IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monograph "5th Internet, Law and Politics Congress. The Pros and Cons of Social Networks"

ARTICLE

Facebook and Risks of "De-contextualization" of Information

Franck Dumortier

Submitted: July 2009
Accepted: September 2009
Published: December 2009

Abstract

Participation in online social networking sites (OSNS) has increased dramatically in recent years. Services such as the well-known Facebook and Myspace but also Frienster, WAYN, Bebo, Google's Orkut and many others, have millions of registered active users and are continuously growing. The most common model for these sites is based on the presentation of the participants' profiles and the visualisation of their network of relations to others. OSNS also connect participants' profiles to their public identities, using real names and other real-world identification signs (pictures, videos, e-mail addresses, etc.) to enable interaction and communication between real-world subjects. Hence, a site like Facebook cannot be considered purely as a playground for "virtual bodies" in which identities are flexible and disconnected from "real-world bodies". Not only is the provision of accurate, current and complete registration information from the users encouraged, it is even required by Facebook's terms of use. This requirement, along with the service's mission of organizing the real social life of its members, provides major incentives for users to publish only real and valid information about themselves. This accurate information being provided, privacy threats derive from interactions on Facebook. In this paper, I argue that the main privacy risk on Facebook is the one of loss of context of the information spread by users. This de-contextualization threat is due to three major characteristics of Facebook: 1) the simplification of social relations, 2) the high level of information diffusion and 3) the network globalization and normalization effects of Facebook. This loss of context is a risk not only to data protection rights, meaning the right of the individual to control their informational identity presented in a certain context, more fundamentally it threatens the human right to privacy: the right to be a conscious, multiple and relational self not suffering any form of discrimination.

Keywords

privacy, data protection, online social networking, de-contextualization of information

Subject

Privacy and data protection

Facebook y los riesgos de la «descontextualización» de la información

Resumen

En los últimos años, ha aumentado drásticamente la participación en sitios de redes sociales virtuales (en lo sucesivo, OSNS). Servicios como los conocidísimos Facebook y Myspace, u otros como Frienster, WAYN, Bebo, Orkut de Google y muchos más cuentan con millones de usuarios registrados y no dejan de crecer. El modelo más común de estos sitios se basa en la presentación de los perfiles de los participantes y la visualización de su red de relaciones con los demás. Asimismo, las redes OSNS conectan los perfiles de los participantes con sus identidades públicas, usando nombres reales u otros símbolos de identificación del mundo real (como fotos, vídeos, direcciones de correo electrónico, etc.) a fin de permitir la interacción y comunicación entre individuos del mundo real. Por tanto, un sitio como Facebook no se puede considerar únicamente como un patio de recreo para «entes virtuales» en el que las identidades son flexibles y están desconectadas de sus «cuerpos reales». La disposición de información de registro completa, exacta y actualizada por parte de los usuarios no sólo es deseable, sino que es un requisito incluido en las condiciones de uso de Facebook. Este requisito, junto con la misión del servicio de organizar la vida social real de sus miembros, supone un incentivo importante para los usuarios, instándoles a publicar únicamente información real y válida sobre sí mismos. Una vez proporcionada esta información exacta, las interacciones en Facebook implican una amenaza para la privacidad. En este informe, argumento que el principal riesgo para la privacidad en Facebook es el de la descontextualización de la información que proporcionan los participantes. En mi opinión, esta amenaza de la descontextualización se debe a tres de las características principales de Facebook: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización en la red de Facebook. El fenómeno de descontextualización no sólo supone una amenaza para el derecho a la protección de datos, en el sentido del derecho a controlar la identidad informativa que un ser humano proyecta en un cierto contexto. De un modo más fundamental, es una amenaza al derecho a la privacidad como ser humano: el derecho del ser humano a ser un yo conscientemente múltiple y gregario sin una discriminación injustificada.

Palabras clave

privacidad, protección de datos, redes sociales virtuales, descontextualización de la información

Tema

Protección de datos y privacidad

Introduction

Participation in online social networking sites (OSNS) has grown continuously in recent years with the number of users multiplying at an exponential rate. For instance, while Facebook's international audience totalled 20 million users in April 2007, that number increased to 200 million two years later with an average of 250,000 new registrations per day since January 2007. The 'active' proportion of Facebook's audience is also impressive: according to statistics published on the website, more than 100 million users log on to Facebook at least once a day while more than 20 million users update their status at least once each day.[1] Founded in February 2004, Facebook develops technolo-

1. Detailed statistics are available on Facebook's website: http://www.facebook.com/press/info.php?timeline

gies that "facilitate the sharing of information through a social graph, the digital mapping of people's real-world social connections".[2] According to danah boyd's[3] definition, Facebook is thus a "social network site" in the sense that it is a "web-based service that allows 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".[4] Moreover, the main characteristic of a site like Facebook is to connect participants' profiles to their public identities, using real names and other real-world identification signs such as pictures, videos and e-mail addresses in order to enable interaction and communication between real-world subjects. Therefore, Facebook is a thousand miles away from pseudonymous chat rooms and cannot purely be considered as a playground for "virtual bodies" in which identities are flexible and disconnected from "real-world bodies". In fact, there is almost nothing virtual in sites like Facebook. Not only is the provision of accurate and current information from the users encouraged, it is even required by the terms of use. Indeed, Facebook asks its users to "provide their real names and information", to keep their "contact information accurate and up-to-date" and users must not "provide any false personal information".[5] These requirements, along with the site's mission of organizing the real social life of its members, provide important incentives for users to publish only real and valid information about themselves. Statistics speak for themselves: already in 2005, 89% of the Facebook profiles were real names and 61% of the profiles contained images which allowed for direct identification.[6]

According to Facebook's statistics, more than 850 million photos and more than 8 million videos are uploaded each month. Also, more than 1 billion pieces of content (web links, news stories, blog posts, notes, photos, etc.) are shared each week. Given the widespread use and sharing of personal information deemed to be accurate and up-to-date, major privacy threats can derive from interactions on Facebook, the main one being the risk of de-contextualization of the information being provided by the participants. This de-contextualization threat is due to three major characteristics of Facebook: 1) the simplification of social relations, 2) the high level of information diffusion and 3) the network globalization and normalization effects of Facebook. The risk of de-contextualization not only threatens the right to data protection, i.e. the right of the individual to control their informational identity presented in a certain context. More fundamentally it threatens the human right to privacy: the right to be a conscious, multiple and relational self not suffering any form of discrimination.

In part 1, I examine the various characteristics of Facebook which imply a risk of de-contextualization of the circulating information. Part 2 discusses why this de-contextualization phenomenon threatens both the rights to privacy and to data protection. Finally, I argue that protecting privacy and data protection on Facebook must focus not merely on remedies and penalties for aggrieved individuals but on shaping an architecture to govern the multi-contextual data flows on the site. Given the importance of the de-contextualization threat, the architecture of Facebook must be built to prevent any interference with rights to privacy and to data protection when such interference is not necessary in a democratic state.

1. The risks of de-contextualization deriving from interactions on Facebook

Here I use the term *de-contextualization* to conceptualize what happens when behaviours or information are used in

2. *Ibidem*.
3. danah boyd does not capitalize her name.
4. D. BOYD; N. ELLISON (2007). "Social Network Sites: Definition, History, and Scholarship" [online article]. *Journal of Computer-Mediated Communication*, vol. 1, no. 13, art. 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>. Boyd and Ellison use "social *network* site" rather than "social *networking* site" because "participants are not necessarily 'networking' or looking to meet new people; instead, they are primarily communicating with people who are already a part of their extended social network".
5. See Facebook's "Statement of Rights and Responsibilities": http://fr-fr.facebook.com/terms.php
6. R. GROSS; A. ACQUISTI (2005). "Information Revelation and Privacy in Online Social Networks". In: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. P. 77.

a context other than that for which they were intended. As Nissembaum argues, the de-contextualization phenomenon arises when individuals do not respect contextual norms of distribution and appropriateness.[7] For example, when a form of behaviour appropriate with a close friend in a bar is conducted in public or at work it violates contextual norms of appropriateness. In the same way, if my boss discovers information that was originally intended for my girlfriend it violates contextual norms of distribution. The problem with these contextual norms is that they cannot be precisely defined since they derive from personal sensations about how information should circulate in the physical, or should I say "offline world". Indeed, norms of appropriateness and distribution both assume a certain situational environment because the way information is divulged depends on very granular properties of that environment such as its architectural, temporal and inter-subjective characteristics.[8] As an example, I would not behave the same way with my boss in a bar at 10 pm as I would at 8 am at work, nor would I disclose the same information at 10 pm in the same bar with my boss if my mother joined us. In the physical world, contextual norms of distribution and appropriateness are thus based on something typically human: feelings.

However, as I explain in the next sections, Facebook has a completely different design from the physical world, and its architectural, temporal and inter-subjective properties can potentially create an asymmetry between users' feelings and the way information can be propagated. Therefore, the concept of de-contextualization is particularly interesting when applied to the case of Facebook since it is an environment "when worlds collide, when norms get caught in the crossfire between communities, when the walls that separate social situations come crashing down".[9]

In the next sections I argue that the de-contextualization threat on Facebook is due to three of its major characteristics: 1) the simplification of social relations, 2) the large information dissemination and 3) Facebook's globalization and normalisation effects.

1.1. The simplification of social relations on OSNS

According to statistics published on Facebook, an average user has 120 friends on the site. This means that when a user updates their profile (by uploading a picture or a video, modifying their religious or political preferences, or by changing their relational status), posts a message on their wall or answers a quiz, this information is, by default available and, on average, to more than one hundred persons with whom the user has different kinds of relationships. Indeed, connections of a user on Facebook can be as diverse as family members, colleagues, lovers, real friends, bar acquaintances, old schoolmates or even unknown people. Social network theorists have discussed the relevance of relations of different depths and strengths in a person's social network.[10] Noteworthy is the fact that the application of social network theory to information disclosure highlights significant differences between offline and online scenarios. In the offline world, the relation between information divulgation and a person's social network is traditionally multi-faceted: "In certain occasions we want information about ourselves to be known only in a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better".[11] Hence, offline social networks have ties that can only be loosely defined as weak or strong ties, but in reality these ties are extremely diverse in terms of how close and intimate a subject perceives a relation to be. Online social networks, on the

7. See H. NISSENBAUM (2004). "Privacy as Contextual Integrity". *Washington Law Review*, vol. 79, no. 1.
8. This idea was also formulated by C. PETERSON in "Saving Face: The Privacy Architecture of Facebook" (Draft for comments – Spring 2009), *The Selected Works of Chris Peterson*, p. 9. Available at: http://works.bepress.com/cpeterson/1
9. See C. PETERSON (2009). "Saving Face: The Privacy Architecture of Facebook" (Draft for comments – spring 2009). *Op. cit*, abstract.
10. See e.g. M. GRANOVETTER (1973). "The strength of weak ties". *American Journal of Sociology*, no.78, pp. 1360–1380. See also M. GRANOVETTER (1983). "The strength of weak ties: A network theory revisited". *Sociological Theory*, no. 1, pp. 201–233. The privacy relevance of this theory has been highlighted by Strahilevitz. See L. J. STRAHILEVITZ (2005). "A social networks theory of privacy". *University of Chicago Law Review*, vol. 72, p. 919.
11. R. GROSS; A. ACQUISTI (2005). "Information Revelation and Privacy in Online Social Networks". In: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, p. 81.

other hand, often reduce these nuanced connections to simplistic binary relations: "Friend or not". Observing online social networks, danah boyd notes that "there is no way to determine what metric was used or what the role or weight of the relationship is. While some people are willing to indicate anyone as Friends, and others stick to a conservative definition, most users tend to list anyone who they know and do not actively dislike. This often means that people are indicated as Friends even though the user does not particularly know or trust the person".[12]

Increasingly, Facebook users tend to list as friends anyone they do not actively hate[13] and share with them an incredible amount of data which can potentially be inappropriate in Facebook's *heterotopical*[14] context. Let's take for example a Facebook user who has 100 friends: 4 of them family members, 16 close friends, 1 lover, 4 ex-lovers, 30 old school mates, 30 acquaintances (from different contexts), 14 work colleagues and their boss. Now imagine that our user installs a third party application on Facebook to answer an amusing 'Are you alcoholic?' quiz and at the same time sets their 'relationship status' to single. There is no doubt that the combination of information will have a different meaning for their friends and lover than for colleagues, boss or mother. This is where the threat of de-contextualization arises: the difficulty an individual has to control the information they want to share with Friends in different contexts. Simply said, answering a quiz on 'What's your favourite sexual position?' can certainly provide interesting information to my girlfriend but is surely not appropriate for any of my colleagues.

In this regard, the "Friend lists" feature provided by Facebook which enables users to organize friends into different categories is a start. The tool allows them to include and exclude groups of friends from being able to see parts of their profile and content. In our example, an aware user could group each type of "friend" into different, predefined categories and grant them different access to information such as pictures, videos, status, messages, etc. However, making the problem of limiting access to certain information easier by adding more specific control, Facebook also introduced more complexity and conceptual overhead for users: they now have to categorize their friends. This is precisely why the "Friends lists" feature can't be considered as accurately mimicking the way in which we all limit access to certain personal information to specific friends in the real world. Indeed, the feature looks much more like how a system administrator might set up permissions to computer resources than how information diffusion processes happen in every day life: labelling friends and creating friend lists does not happen consciously in the offline world.

The simplification of social relations on OSNS thus induces a first threat of de-contextualization of information given that the binary relationships on these sites can lead to breaches of contextual norms of appropriateness or norms of distribution: information divulgation will never be as granular in the online world as it is in the offline world.

1.2. The high level of information diffusion implied by interactions on Facebook

It is not only the simplification of social relations on Facebook that involve a threat of de-contextualization, so does the way in which information can potentially be widely disseminated along the social graph. In offline scenarios, it is rare that information about a person will be interesting beyond two degrees of information, as noted by Duncan Watts: "anyone more distant than a friend of a friend is, for all intents and purposes, a stranger [...] Anything more than two degrees might as well be a thousand".[15] In other words, at least in the pre-Facebook era, no one much cared about those people who were removed from us by more than two links. Strahilevitz illustrates this perfectly in the following quote:

12. D. BOYD (2004). "Friendster and publicly articulated social networking". In: *Conference on Human Factors and Computing Systems (CHI 2004)*, April 24-29, Vienna, Austria, p. 2.
13. Note that Hatebook.org, the exact opposite of Facebook, defines itself as "*an anti-social utility that disconnects you from the things you hate*".
14. For more details about Facebook as a heterotopical space, see section 2.1, p. 11.
15. D.J. WATTS. *Six Degrees: The Science of a Connected Age*. New York: Norton, pp. 299-300.

"Extra-marital affairs are fascinating events. That said, no self-respecting person would go to a cocktail party and tell a private story about a friend of a friend of a friend who is having an adulterous affair with someone unknown to the speaker and listener. It is only if the speaker or listener knows who the adulterers are, or if the details of the affair are particularly sordid, humorous, or memorable that the information is likely to get disseminated further through the social network. And by the time the information makes it through this chain, it seems likely that the participants' names would have dropped out of the story."[16]

Thus, when dealing with events described word-of-mouth, a listener should have a "reasonable expectation of contextual integrity" beyond two links in a social network. This rule of thumb does not appear to be as strong when one moves away from offline communications and to online network services such as Facebook, for five main reasons.

Firstly, dissemination of information along the social graph is encouraged with the visible network of friends in every participant's profile. In the real-world, years can pass without friends knowing that they share a mutual friend, whereas on Facebook they can very easily find out which friends they have in common. Such a list also makes it easier for anyone to know who the friends of a friend of a friend are. Moreover, each profile of the list of friends of a friend can be "shared" and commented on the user's profile. As an example, I could go through my contacts list, pick out one of my friends, look at his friends then at the friends of his friends and finally publish the limited profile of one of them on my profile with a disgraceful comment that can then again be shared and commented on further through the social graphs of my own "friends".

Secondly, Facebook is made up of thousands of networks worldwide, and users are encouraged to join them in order to meet and make friends with people in their area. The biggest of these networks are the so-called "geographic networks", the Belgian one bringing more than 780,000 people together. Having joined such a network, a user can then classify users of the same network on the basis of criteria such as gender, age, relationship status, interests and political views. Moreover, depending on the target's privacy settings, users can then access parts or all the friends of friends of friends' profiles.[17]

Another factor that can potentially cause wide dissemination of information is the tagging feature proposed by Facebook. A tag is a keyword, often the real name of a participant associated with or assigned to a piece of information (a picture, a video clip, etc.), thus describing the item and enabling keyword-based classification and search of information. When associated with a picture or a video, a tag directly provides a link to the represented user's profile. This is the classic Facebook problem: you get carried away for a few hours one night (or day) and photos (or videos) of the moment are suddenly posted for all friends of a friend to view, not just your close friends who shared the moment with you. Indeed, Facebook has not created a default privacy setting to allow users to approve or reject photo tags before they can appear on the site.[18]

16. L. J. STRAHILEVITZ, *op.cit,* p. 47.
17. In 2007, the IT security and control firm Sophos revealed that members unwittingly exposed their personal details on a mass scale to millions of strangers, putting themselves at risk of identity theft. The security company took a random snapshot of 200 users in the London Facebook network, which is the single largest geographic network on the site, with more than 1.2 million members, and found that a staggering 75 percent allowed their profiles to be viewed by any other member, regardless of whether or not they had agreed to be friends. Sophos found evidence that Facebook users in other geographic regions are similarly exposing personal information to complete strangers. The reason for this unwanted divulgation of information was that, even if you had previously set up your privacy settings to ensure that only friends could view your information, joining a network automatically opened your profile to every other member of the network. Only in 2009, Facebook changed the default privacy settings for geographical networks to avoid unwanted open profiles.
18. There is a possibility to indirectly restrict the visibility of the tagged photos by first visiting your profile privacy page and modify the setting next to "Photos Tagged of You", select the option which says "Customize...", select the option "Only Me" and then "None of My Networks". If you would like to make tagged photos visible to certain users you can choose to add them in the box under the "Some Friends" option. In the box that appears after you select "Some Friends" you can type either individual friends or friend lists.

A fourth worry for unwanted dissemination of information comes from Facebook Platform for Mobile. According to Facebook's statistics, "there are more than 30 million active users currently accessing Facebook through their mobile devices. People that use Facebook on their mobile devices are almost 50% more active on Facebook than non-mobile users".[19] The biggest privacy threat of such a feature is due to the ubiquity of mobile devices that can let online information enter the offline world anytime, anywhere and anyplace. Indeed, privacy settings do not matter in the offline world: with his mobile, one of my real-world friends could easily show me the complete Facebook profile of one of his "friends" who I do not know at all, just because one of their characteristics was interesting in the context of our personal conversation.

Finally, the introduction of third-party applications on Facebook has opened up users' personal data to an increasingly large group of developers and marketers. According to a 2007 review[20] of the top 150 Facebook applications, nearly 91% had access to unnecessary personal data. Given the recreational nature of many top applications today, this statistic has probably not changed drastically. Users have become accustomed to authorizing even simple applications and do not know what data will be used and to whom it will be transferred prior to authorizing an application. "We're related" is one such third-party application that has been the source of these concerns. According to one report, this application, which claims 15 million active users each month, seeks to identify and link family members who are already on the network, even if they are only distantly related: "New users are asked to give a blanket approval to let the application "pull your profile information, photos, your friends' info and other content that it requires to work". The application then appears to give itself the power to release this information to anyone else on Facebook – even if users have set stricter privacy settings to limit access to their personal data."[21] However, as indicated in Facebook's user terms, the company does not consider itself responsible for inaccurate privacy practices of third party applications developers.[22]

Combined, these five factors induce a risk of unwanted dissemination of data beyond the "reasonable expectations of contextual integrity" of Facebook users since important information exchanged with their "friends" can potentially be spread much further than two links.

In the next section, I argue that this de-contextualization threat can potentially be increased by Facebook's globalization and normalization effects.

1.3. The globalization and normalization effects of Facebook

Many people have experienced the increasing pressure from contacts to finally get with the program and join the network. This can be partly explained by the fact that, when someone registers on Facebook, the site invites the new user to "find out which of [his] email contacts are on Facebook". Facebook then asks users for their email address and password for many of the major providers of webmail services (Yahoo, Hotmail, Gmail, etc.). Facebook then logs on to the account, and downloads all the contacts there. Users are then shown a list of those individuals who are current Facebook members, and have the choice of sending friend requests to each of them. The screen displays all the contacts pre-selected. The user is then given the option of inviting all of their other contacts to join Facebook.[23] By default, all of the contacts are pre-selected so that messages are sent

19. See Facebook statistics on: http://www.facebook.com/press/info.php?statistics
20. A. FELT; D. EVANS (2008). "Privacy Protection for Social Networkin APIs". *W2SP*, May 2008. Available at: http://www.cs.virginia.edu/felt/privacybyproxy.pdf
21. See R. WATERS (2009). "Facebook applications raise privacy fears". *Financial times online*. Available at: http://www.ft.com/cms/s/0/2a58acfa-5c35-11de-aea3-00144feabdc0.html
22. See Facebook's Platform Application Terms of Use: "*When you install a Developer Application, you understand that such Developer Application has not been approved, endorsed, or reviewed in any manner by Facebook, and we are not responsible for your use of or inability to use any Developer Applications, including without limitation the content, accuracy, or reliability of such Developer Application and the privacy practices or other policies of the Developer. YOU USE SUCH DEVELOPER APPLICATIONS AT YOUR OWN RISK*". Available at: http://developers.facebook.com/user_terms.php
23. See http://epic.org/privacy/facebook/

to all of one's contacts inviting them to become friends on Facebook.

Incentives to be on the program become even more concrete when one examines the "tagging" feature proposed by Facebook. A problematic element about this feature is that even people who did not register on the network can be tagged (possibly by so-called friends, complete strangers or even enemies). Of course, the right of access and the right to rectification/deletion can be used if someone wants to remove a particular tag, but to do this it is necessary to first register on Facebook. This is what we could call the globalization effect of Facebook: without being on the program, someone can already be a data object defined by pictures and articles. Without even knowing it and without being able to react, someone can already be a well-documented widely disseminated discussion topic. To become a real data subject, the data object has first to register on Facebook before being able to exercise data protection rights. To become active players in the control over their informational identity, people are obliged to sign up.

Given the impressive growth of Facebook (314% in the last year), the service is increasingly becoming an every day communication tool with, for example, 21% of the Belgian population being registered.[24] Paradoxically, it thus becomes increasingly more abnormal not to be on Facebook than the contrary. This is what we could call the normalization effect of Facebook: a future where employers will ask themselves the question: "Why is Mr X not on Facebook? That's strange... does he have something to hide?" is maybe not so far away.

Having described the three main characteristics of Facebook leading to a risk of de-contextualization of personal information, in the next section I analyze the consequences of this as a threat with respect to rights to privacy and to data protection.

2. Consequences of the threat of de-contextualization on rights to privacy and to data protection

The three characteristics of Facebook that I have discussed simplification of social relations, wide dissemination of information and globalization and normalization effects can potentially lead to major risks of de-contextualization of information, and the threat of de-contextualization of personal information on Facebook can potentially affect both the right to privacy and the right to data protection of the service's users.

The links between these rights have already been examined by influential authors.[25] For the purposes of our discussion, let us take as a starting point the mere fact that the right to privacy is traditionally seen as a human right for all, whereas the right to data protection is provided to data subjects by significant legal instruments at the European level. Indeed, where privacy and the ECHR are all about humans, Directive 95/46 is about data subjects. Why? The question may seem somewhat simplistic or trivial, but understanding the respective meanings of rights to privacy and to data protection from this angle can, I think, help us understand how de-contextualization of information threatens both rights.

24. See statistics on: http://katrin-mathis.de/wp-mu/thesis/
25. Gutwirth and De Hert, for example, discuss the distinction by viewing the right to privacy as being a kind of "*tool of opacity*" whereas, according to the authors, the right to data protection is a "*tool of transparency*". See S. GUTWIRTH; P. DE HERT (2006). "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power". In: E. CLAES; A. DUFF; S. GUTWIRTH (eds.) (2006), *Privacy and the criminal law*. Antwerp: Intersentia, pp. 61-104.

2.1. Consequences of the threat of de-contextualization on privacy as a right of the human being

Recalling that privacy is a right provided to human beings can appear trivial, however the term *human* is extremely ambiguous and has had an extraordinary historical and philosophical evolution. In order to properly introduce this topic and to avoid unnecessary discussions, let us only acknowledge that a human being cannot be reduced to a body nor to a physical person. Of course, human rights should ideally be conferred to all bodies having human specifications as defined by anatomy, but, historically, there is no doubt that lawyers were also influenced by philosophical conceptions of the inner self when designing the human rights framework. As an example, article 1 of the Universal Declaration of Human Rights defines the human as being "endowed with reason and conscience", recalling a very Kantian point of view according to which the definitive characteristic of the human self is its capacity for reason. Reason, according to Kant, allowed the self to understand and order the world with certainty. In consequence, the Kantian self was conceived as an identity pole of coherent subjectivity, standing above the stream of changing experience. However, increasingly in the twentieth century, the liberal modernist notion of the self as a unitary, stable, and transparent individual has come under heavy criticism. Indeed, many postmodern and late modern theories of the self asserted that it is fractured and multiple. According to these, the self is an illusory notion constructed as static and unitary, but in reality completely fluid.[26] Evolution of these reflections leads to conceptions of the human being as a "multiple-self"[27] which is relational, inter-subjective and context-dependent. Goffman's nuanced idea of a cosmopolitan person perfectly reflects the philosophical debate between unification and fragmentation of the modern self which is constantly evolving in a plurality of contexts. According to him, "In many modern settings, individuals are caught up in a variety of differing encounters... each of which may call for different forms of appropriate' behaviour... As the individual leaves one encounter and enters another, he sensitively adjusts the 'presentation of self' in relation to whatever is demanded of a particular situation. Such a view is often thought to imply that an individual has as many selves as there are divergent contexts of interaction... Yet again it would not be correct to see contextual diversity as simply and inevitably promoting the fragmentation of the self, let alone its disintegration into multiple 'selves'. It can just as well, at least in many circumstances, promote an integration of self... A person may make use of diversity in order to create a distinctive self-identity which positively incorporates elements from different settings into an integrated narrative. Thus a cosmopolitan person is one precisely who draws strength from being at home in a variety of contexts."[28]

Behind the postmodern dilemma between unification and fragmentation of the self, important for the purposes of our discussion is the fact that human beings are increasingly conceived as contextual selves constantly reinventing themselves, adopting different roles, postures and attitudes in a complex open network of networks. Taking into account this conceptual evolution of the self towards a contextual self, it is then interesting to analyze the evolution of the meaning of right to privacy.

Since its acceptance as the "right to be left alone",[29] the right to privacy has experienced significant developments. Interestingly, the European Court of Human Rights has asserted that it would be too restrictive to limit the notion of private life to an inner circle in which the individual may live their own personal life as they choose and to entirely exclude the outside world not encompassed

26. See, e.g., K. P. EWING (1990). "The Illusion of Wholeness: Culture, Self, and the Experience of Inconsistency". *Ethos*, vol. 18, no. 3, pp. 251-278 (arguing that people "project multiple, inconsistent self-representations that are context-dependent and may shift rapidly"); A. P. HARRIS (1996). "Foreword: The Unbearable Lightness of Identity". *Berkeley Women's Law Journal*, vol. 11, pp. 207-211 (arguing that the problem with any general theory of identity "is that 'identity itself' has little substance"); J. WICKE (1991). "Postmodern Identity and the Legal Subject". *University of Colorado Law Review*, vol. 62, pp. 455-463 (noting that a postmodern conception of identity recognizes the self as fragmented and captures "its fissuring by the myriad social discourses which construct it").
27. See, e.g., J. ELSTER (1986). "The Multiple Self". *Studies in Rationality and Social Change*. Cambridge University Press.
28. GOFFMAN, cited in A. GIDDENS (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Stanford University Press, 1991, p. 189.
29. WARREN and BRANDEIS (1890). "The right to privacy". *Harvard Law Review*, vol. 4, no. 5.

within that circle: "Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other Human beings".[30] Privacy is now obviously conceived as a phenomenon that regards the relationships between a self and its environment/other selves. As Fried observes,

"Privacy is not just one possible means among others to insure some other value, but that it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence."[31]

Furthermore, as "people have, and it is important that they maintain, different relationships with different people",[32] relationships between selves are by nature extremely contextual. Therefore Nissenbaum asserted that the definitive value to be protected by the right to privacy is the contextual integrity[33] of a given contextual-self having different behaviours and sharing different information depending on the context in which the self is evolving. In this regard, Rachels notes that:

"[T]here is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people... privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have and that is why it is important to us."[34]

In a similar way, Agre defined the right to privacy as "the freedom from unreasonable constraints on the construction of one's own identity".[35] Given that identity-building is increasingly conceived as a progressive autonomic and narrative integration of different elements deriving from a contextual diversity, many authors tend to consider the right to privacy as a right to self-determination which is a major precondition for individual autonomy.[36] In other words, as relations with others are essential for the construction of an individual's personality, the right to privacy also encourages self-development[37] by protecting a diversity of contextualized relations from unreasonable intrusions or leaks. With this perspective, the right to privacy can be conceived as a "right to self-determination of the contextual self" which guarantees the possibility to act and communicate the way the individual contextually wants to without having to fear unreasonable de-contextualization of behaviours or information.

Let us imagine a 45 year old father, working as a bank employee and politically involved in a left-wing anti-militarist party, who goes hunting with his friends on Saturday, goes with his family to church every Sunday and loves to analyse Playboy magazine each Monday with a few colleagues during the morning break. Some might think that some of these context-dependent self-representations are inconsistent or mutually incompatible. Others can easily imagine how inappropriate a behaviour or information from one of these contexts could appear in some of the others. But, more fundamentally, everyone will agree that none of these contexts or situations are *per se* illegal or harmful. This is precisely what the right to privacy is all about: showing respect for individual autonomy, even if a person's inter-contextual identity-building may seem incoherent to some of us. In this perspective, the right to privacy is not only an important precondition for individual autonomy but more generally for the persistence of a living democracy. Antoinette Rouvroy provides one of the best-informed versions of this claim:

30. See e.g. ECHR, *Niemietz v. Germany*, 16 December 1992, nºA 251-B, § 29.
31. C. FRIED (1968). "Privacy". *Yale Law Journal*, no. 77, pp. 475-493.
32. F. SCHOEMAN (1984), "Privacy and Intimate Information". In: *Philosophical Dimensions of Privacy: an anthology*. Pp. 403-408.
33. H. NISSENBAUM, *op.cit.*.
34. J. JAMES (1975). "Why Privacy Is Important". *Philosophy and Public Affairs*, vol 4, no, 4, pp. 323-333.
35. P. E. AGRE; M. ROTENBERG (eds.) (1998). *Technology and Privacy. The New Landscape*. MIT Press, p. 3.
36. See e.g. A. ROUVROY; Y. POULLET (2009). "The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy". In: S. GUTWIRTH; P. DE HERT; Y. POULLET (eds.), *Reinventing Data Protection*. Springer.
37. See ECHR, *Odièvre v. France,* 13 February 2003, where the Court acknowledged that the right to privacy (Article 8 of the European Convention on Human Rights) protects, among other interests, the right to personal development.

"The right to privacy guarantees the possibility for the subject to think differently from the majority and to revise his first order preferences. Thus, privacy is a condition for the existence of 'subjects' capable of participating in a deliberative democracy. As a consequence, privacy also protects lawful, but unpopular, lifestyles against social pressures to conform to dominant social norms. Privacy as freedom from unreasonable constraints in the construction of one's identity, serves to prevent or combat the "tyranny of the majority". The right to privacy and the right not to be discriminated against have in common that they protect the opportunities, for individuals, to experiment a diversity of non-conventional ways of life. Privacy is itself a tool for preventing invidious discriminations and prejudices".[38]

The right to privacy can thus be conceptualized as a right to contextual integrity preserving the possibility for anyone to build their own identity through differentiated relationships. The aim of such a "right to difference" is to ensure multiplicity, creation, novelty and invention in a democratic society and to avoid immobility or sterile, heavy normalization. That is why de-contextualization of personal information can be considered as one of the main threats to the right to privacy.

Such a threat of de-contextualization is particularly present in the case of Facebook which is a platform of collapsed contexts. Indeed, the service merges every possible relationship into one single social space: friendship, politics, work, love, etc. are all mixed together in a single environment. Therefore, Facebook can be seen as what Foucault calls a heterotopia. According to the philosopher,

"Heterotopias are counter-sites, a kind of effectively enacted utopia in which the real sites, all the other real sites that can be found within the culture, are simultaneously represented, contested, and inverted. Places of this kind are outside of all places, even though it may be possible to indicate their location in reality".[39]

This definition, applied to Facebook, reveals all its accuracy. Facebook's servers are situated somewhere in the US, making it possible to indicate their location in reality. Moreover, just as heterotopias, Facebook is "capable of juxtaposing in a single real place several spaces, several sites that are in themselves incompatible".[40] In this sense, Facebook can be considered as being outside of all places. Whereas in the physical world, doors regulate entry, walls muffle sound, curtains block spying eyes, the volume of our voices during a conversation can be modulated depending on the sensitivity of the content and who is in earshot, the "de-contextualizing" architecture of Facebook is above space, and therefore makes it much more difficult to tailor our presentation to fit different situations.[41] Therefore Facebook's heterotopical architecture can potentially create an asymmetry between a user's imagined and actual audience, simply because the platform lacks a separation of spaces. In this way, the service makes it much more difficult for users to evaluate which contextual norms of appropriateness or distribution they should expect respect for when divulgating information on the site.

This is where the phenomenon of de-contextualization on Facebook threatens the right to privacy: it threatens the possibility of the individual to act as a contextual and relational self and prevents them from building their own identity through differentiated relationships. By this, Facebook can also cause major discriminations and prejudices.

2.2. Consequences of the threat of de-contextualization on data protection as a right of data subjects

The de-contextualization phenomenon of Facebook not only threatens the right to privacy of human beings but also the right to data protection of data subjects. Whereas the right to privacy considers human beings, the most important data protection instruments create rights

38. A. ROUVROY (2008). "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence". *Studies in Ethics, Law, and Technology*, vol. 2, Iss. 1, p. 34.
39. M. FOUCAULT (1967). "Of Other Spaces". *Heterotopias*.
40. *Ibidem*.
41. The same idea can be found in C. PETERSON (2009). "Saving Face: The Privacy Architecture of Facebook" (Draft for comments – Spring 2009), *op. cit*, p. 9 and 35.

for data subjects. Directive 95/46 defines a *data subject* as an identified or identifiable natural person and an *identifiable person* as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. A subject of data is thus conceived as someone who can be identified by reference to one or more factors specific to one aspect of their identity. Agre defines the right to data protection as "the right to control over an aspect of the identity one projects to the world".[42] Interestingly, the right to data protection can thus be seen as a means of control on a *partial* projection of someone's "identity", which, as already mentioned, is extremely contextual and relational.

For this reason, I believe that the right to data protection can be conceptualized as a right provided to "dividuals". Registered since the first Noah Webster's Dictionary (1828), the term *dividual* means 'divided, shared, or participated in, in common with others'. The Random House Unabridged Dictionary gives the following meanings: 1) divisible or divided; 2) separate, distinct; 3) distributed, shared. Hence the word *dividual* contains both the meanings of 'shared' and 'divided', basic characteristics of *contextual relationships* in which differentiated content is shared depending on who someone communicates with. The term *dividual* has also been used by Deleuze in his description of societies of control, "which no longer operate by confining people but through continuous control and instant communication".[43] For Deleuze, contemporary society caused a generalized crisis where spaces of enclosure mould people into data "*dividuals*". According to the philosopher,

"The disciplinary societies have two poles: the signature that designates the individual, and the number or administrative numeration that indicates his or her position within a mass. [...] In the societies of control, on the other hand, what is important is no longer either a signature or a number, but a code: the code is a password, while on the other hand disciplinary societies are regulated by watchwords (as much from the point of view of integration as from that of resistance). The numerical language of control is made of codes that mark access to information, or reject it. We no longer find ourselves dealing with the mass/individual pair. Individuals have become "dividuals" and masses, samples, data, markets, or banks."[44]

As the quote illustrates, one of the characteristics of the societies of control is the emergence of "dividuals" conceived as "physically embodied human subjects that are endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems".[45] As Williams writes, via the data collected on us, the technologies of control can separate who we are and what we are from our physical selves. The data become the representations of ourselves within the web of social relations; the data are the signifiers of our preferences and habits. Borrowing from Laudon, this can be called our "data images":[46] since we are not physically present, we are threatened to be reduced to our documented interests and behaviours. As Williams notes, "complex processes of self-determination are thereby threatened to be reified by a few formulae in some electronic storage facility. The separation of our selves from our representations highlights a second aspect of our dividuality. As data, we are classifiable in diverse ways: we are sorted into different categories, and can be evaluated for different purposes. Our divisibility hence becomes the basis for our classifiability into salient, useful, and even profitable categories for third parties that manipulate the data".[47] Thirdly and fundamentally, given the divisibility of our data images into various contexts of representation, "contextual dividuals" are increasingly threatened by the risk of de-con-

42. P. E. AGRE; M. ROTENBERG (eds.). *Technology and Privacy. The New Landscape*. MIT Press, p. 3.
43. G. DELEUZE (1992). "Postscript on the Societies of Control". *October*, no. 59, Winter, pp. 3-7. Cambridge: MIT Press, MA. Available on: http://www.spunk.org/texts/misc/sp000962.txt
44. *Ibidem*.
45. R. W. WILLIAMS (2005). "Politics and Self in the Age of Digital Re(pro)ducibility". *Fast Capitalism*, vol. 1, no. 1. Available on: http://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.html
46. See L. KENNETH (1986). *The Dossier Society: Value Choices in the Design of National Information Systems*. New York: Columbia University Press.
47. R. W. WILLIAMS, *op.cit*.

textualization. Indeed, given the extreme fluidity of electronic data, information collected in one situational context can increasingly be re-used in another, sometimes very inappropriately.

Taking into account these various threats resulting from our increasing divisibility, I argue that European data protection regulation was designed to provide "dividuals" with the means to control the informational image they project in their "dividual context" by enacting general data protection principles and procuring rights to "data subjects". In other words, "data subjects" can be seen as empowered "dividuals" having legal means to challenge any de-contextualization of the information processed on them. Concrete examples of their means of empowerment as regards their contextual informational image can be found in Directive 95/46. First and foremost, Article 6 states that data must be processed "for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". In a certain way, the limitation of purpose principle ties adequate protection for personal data to informational norms of specific contexts, requiring data controllers not to further distribute data when this new flow does not respect the contextual norms. The same article of the Directive also requires data to be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed", demanding that information gathering and dissemination be appropriate for that context and obey the governing norms of information within it. These two principles of the European Directive (purpose limitation and data quality) can thus be interpreted as a consecration of Helen Nissenbaum's theory, according to which "a normative account of privacy in terms of contextual integrity asserts that a privacy violation has occurred when either contextual norms of appropriateness or norms of distribution have been breached".[48] In consequence, the rights of information, access, rectification and opposition can be seen as legal means of empowerment provided to "contextual dividuals" for challenging any breach of contextual norms (of appropriateness or distribution) by data controllers.

In summary, whereas the right to privacy guarantees the individual the possibility to be multi-faceted and to act contextually differently in order to ensure the perseverance of a vivid and deliberative democracy, the right to data protection can be seen as a tool to empower "contextual dividuals" with the means to ensure the contextual integrity of their informational image.

Conceptualizing the right to data protection as a right of "contextual dividuals" can, I think, help us understand why the de-contextualization phenomenon is so particularly harmful for our data protection rights on a site like Facebook. Indeed, one of the prime effects of heterotopical environments such as Facebook is to artificially recompose the individuals. Quoting Foucault,

"The individual is not to be conceived as a sort of elementary nucleus, a primitive atom, a multiple and inert material on which power comes to fasten or against which it happens to strike, and in so doing crushes or subdues individuals. In fact, it is already one of the prime effects of power that certain bodies, certain gestures, certain discourses, certain desires come to be identified and constituted as individuals. The individual, that is, is not the vis-a-vis of power; it is I believe, one of its prime effects".[49]

On Facebook, personal information a user posts online, combined with data outlining the user's actions and interactions with other people, can create a rich profile of that person's interests and activities. The multi-contextual collation of all of my and my friends' contributions can thus easily paint an individual picture of me. Hence, by merging every possible context into one single informational environment, Facebook negates the existence of our dividualities, and by consequence denies our rights as dividuals.

In other words, the purpose described on Facebook's main page – "Facebook helps you connect and share with the people in your life" – is far too broad to determine which data are adequate, relevant and not excessive in relation to that purpose. If Facebook's architecture destroys contextual integrity, it is because the most funda-

48. H. NISSENBAUM (2004). "Privacy as Contextual Integrity". *Washington Law Review*, vol. 79, no. 1, p.138.
49. M. FOUCAULT. "Body/Power". In: Colin GORDON (ed.) (1980). *Foucault on Power/Knowledge: Selected Interviews and other writings 1972-1977*. London: Harvester Press / New York: Pantheon Books, p. 91.

mental characteristics of its design is in direct conflict with norms of distribution and appropriateness. Global multi-contextuality cannot be concealed with a right to data protection because, when the purpose of a service is defined as "everything", then all data can be considered as adequate, relevant and not excessive and every further distribution can be considered as compatible.

Conclusion

The de-contextualization phenomenon on Facebook certainly constitutes a major threat to both rights to privacy and to data protection. European regulators share a similar point of view. In its recent opinion "on online social networking", the Article 29 Working Party stressed that one of its key concerns was "the dissemination and use of information available on SNS for other secondary, unintended purposes".[50] To prevent de-contextualization of information on OSNS, the Working Party advocates "robust security and privacy-friendly default settings"[51] but also wants to increase users' responsibilities by imposing on them duties of a data controller when the OSNS are used as "a collaboration platform for an association or a company", when the OSNS are mainly used "as a platform to advance commercial, political or charitable goals", when "access to profile information extends beyond self-selected contacts" or when "the data is indexable by search engines". Moreover, according to the Working Party, "a high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller".[52]

Given that only 20% of users ever touch their privacy settings,[53] I certainly believe that strong default privacy settings would constitute a first guarantee against de-contextualization. This being said, I have more doubts as regards the Working Party's second proposal. Indeed, raising the users' responsibilities with the hope that there will be less de-contextualization, assumes high levels of awareness and knowledge from users. However, awareness of data protection rights and duties amongst citizens seems to be quite low. According to a recent Eurobarometer, "despite drastic technological changes occurring in the last two decades, the level of concern about data protection hasn't practically changed".[54] The highest levels of awareness of the existence of data protection rights were in Poland (43%), followed by Latvia (38%), France and Hungary (both 35%). Less than one in five citizens in Sweden (16%) and Austria (18%) said they were aware of the legal possibilities for controlling the use of their own personal data.[55]

For this reason, and because it is important for the ECHR "to be interpreted and applied so as to make its safeguards practical and effective, as opposed to theoretical and illusory",[56] I sincerely believe that protecting privacy and data protection on Facebook must focus not merely on remedies and penalties for aggrieved individuals but on shaping an architecture to govern the multi-contextual data flows on the site. Given the importance of the de-contextualization threat, the architecture of Facebook must be built in such a way that it prevents any interference with rights to privacy and to data protection when such interference is not strictly "necessary in a democratic state".

To achieve this goal, European authorities could increase the responsibility of the operators of social networking sites by making them accountable for the design of their sites. Such mechanisms already exist as regards terminal

50. Article 29 Working Party, Opinion 5/2009 on online social networking, 12 June 2009, p. 3.
51. *Ibidem*.
52. *Ibidem*, p. 4
53. According to Facebook CPO Chris Kelly, only 20% of users ever touch their privacy settings. See. R. STROSS, "When Everyone's a Friend, Is Anything Private?". *The New York Times*, March 7 2009. Available at: http://www.nytimes.com/2009/03/08/business/08digi.html
54. See RAPID PRESS RELEASE (April, 200). "Eurobarometer survey reveals that EU citizens are not yet fully aware of their rights on data protection". IP/08/592.
55. See EUROBAROMETER (Feb., 2008). "Data Protection in the European Union: Citizens' perceptions". Analytical report. Available at: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf
56. See ECHR, *Artico v. Italy*, 13 May 1980, Series A no. 37, pp. 15-16, § 33, and *Stafford v. the United Kingdom* [GC], no. 46295/99, § 68, ECHR 2002-IV.

equipment in the electronic communications context. According to article 14(3) of Directive 2002/58, "where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data". In the same manner, Article 3, 3 (c) of Directive 1999/5 states that "the Commission may decide that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected".

In doing so, European authorities could impose less multi-contextual content in OSNS by demanding the operators of such sites to adapt their architecture in accordance with each user's specific intents. As an example, before a user registers on Facebook, a question could be asked such as "For which purpose do you intend to use Facebook?" with a list of answers such as "commercial", "political", "dating", "work relations", "real-world friendship", etc. After having determined more precisely the purpose of each user's registration, Facebook should then collect only adequate, relevant and non-excessive data in relation to that purpose. If a user wants to use the service for multiple purposes, multiple accounts should be encouraged. More generally, Facebook operators should consider carefully "if they can justify forcing their users to act under their real identity rather than under a pseudonym".[57] When the specific purpose of use does not require the real name, pseudonyms should be encouraged.

Reconstructing places inside Facebook is an absolute necessity for users to evaluate which contextual norms of distribution and appropriateness they can expect. Such a claim is not only useful to respect each user's dividuality as regards the right to data protection. More fundamentally it is essential to allow users to construct their identity as multiple and relational selves and hence to act as human beings.

57. Article 29 Working Party, Opinion 5/2009 on online social networking, 12 June 2009, p. 11.

Recommended citation

DUMORTIER, Franck (2009). "Facebook and Risks of 'De-contextualization' of Information". In: "5th Internet, Law and Politics Congress. The Pros and Cons of Social Networks" [online monograph]. *IDP. Revista de Internet, Derecho y Política*. No. 9. UOC. [Accessed: dd/mm/yy].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_eng

ISSN 1699-8154

About the author

Franck Dumortier
franck.dumortier@fundp.ac.be

Franck Dumortier is senior researcher at the Information Technology and Law Research Centre (CRID) and, since 2005, assistant at the Law School of the Notre Dame de la Paix University in Namur. His research particularly focuses on the impact of technologies such as RFIDs, biometrics, surveillance cameras and online social networks on the fundamental human right to privacy.

Université de Namur
Centre de recherche informatique et droit (CRID)
Rempart de la Vierge 5,
B-5000 Namur, Belgium