the provisions of the E-Privacy Directive with regards to this specific service (but not for their other services).[123]

c. Confidentiality of communications and devices

One of the objectives of the E-Privacy Directive is to ensure confidentiality of communications. Article 5 provides that the interception or surveillance of electronic communications shall be prohibited, unless (a) the users concerned have consented or (b) there exists an explicit legal authorization (article 5(1)).[124] Article 5 also aims to protect the confidentiality of the 'terminal equipment' of end-users.[125] To this end, article 5(3) provides that

> '*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.*'

The scope of article 5 is not limited to the providers of electronic communications services or public communications networks. It contains rules of general application, which restricts (a) any interception or surveillance of electronic communications (article 5(1)), as well as (b) any storage of (or subsequent access to) information on the terminal equipment of end-users (article 5(3)).

Article 5(3) is sometimes referred to as the "*cookie rule*". The current version of this provision entails that individuals must in principle provide prior consent before the placement of (or subsequent access to) cookies on their computer.[126] There are two (narrow) exceptions to this rule, namely where the storage or access is (a) carried out for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (b) is strictly necessary in order for the provider of an

---

[123] *Id.*

[124] This legal authorization must have been adopted in accordance with article 15(1). Article 15(1) refers to legislative measures necessary to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.

[125] The terminal equipment of an end-user is essentially any equipment used to receive an electronic communications service (e.g., computer, phone, tablet).

[126] The previous version of this provision was slightly less stringent, stating that the use of cookies was only allowed when the user was informed about it, in a clear and comprehensive way, in accordance with the 95/46/EC Directive, and was offered the right to object to such processing by the data controller. (E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, *o.c.*, p. 239 et seq.) See also Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising', *l.c.*, p. 13.

information society service explicitly requested by the subscriber or user to provide the service.[127]

Although article 5(3) appears to have been aimed primarily at the use of cookies, this provision applies to any storage of (or subsequent access to) information on the terminal equipment of end-users. As a result, this provision also applies to applications which run on mobile devices, as well as any other application which gains access to data contained on an end-user's device.[128] The rules of article 5(3) of the E-Privacy Directive shall therefore be relevant to most OSN providers, website operators, application providers and trackers.

d. Use of location data

Location-based services are services whose main functionality depends on the processing of location data.[129] Location data are defined by article 2(c) of the E-Privacy Directive defined as

> '*any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*'.

In digital mobile networks, location data are often processed to enable the transmission of communications. However, such data may also be useful in providing additional functionalities, such as location-based direct marketing. They may also enable interesting applications in the context of OSNs (e.g., a friend proximity service, sharing of location tracked through GPS).

The E-Privacy Directive in principle only regulates location-based services offered by the providers of electronic communications services or public communications networks.[130] According to the Article 29 Working Party, it does not regulate the use of location data by other service providers (so-called 'information society service providers')[131], such as OSN providers or application providers. However, as location data

---

[127] The former exception can be seen as authorizing the use of mere "session cookies". The latter exception concerns storage or access which is strictly necessary to provide a service that has been explicitly requested by the individual concerned. (E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, *o.c.*, p. 251).

[128] See Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', l.c., p. 7 (stating that article 5(3) of the E-Privacy Directive applies to '*every entity that places or reads information from smart devices*').

[129] See E. Kosta, *o.c.*, 264.

[130] See also Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices', WP185, 16 May 2011, p. 8-9, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf (last access 31 January 2014).

[131] *Id.* The term 'information society service provider' is not defined by Directive 2000/58, but rather by article 1(2) of Directive 98/34/EC as 'any service normally provided for remuneration, at a distance, by

are generally also considered 'personal data' within the meaning of Directive 95/46/EC, these entities will still be bound by the requirements contained in the latter instrument when offering location-based services.[132]

electronic means and at the individual request of a recipient of services'". Information society services excluded from the scope of the E-Privacy Directive by virtue of article, unless their service consists wholly or mainly in the conveyance of electronic signals over public communications networks.

[132] *Ibid*, p. 9.

4. Rights and obligations

In the previous section, we analyzed the legal position of OSN providers, OSN users and application providers under both Directive 95/46/EC and Directive 2002/58/EC. The purpose of this section is to detail the main rights and obligations of these entities in light of their respective roles. Rather than providing an exhaustive account of every requirement or restriction, we will limit ourselves to a discussion of the most pertinent rights and obligations of each entity.

4.1 OSN provider

a. Duty to inform

As controllers, OSN providers are obliged to provide individuals with certain information regarding the processing of their personal data (articles 10-11).[133] As a rule, each data subject must be informed of at least (1) the *identity of the controller* (and, if applicable, of his representative) and (2) the *purposes* of the processing.[134] In addition, controllers may be required to provide the data subject with supplemental information 'in so far as such further information is necessary, *having regard to the specific circumstances in which the data are collected*, to guarantee *fair processing* in respect of the data subject'.[135] Such additional information can refer to (1) the categories of data concerned, the recipients or categories of recipients of the data, information with regard to the existence of the right of access, the right to rectify inaccurate data, etc.[136] According to Article 29 Working party, an OSN provider should at a minimum (also) inform its users about[137]:

---

[133] At the outset, these provisions make a distinction between two scenarios: one in which the information is obtained directly from the data subject (art. 10), and one in which the information is collected indirectly (i.e. from an entity other than the data subject) (art. 11). The notice obligations of the controller in each scenario are largely similar; the main differences concern (a) the moment by which notice must be provided and (b) the exemptions to the notice obligation.

[134] The use of plural "purposes", in Articles 10-11, implies that the data subject has to be informed not only about the main purpose to be accomplished, but also about any secondary purposes for which the data will be used. See also D. Korff, 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Country Study A.4 – Germany' (2010), p. 33, available online at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf (last accessed on 23 March 2011), commenting on the relevant provision of the German Data Protection Act, which uses the term "purposes" as well.

[135] Art. 10-11, 1(c) (emphasis added).

[136] Member State laws vary considerably with regard to the kinds of information which must actually be provided in order to ensure fairness of processing. Sometimes the examples given in the are repeated, other times somewhat different examples are included, and sometimes there are no examples at all. (see Article 29 Data Protection Working Party, 'Opinion on More Harmonised Information Provisions', WP100, 25 November 2004, p. 3, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf (last accessed 30 June 2012).

[137] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 7.

- the usage of their data for *advertising purposes* (e.g., the use of profile information for purposes of targeting advertisements);
- any sharing of their data with *third parties* (e.g., third-party application providers);
- any *profiling* to which the users might be subject, including an identification of the main data sources (e.g., personal details submitted during registration, cookies, purchase records); and
- any usage of any *sensitive data*.

The Working Party also recommends that OSN providers:

- provide users with adequate *warnings about the privacy risks* related to themselves and to others when they upload information to the OSN;
- remind users that uploading *information about other individuals* might impinge upon their privacy and data protection rights; and
- advise users that they should in principle only upload pictures or information about others with the *consent of the individuals concerned*.[138]

OSN providers processing *location data* of its users are obliged to mention this explicitly.[139] They must also inform their users of any *cookies* that they place which are not strictly necessary to provide the service.[140] Finally, as publishers of third-party advertisements, OSNs must ensure that their users are informed of the fact that use of their services may result in *monitoring by trackers*, in particular by ad network providers or other ad serving entities (who might place a third-party cookie when serving an add).[141]

In principle, the OSN provider may provide the necessary information via a so-called 'privacy notice', provided that the information contained in this notice is sufficiently comprehensive and presented in an understandable way.[142] However, for certain types of information or actions, it may be recommended to present information (again) at the moment of a specific action. For example, an OSN provider can help increase audience awareness by showing its users (a subset of) the people who will have access to the content which the user is planning to share.[143]

---

[138] *Id.* See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 106-107.

[139] Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices', WP185, 16 May 2011, *l.c.*, p. 13-14.

[140] Article 5(3) of the E-Privacy Directive.

[141] For more information see Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioral advertising', *l.c.*, p. 17-19 and 24. See also *supra*; section 2.4.

[142] See also P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 545. For more information regarding the role of privacy notices, as well as a number of practical guidelines for the implementation of such notices, we refer the reader to SPION D6.1 ('Legal requirements for privacy-friendly model privacy policies') and D9.3.5 ('Privacy-friendly 'model' privacy policies'), available at www.spion.me.

[143] See e.g. Y. Wang, P.G. Leon, K. Scott, X. Chenz, A. Acquisti, L.F. Cranor, 'Privacy Nudges for Social Media:

b. Legitimacy of processing

Under Directive 95/46/EC, processing of personal data may only take place to the extent that there is a 'legitimate ground' justifying the processing. The legitimate grounds recognized by the Directive are enumerated (exhaustively) in article 7. Of these grounds, there are three grounds in particular which the provider of an OSN might invoke, namely:

- the unambiguous consent by the data subject (art. 7(a));
- a necessity for the performance of a contract (art. 7(b)); and
- an (overriding) legitimate interest (art. 7(f)).

For processing that is strictly necessary to provide the OSN service (e.g., initial creation of profile, offering of basic functionalities), the provider can in principle rely on the ground of 'necessity for the performance of a contract'.[144] For a limited number of operations, the provider may also be able to rely on the 'legitimate interest' ground (e.g., processing for purposes of ensuring system security).[145] For all other processing operations, such as the use of users' personal data for targeting purposes, the provider will in principle have to obtain the 'unambiguous consent' of its users.[146]

There are situations in which data subject consent is mandated by law, even though the controller might theoretically be able to invoke another ground to legitimate the processing. For instance, article 5(3) of the E-Privacy Directive entails that the provider of an Online Social Network must obtain the consent of its users prior to:

- the *installation of any software* on the device of an end-user (e.g., when offering a mobile application for the OSN);
- any *placement of cookies* which are not strictly necessary to provide service (e.g., to monitor web-browsing activities outside the OSN).[147]

As far as the use of OSN data for purposes of *targeted advertising* is concerned, the situation is somewhat less clear-cut. Directive 95/46/EC does not formally require that individuals express their consent before their data is used for purposes of direct marketing or targeted advertising.[148] As a result, one might argue that the use of profile information of

---

An Exploratory Facebook Study', PSOSM 2013, available at http://precog.iiitd.edu.in/events/psosm2013/9psosm6-wang.pdf (last accessed 1 February 2013).

[144] P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 542.

[145] *Id.*

[146] For a more detailed analysis on the role of consent as a basis for legitimating the processing of personal data see section 2.2 of SPION deliverable D6.1 ('Legal requirements for privacy-friendly model privacy policies') and D9.3.5 ('Privacy-friendly 'model' privacy policies'), available at www.spion.me.

[147] Cf. *supra*; section 3.2.c.

[148] In principle, it is sufficient that individuals are given a right to object in accordance with article 14(b). (See also E. Kosta, *o.c.*, p. 164 et seq.) Directive 2002/58/EC does require prior consent of individuals when certain data or techniques are used for purposes of 'direct marketing'. Specifically, explicit prior consent shall be necessary where the marketing activity involves either (1) use of cookies (article 5(3)); or (2) the use of 'automated calling and communication systems without human intervention', 'facsimile machines' or

OSN users (e.g., name, age, location, etc.) for purposes of targeted advertising does not necessitate consent. However, even in absence of a legal provision mandating consent, a normal reading of article 7 of Directive 95/46/EC *de facto* also requires users' consent in order to legitimate these types of processing activities. The same arguably applies for any processing of data intending to locate the *geographic position* of the end-user, regardless of whether it involves any storage of information on the device of the end-user.[149]

c. Privacy settings

Every controller is under a duty to ensure the security and confidentiality of its personal data processing (articles 16-17 Directive 95/46/EC). Specifically, every controller is obliged to

> '*implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*'[150]

Applying notions of security and confidentiality in the context of OSNs may seem counter-intuitive at first. After all, OSNs are about sharing data rather than about keeping secrets. Nevertheless, OSN providers are obliged take reasonable steps to prevent '*unauthorized access*' as well as '*any other forms of unlawful processing*'.

In practice, accessibility of an OSN profile is determined, to greater or lesser extent, by the 'privacy settings' associated with that profile.[151] These settings enable individuals to exercise a certain degree of control as to who may access their OSN data. Many users wish to limit their disclosure of personal information to people they know, or perhaps even to a subset of their contacts. Other users may want to share information with the public at large. This raises the issue of what the *default* settings should be on OSNs. According to the Article 29 Working Party, the OSN provider should offer default settings

> '*which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties*'.[152]

---

electronic mail (article 13(1)). Use of 'pop-up windows' or 'banners' on the side of a webpage arguably does not (in and of itself) bring an advertising activity within the remit of article 13(1). (See also E. Kosta, *o.c.*, p. 299-300.) However, where the advertisements are targeted to individual users by means of data collected via cookies, article 5(3) of the Privacy Directive takes full effect.

[149] See also Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices', WP185, 16 May 2011, l.c. p. 14)

[150] Article 17(1) Directive 95/46/EC (emphasis added).

[151] For a comprehensive discussion of privacy settings see J. Ausloos, 'Guidelines for privacy-friendly default settings', SPION D6.4, 2012, available at www.spion.me.

[152] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 7.

In other words, access to the profile information of OSN users should be restricted to self-selected contacts (e.g., 'friends', 'network members') by default. OSN users should be asked for permission before access is extended to any other entity.[153] For example, information contained in a user's profile should not be made available for indexation by (internal or external) search engines unless the user has explicitly agreed to this.[154] By restricting access to self-selected contacts by default, OSN providers may also solidify the legitimacy and fairness of their processing activities (as users need to take affirmative action before these data are made available to other third parties).[155]

d. Data accuracy

Article 6(1)d of Directive 95/46/EC provides that 'all personal data should be accurate and, where necessary, kept up to date'. In first instance, this provision requires controllers to put in place mechanisms and procedures that enable them to establish an appropriate level of accuracy. As is the case for the other controller obligations, the precise scope of this duty must be interpreted within reason. For example, the standard of care for ensuring data accuracy will be higher in a medical setting than in the context of OSNs.[156] While this seems straightforward as a matter of principle, it still leaves open the following question: which measures are providers of OSNs obliged to adopt in order promote accuracy of data uploaded by their users?

In this regard, it is worth taking note of recent guidance issued by the UK Information Commissioner's Office (ICO):

> '*[In] a situation where the vast majority of the site content is posted directly by third parties, the volume of third party posts is significant, site content is not moderated in advance and the site relies upon users complying with user policies and reporting problems to the site operator, we would not consider that taking 'reasonable steps' requires the operator to check every individual post for accuracy*.'[157]

---

[153] This includes access to personal data by application providers, including when this application has not been downloaded by the OSN user herself, but rather by one of her contacts.

[154] Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', *l.c.*, p. 7.

[155] See also SPION 6.4, p. 30 et seq. Similar reasoning regarding the controller's duty to ensure the confidentiality and security of processing can also be found in the opinions of the Article 29 Working Party regarding applications for smart devices and location-based services. See in particular Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', *l.c.*, p. 11 and 15 and Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices', *l.c.*, p. 13-14.

[156] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, 'Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?', ICRI Working Paper 15/2013, September 2013, p. 36, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494.

[157] Information Commissioner's Office (ICO), 'Social networking and online forums – when does the DPA apply?', *l.c.*, paragraph 37 (emphasis added). The ICO did indicate that it might hold otherwise in situations where data controller plays a more active role in selecting, allowing or otherwise moderating content. (*Ibid*, paragraphs 35-36)

In these situations, the ICO continued, it would be sufficient for the OSN provider to

- have a *clear and prominent policy* for its users about acceptable and non-acceptable posts;
- have clear and easy to find *procedures* in place for data subjects to dispute the accuracy of posts and ask for them to be removed; and
- *respond to disputes* about accuracy quickly, and have procedures to remove (or suspend access to) content, at least until such time as the dispute has been settled.[158]

e. Access by third-party apps

OSN providers play a central role in mediating access to the personal data of OSN users. In addition to controlling access by fellow OSN users, they also control access by third-party applications. As explained earlier, many OSNs currently enable access to OSN data by means of an Application Programming Interface (API).[159]

Third-party application providers are in principle 'separate' controllers: they determine their own purposes and means for their processing of personal data. Once access has been granted, an application provider will typically collect the data and export them to its own servers for further processing.[160] As a result, application providers are subject to their own data protection obligations, which exist independently of those incumbent on the OSN provider. The OSN provider, however, still acts as a controller in relation to its own processing activities, including any disclosure to third parties. This means that the OSN provider is obligated to take reasonable steps to ensure that these data are not disclosed to unauthorized entities.[161]

An interesting question to consider is whether OSN providers are under a duty to ensure that data is only being shared with 'reliable' entities.[162] OSNs generally tend to dissociate themselves from application providers, who they consider as 'third parties'.[163] They typically disclaim any and all responsibility for actions undertaken by these third parties.[164] Nevertheless, one could argue that OSN providers have a basic duty of care to

---

[158] *Ibid*, paragraph 38.
[159] Cf. *supra*; section 2.3.
[160] These servers are outside of the OSN domain, meaning they are beyond the OSN provider's direct control or supervision. (M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 2.)
[161] Cf. *supra*; section 4.1.c.
[162] F. Le Borgne-Bachschmidt et al., 'User-Created-Content: Supporting a participative Information Society', *l.c.*, p. 243-244.
[163] P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. p. 541.
[164] See also F. Le Borgne-Bachschmidt et al., 'User-Created-Content: Supporting a participative Information Society', *l.c.*, p. 243-244 and E. Denham (Assistant Privacy Commissioner of Canada), 'Report of Findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.

establish that the recipients of the data under their control are in fact trustworthy (i.e. likely to process it in a lawful manner).[165] Opponents will argue that this interpretation is excessive, and that it is sufficient for the OSN provider to assume responsibility for its own operations (i.e., the boundaries of its control establish the boundaries of its obligations).

In practice, OSN providers require application providers to stipulate which permissions they need. When an OSN user wants to make use of (or download) a particular application, he or she will be notified of which permissions are being requested by the application provider.[166] Even under a narrow construction of the OSN provider's responsibilities, the OSN provider is still obliged to

- provide for a *level of granularity* that enables selective access and disclosure of personal data related to OSN users[167];
- ensure that application providers do not obtain access to more data than has been *authorized* by users; and to
- take reasonable measures to ensure that *meaningful consent* is obtained from their users[168]; and
- deploy appropriate measures to detect *apparent misuse* by application providers (e.g., complaint handling mechanisms, use of basic malware detection tools)[169].

Finally, it is worth noting that the duties of OSN providers in relation to third party apps may also depend on how these apps are presented to users. In 2008, Facebook introduced a "verified apps" program, to which application developers could apply on a

---

under the Personal Information Protection and Electronic Documents Act, 2009, paragraphs 166 et seq. available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf

[165] F. Le Borgne-Bachschmidt et al., 'User-Created-Content: Supporting a participative Information Society', *l.c.*, p. 244 . These authors argue that such an obligation can be derived from article 6(1) of Directive 95/46, which requires that personal data must be processed 'fairly and lawfully'. They draw further support for this proposition through a comparison with article 17(2) of the Directive, which provides for a duty of care when choosing a processor who will process personal data on behalf of a controller (Id.) An alternative way of phrasing this argument would be to say that the OSN provider acts as a 'custodian' (or 'steward') of data entrusted by its users, who as a result has a certain duty of care before releasing data to third parties.

[166] Cf. *supra*; section; 2.3.

[167] Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', *l.c.*, p. 8-9. See also Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', l.c., p. 11. Here the reasoning is essentially that OSN providers have a duty to ensure that application providers have at least the ability to comply with provisions of Directive (in other words, to prevent 'unlawful forms of processing'). Granular access capabilities are considered necessary so that apps are capable of collecting no more information than is necessary to realize the purposes of their processing in accordance with article 6, 1(c).

[168] See also E. Denham, 'Report of Findings - CIPPIC v. Facebook Inc.', *l.c.*, p. 3 and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *l.c.*, p. 137. For example, the OSN provider could require its application providers to use a standardized privacy notice. The OSN provider can also do its own part by ensuring that the requested permissions and (references to) privacy notices are displayed in a prominent way.

[169] These issues were also investigated by the Irish Data Protection authority in its 2011 audit of Facebook: see Data Protection Commissioner, 'Report of Audit – Facebook Ireland Ltd.', *l.c.*, p. 87-97. See also Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', *l.c.*, p. 20-21.

voluntary basis. If approved, the application would receive a "Facebook-verified badge" as well as increased distribution.[170] Facebook also implied that verified applications were 'secure, respectful and transparent'.[171] In 2012, the US Federal Trade Commission issued a complaint alleging that Facebook in fact did not take any steps to verify the security practices of a Verified Application provider ('beyond such steps as it may have taken regarding any other application').[172] This complaint eventually resulted in a decision which ordered that Facebook refrain from misrepresenting 'the steps it takes or has taken to verify the privacy or security protections that any third party provides'.[173]

f. Data subject rights

In addition to imposing obligations upon controllers, Directive 95/46 also provides data subjects with certain rights. Specifically, each individual whose personal data are being processed have a right to

a) obtain certain information with regards to the processing of his or her personal data (*right of access*) (article 12(a));
b) object to the processing of their personal data, save where otherwise provided by national legislation (*right to object*) (article 14); and
c) obtain, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, (*right to rectification, erasure or blocking*) (article 12(b)).

As a controller, the provider of an OSN must accommodate the exercise of data subject rights. In principle, this duty extends to any personal data it has collected. As indicated earlier, however, many data shared on OSNs are not actively solicited by the OSN provider, but instead shared spontaneously by its users. An interesting question to consider therefore is whether OSN providers are also obliged to accommodate the exercise of data subject rights in relation to such content. We shall return to this question later on in this deliverable (cf. *infra*; section 4.3.b).

---

[170] E. Denham, 'Report of Findings - CIPPIC v. Facebook Inc.', *l.c.*, p. 43.
[171] United States Federal Trade Commission (FTC), *In the matter of Facebook Inc. - Complaint*, Docket No. C-4365, 2012, p. 15, available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (last accessed 4 February 2014).
[172] *Id.*
[173] United States Federal Trade Commission (FTC), *In the matter of Facebook Inc. – Decision and Order*, Docket No. C-4365, 2012, p. 4, available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (last accessed 4 February 2014).

4.2 Application providers (and other entities)

There is considerable similarity among the obligations incumbent upon OSN providers and those incumbent upon application providers. In principle, the latter will be considered controllers in their own right (cf. *supra*), which implies that they are essentially subject to the same obligations as OSN providers. As a result, application providers are obliged to ensure:

a) transparency of processing;
b) legitimacy of processing;
c) respect for data quality principles (e.g. accuracy, proportionality, finality);
d) confidentiality and security of processing; and
e) accommodation of data subject rights.

a. Duty to inform

Application providers are obliged to provide their users with information specified in articles 10-11 of the Data Protection Directive. Prior to offering its service, the application provider must specify:

- its identity and contact information;
- the precise categories of personal data (OSN and other) it will collect;
- for which specific purposes;
- how users may exercise their rights.[174]

This information should be displayed prominently prior to usage of the application and remain easily accessible afterwards.[175]

b. Legitimacy

Similar to OSN providers, there are essentially three grounds available to application providers to legitimate their processing of personal data, namely:

- the unambiguous consent by the data subject (art. 7(a));
- a necessity for the performance of a contract (art. 7(b)); and
- an (overriding) legitimate interest (art. 7(f)).[176]

Unambiguous consent of the user shall in principle be necessary for

[174] See also Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', *l.c.*, p. 22. For applications installed on smart devices, the Working Party has also recommended that users be informed of the retention periods of their data as well as security measures applied by the controller (*Ibid*, p. 23).
[175] *Id.*
[176] See also p543 Van Eecke Truyens and Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', *l.c.*, p. 14-16.

- the installation of any software on the device of an end-user (e.g., when offering a mobile application for the OSN);
- any placement of cookies which are not strictly necessary to provide service (e.g., to monitor web-browsing activities outside the application environment);
- any use of OSN or other personal data for purpose of targeted advertising; and
- any processing of data intending to locate the geographic position of the end-user.[177]

As explained earlier, obtaining the informed consent of OSN users shall in principle be a shared responsibility among application providers and OSN providers (at least where access to OSN data is concerned). The application provider must clearly articulate which permissions it requires and for which purposes, while the OSN provider will de facto be responsible for communicating this information to its users and obtaining their authorizations.

c. Data quality principles

As controllers, application providers are also obliged to respect the principles of data quality, which include inter alia the principle of purpose specification and data minimization (article 6). These principles require that no more data is collected than is necessary to achieve the purposes of the processing. In practice, many application providers request (access to) more data than are necessary to deliver the app's functionality. These data are then used for a variety of (other) purposes, e.g. to facilitate targeted advertising. In principle, application providers may collect and use such additional data on the condition that they provide their users with clear information and obtain their consent before doing so. However, the retention and use of such data should be limited in time, taking into account the need to ensure a fair balance between the business interests of application providers and the privacy interests of their users.

d. Confidentiality and security

Application providers are obliged to ensure the security and confidentiality of the personal data which they process (articles 16-17). In practice, many application providers will export (a subset of) the data they collect from OSN providers to their own servers for further processing.[178] In its Opinion on apps for smart devices, the Article 29 Working Party highlighted a number of security considerations for app developers, including:

- measures to protect data both in transit and at rest;

[177] Cf. *supra*; section 4.1.b.

[178] These servers are outside of the OSN domain, meaning they are beyond the OSN provider's direct control or supervision. (M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, 'AppInspect – Large-scale Evaluation of Social Apps', *l.c.*, p. 2.)

- measures to prevent 'buffer overflow' or 'injection' attacks;
- use of low entropy app-specific or temporary device identifiers;
- use of secure identification and authentication mechanisms.[179]

e. Data subject rights

App users must be given the ability to exercise their rights as data subjects provided by articles 12 and 14. Application providers should inform their users about how they can exercise these rights, preferably by means of a secure online access tool.[180] Application users should also be provided the ability to withdraw their consent at any time.[181] Given their role in facilitating access to OSN data, OSN providers may also be expected to offer tools which allow OSN users to discontinue access to their profile data (unless such access is already limited by default, e.g., to moments at which the application is being used by the OSN users).

4.3 OSN Users

a. As 'controllers'

In section 2, we analyzed the extent to which a user of an OSN may be considered as a 'controller' within the meaning of article 2(d). There we concluded that every OSN user, at least in theory, acts as a 'controller' when processing data related to other individuals. This implies that OSN users shall in principle be subject to the same requirements and obligations as other controllers, unless they can avail themselves from one of the exemptions recognized by Directive 95/46/EC.

In its Opinion on social networking, the Working Party considered that the processing activities of private OSN users will generally be covered by the personal use exemption.[182] Since then, several commentators have contested this view; arguing that in practice there are many situations in which the exemption is inapplicable.[183] First, it appears to be common ground that the exemption does not apply in situations where data

[179] Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices', *l.c.*, p. 18-20.
[180] *Ibid*, p. 24.
[181] *Ibid*, p. 25.
[182] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 5.
[183] See e.g. P. Van Eecke and M. Truyens, 'Privacy and Social Networks', l.c., p. 540; N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 101 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *l.c.*, p. 147 et seq. Even before Opinion 5/2009, several authors considered it likely that a substantial number of OSN users might not be able to benefit from the personal use exemption. See e.g. R. Wong, 'Social Networking: Anybody is a Data Controller!', (last revised) 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668 and B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 75.

are made accessible to 'an indefinite number of people'.[184] As a result, OSN users with 'public' profiles will almost certainly fall outside the scope of article 3(2). Even if a profile is set to 'private', however, it is quite possible that the information is still *de facto* accessible to an 'indefinite' number of people (e.g., due to access by 'friends-of-friends').[185] Second, a substantial share of individuals does not only (or not exclusively) use OSNs for personal purposes, but also for professional networking or for political, commercial or charitable ends.[186] Given that the exemption of article 3(2) only applies to 'purely' personal or household activities, those users would find themselves outside its protective remit.

In cases where the personal use exemption cannot be applied, the OSN user in question shall in principle be subject to the same requirements as those incumbent upon controllers in any other context.[187] This outcome is warranted where organizations are concerned, who make use of OSNs to realize their commercial, political or other objectives. This outcome is more problematic, however, where private individuals are concerned. If an OSN user is subject to data protection law, it implies, inter alia, that this OSN user is required to ensure:

- the legitimacy of processing (e.g., by asking for consent before posting data relating to others);
- transparency of processing (e.g., by notifying the individuals concerned of the fact that information about them is now included on an OSN profile);
- respect for the data quality principles such as fairness, proportionality, finality and accuracy (e.g., by refraining from posting erroneous statements);

---

[184] Cf. *supra*; section 3.1.c.

[185] Previous research has indicated that many users set a relatively low threshold for deciding whether to accept someone as a 'friend' (See e.g. R. Gross and A. Acquisti, 'Information Revelation and Privacy in Online Social Networks', in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (WPES'05), Virginia, 2005. p. 73 and D. Boyd, 'Friendster and Publicly Articulated Social Networks', in *Conference on Human Factors and Computing Systems* (CHI 2004), Vienna, ACM, April 24–29, 2004, p. 1280. Contra: R. Goettke and J. Christiana, 'Privacy and Online Social Networking Websites', Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, May 14, 2007. http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf). Given that many profiles are accessible also to 'friends of friends', even a profile with a relatively low number contacts may in practice have an extremely large audience. According to a recent study by the Pew Research Institute, the *median* Facebook user can reach *31,170* people through their '*friends-of-friends*'. (K. N. Hampton, L.S. Goulet, C. Marlow and L. Rainie, 'Why Facebook users get more than they give', *Pew Research Center's Internet & American Life Project*, 2012, p. 5, available at http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Facebook%20users_2.3.12.pdf). See also M. Isaac, 'On Facebook, There's No Privacy Setting for Your Friends' Bad Judgment', *All things D*, 26 December 2012, available at http://allthingsd.com/20121226/on-facebook-theres-no-privacy-setting-for-your-friends-bad-judgment/ (last accessed 10 February). Finally, regarding the "blurry-edged" nature of social networks see also L. Gelman, 'Privacy, Free Speech, and "Blurry-Edged" Social Networks', *Boston College Law Review* 2009, vol. 50, in particular at p. 1326 et seq.

[186] N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 103.

[187] Cf. supra; section 3.1.c.

- that data subjects have the ability to exercise his rights towards the processing (i.e. right of access, rectification, erasure or blocking);
- the confidentiality and security of processing (e.g., by restricting access to individuals from the same community);
- that, where required, notification to national supervisory authorities is performed.

At first glance, it seems as if a number of these requirements could be applied to private individuals in a reasonable way. For example, many of us would agree that 'friends' should refrain from uploading pictures of one and other before checking whether it's ok.[188] Or that they shouldn't post inaccurate or harmful statements about others, regardless of whether or not their profile is set to 'private'. For other data protection requirements, however, there appears to be a clear mismatch between legal provisions and OSN practices. For example, how does one interpret the requirement of not keeping personal data in identifiable form for longer than is necessary (art. 6(1)e) in relation to OSN users? Is it possible to determine a reasonable time-span as to how long a user should be allowed to maintain a picture or remark relating to another person on his profile page? Should we be requiring individuals to make such a determination? Another problematic provision is the controller's duty to inform.[189] Should OSN users be required to formally notify their peers of (1) their identities; (2) the purposes of the processing of their personal data as well as (3) the (categories of) recipients concerned? Or is it sufficient if these things are understood implicitly, as a result of prevailing social norms and common OSN practices?

It is also worth noting that there are a number of controller obligations with which the OSN user cannot comply without co-operation of the OSN provider. Let us assume, for instance, that a data subject exercises his or her right to erasure towards a profile owner. Arguably, the latter would (more often than not) be under an obligation to remove this information immediately. However, what happens when the OSN provider retains these data for a longer period of time, in accordance with the terms and conditions of its service? As indicated earlier, individual OSN users have limited powers of negotiation in relation to the terms specified by the OSN provider.[190]

The mismatch between data protection requirements and OSN practices has led several authors to advocate for a pragmatic approach.[191] Rather than rigid adherence to the provisions of the Directive 95/46/EC, they argue, OSN providers and OSN users should

[188] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 104. Others may find it perfectly acceptable (and even enjoyable) to find themselves 'tagged' unexpectedly in a picture uploaded by a shared contact.
[189] See also D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *l.c.*, p. 132.
[190] *Id.*
[191] N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 105 et seq.

share the burdens of compliance in light of their respective roles. The implementation of this approach corresponds, by and large, to the recommendations issued by the Article 29 Working Party in its Opinion on online social networks (cf. *supra*). For example, the Working Party already recommended that OSN providers make users aware of the privacy risks involved in uploading information related to others, and that they should obtain their consent before doing so. The use of privacy-friendly default settings may similarly be viewed as an example of a technical measure that supports users when they exercise their responsibilities as controllers.[192] While this pragmatic approach seems reasonable (and perhaps even commendable) as a matter of practice, one also can't help but wonder whether the framework of Directive 95/46/EC is being stretched beyond its intended domain of application.

b. As 'data subjects'

Private individuals are generally thought of as 'data subjects' rather than 'controllers'.[193] Data subjects are the intended beneficiaries of data protection laws: it is their interests which these laws aim to protect by imposing requirements and limitations upon the processing of personal data. Directive 95/46/EC endows data subjects with certain rights, which they may invoke in case these requirements or limitations are not respected. For purposes of our current analysis, the most relevant rights are the data subject's right to erasure (art. 12) and the right to object (art. 14).

Article 12(b) stipulates that data subjects have the right to obtain, as appropriate, the '*rectification, erasure or blocking*' of data in case where the processing of which does not comply with the provisions of the Directive. Rectification shall be particularly appropriate in instances where the data being processed is found to be inaccurate. Deletion or blocking may be appropriate where data have been obtained unlawfully or there is no longer a legitimate need to maintain the data.[194]

Article 14(a) provides data subjects with a *right to object* to the processing of their personal data, save where otherwise provided by national legislation. It is important to note, however, that the data subject must in principle provide '*compelling legitimate grounds relating to his particular situation*' when exercising the right to object.[195] Where

---

[192] See N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 107.

[193] Opinion 5/2009, l.c., p. 5. A data subject, pursuant to article 2(a) of the Directive, is essentially any individual whose personal data are being processed, provided he or she is sufficiently identifiable.

[194] In instances where the data subject's request for amendment, deletion or blocking is granted, she may also request that controller provides notification thereof to any third parties to whom the data have been disclosed. The only grounds for the controller to refuse such a request would be to assert that such notification is impossible or involves a disproportionate effort (art. 12, c).

[195] When personal data is processed for direct marketing purposes, the subject does not have to motivate his/her request.

the objection is justified, the processing instigated by the controller may no longer involve those data.

Both the right to object and the right to erasure are intended to give individuals a certain amount of control over what happens to their data. In principle, these rights are to be exercised vis-à-vis the 'controller' of the processing. The previous sections have made clear that the OSN context involves a multitude of actors, who may each be in 'control' of different (aspects of different) processing operations. In principle, each entity is only responsible for those aspects under its own control, i.e. for which it determines the 'purposes and means' of the processing. An interesting question to consider is whether OSN providers are obliged to accommodate the exercise of data subject rights in relation to content shared spontaneously by its users.[196] For example, should an individual have a right to ask an OSN provider to take down a photograph posted by one of its users? While the initiative to share this content lies with the OSN user in question (who may therefore be considered as the 'primary' controller), most regulators seem to agree that OSN providers should put in place a mechanism to enable individuals to exercise their data subject rights directly towards the OSN provider.[197] For example, in its Opinion on online social networks, the Article 29 Working Party considered that

> "*Access and rectification rights of users are not limited to the users of the service but to any natural person whose data are processed. Members and non-members of SNS must have a means to exercise their right of access, correction and deletion. The homepage of SNS sites should clearly refer to the existence of a "complaint handling office" set up by the SNS provider to deal with data protection and privacy issues and complaints by both members and non-members*."[198]

Although it is not stated explicitly as such, the quoted text suggests that OSN providers have a duty to accommodate data subject rights in relation to *any* personal data they process. This would imply that individuals can also exercise their rights as data subjects in relation to content shared by OSN users, seeing as these data are also processed by the OSN provider. This interpretation is also in line with guidance issued by national

[196] See also supra; section 3.1.b.

[197] As indicated earlier, there a number of scholars who have argued that OSN providers (or the providers of similar services) should not be considered as 'controllers' in relation to the content shared via their platforms. As a result, these authors question the duty of these platform providers to accommodate data subject rights vis-à-vis user-generated content. Van Eecke and Truyens, for example, argue that an OSN provider should be considered as a mere processor in relation to content shared by users. In their view, only users should responsible for accommodating data subject rights. See P. Van Eecke and M. Truyens, 'Privacy and social networks', *l.c.*, p. 539 and p. 543.

[198] Article 29 Working Party, 'Opinion 5/2009 on online social networking', *l.c.*, p. 11 (emphasis added).

regulators, such as the Dutch Data Protection Authority[199] and the UK Information Commissioner's Office[200].[201]

While the guidance issued by the Working Party is most welcome, it refrains from offering any additional guidance as to how OSN providers should actually deal with these complaints. Should they remove any content upon request? Should they notify the OSN user from whom the content originated? Should the latter be able to contest the data subject's complaint? We will discuss the potential negative implications of the lack of clear guidance in this respect in a forthcoming deliverable (SPION D9.6.3).

5. Conclusion

Online social networks have come to involve a myriad of actors. While users and providers of OSNs remain the 'key players', several other entities have become involved as well. Many application providers, for instance, offer their services through OSN platforms. Third-party website operators may leverage the authentication services of an OSN or embed its social plug-ins. Other entities engaging with OSNs include third party trackers, data brokers and other observers.

The EU data protection framework was enacted before the emergence of OSNs. For the most part, scholars and regulators have been able to reconcile this framework with new social networking realities. But there are also instances in which this framework is beginning to show its limits. Two areas in particular require further consideration, namely (1) the role of OSN users as 'controllers' and (2) the exercise of data subject rights towards user-generated content.

OSN users actively process personal data about themselves and others. However, the mere fact that an individual may also 'control' certain processing activities is not necessarily a sufficient justification to subject him or her to the same regime as organizations. Further research is necessary to determine how the appropriate balance between private individuals should be achieved.

A second area of concern is the exercise of data subject rights in relation to user-generated content. EU regulators agree that OSN providers should put in place a 'complaint handling mechanism' which allows individuals to exercise their rights as data subjects. The consensus also seems to be that individuals should be able to, if necessary, exercise these rights in relation to content shared by users. Without appropriate safeguards, however, there is a risk of undue interference with OSN users' freedom of expression. How these risks can be mitigated will be discussed in future deliverable (SPION D9.6.4).

---

[199] College Bescherming Persoonsgegevens, 'Publicatie van Persoonsgegevens op het Internet', *l.c.*, p. 42.
[200] Information Commissioner's Office (ICO), 'Social networking and online forums – when does the DPA apply?', *l.c.*, p. 14.
[201] See also R. Wong, R. Wong, 'Social networking: a conceptual analysis of a data controller', *Communications Law* 2009, Vol. 14, No. 5, p. 148.