ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Joergensen, Rikke Frank

Article

The unbearable lightness of user consent

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Joergensen, Rikke Frank (2014) : The unbearable lightness of user consent, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 3, Iss. 4, pp. 1-14, https://doi.org/10.14763/2014.4.330

This Version is available at:
https://hdl.handle.net/10419/213991

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/3.0/de/legalcode

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 3 | Issue 4

The unbearable lightness of user consent

Rikke Frank Joergensen
The Danish Institute for Human Rights, Copenhagen, Denmark, rfj@humanrights.dk

Published on 21 Oct 2014 | DOI: 10.14763/2014.4.330

Abstract: The article discusses challenges to privacy protection in social media platforms, focusing in particular on the principle of user consent. Based on a Danish study, the article argues that in relation to Facebook, user consent de facto served as the price for participating and for gaining access to a social infrastructure. The article opens with a brief introduction to privacy as a human right, followed by a discussion of some of the critique that has been raised towards social media platforms vis-à-vis the right to privacy. Second, it presents the findings from a study conducted amongst 68 Danish high school students in October 2013 concerning their privacy perceptions and practices when using social media platforms. Thirdly, it discusses the implications of these findings in relation to the principle of user consent as a means of providing individuals with control over their personal information in the context of social media platforms.

Keywords: User consent, Privacy, Personal data, Social media

Article information

Received: 21 Aug 2014 **Reviewed:** 09 Sep 2014 **Published:** 21 Oct 2014
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/unbearable-lightness-user-consent

Citation: Joergensen, R. F. (2014). The unbearable lightness of user consent. *Internet Policy Review*, *3*(4). DOI: 10.14763/2014.4.330

Just over a quarter of European social network users feel in complete control with regard to their personal data. More than two-third are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected. Only one-third are aware of the existence of a national public authority responsible for protecting their rights regarding their personal data (TNS Opinion & Social, June 2011:1-2).

INTRODUCTION

The article discusses challenges to privacy protection in social media platforms, with a particular focus on the principle of user consent. User consent is a cornerstone in the data protection regime in Europe and elsewhere, implying that users are entitled to control over the use of their

personal data (Solove, 2012; Kosta, 2013; Bygrave 2002). Based on a Danish study conducted amongst 68 high school students in October 2013, the article argues that in relation to Facebook, user consent has de facto become the price for participating and for gaining access to a social infrastructure. Moreover, while social media companies such as Facebook increasingly speak to their human rights responsibility, their business model is based on extensive data collection and third party sharing, which potentially contradicts basic data protection principles. As such, there is an increasing discrepancy between the individual safeguards stipulated in the EU data protection regime - elaborated in section 3 below - and the users' means of exercising these rights on social media platforms.

In the literature on youth, privacy and social media, at least two conflicting perspectives on privacy are frequently presented. On the one hand, those arguing that the age of privacy is over (Brin, 1998; Kirkpatrick, 2010)[1] and that youth prioritise convenience over privacy, framed as the 'privacy paradox' (Barnes, 2007; Nissenbaum 2010). On the other hand those that argue that youth do care, however, they balance opportunities and risks in their use of social media sites (Tufekci, 2007), which creates a 'privacy dilemma' (Brandtzæg, Lüders et al., 2010). In her study on Facebook, Raynes-Goldie argues that the design and architecture of Facebook is based on radical transparency, whereas users have some expectation of privacy. This divergence between the goals of Facebook and its users is part of the privacy dilemma and one of the reasons users increasingly face increased privacy risks (Raynes-Goldie, 2012:74-75). Also scholars such as boyd (boyd, 2014) have illustrated the complex nature of privacy as it plays out in social media platforms, arguing that the teens' understanding of privacy is related to the ability to control a social situation rather than particular properties of information. The present study, following a number of surveys on the topic[2], shows that privacy in relation to a known circle of friends and family remain a concern to the respondents, whereas they are less occupied with the treatment of their data by Facebook and affiliated companies. It also illustrates the social strategies and interpretations the respondents apply to manage their privacy when using social media.

The article opens with a brief introduction to privacy as a human right, followed by a discussion of some of the critique that has been raised towards social media platforms vis-à-vis the right to privacy by, for example, the European Commission, the Council of Europe, and the Irish Data Protection Agency. Second, it presents the findings from a study conducted amongst Danish high school students in October 2013 concerning their privacy perceptions and practices when using social media platforms such as Facebook. Thirdly, it discusses the implications of these findings in relation to the principle of user consent as a means of providing individuals with control over their personal information in the context of social media platforms.

2. THE RIGHT TO PRIVACY

The right to privacy is a core component of international human rights law stipulated in Article 12 of the Universal Declaration of Human Rights (United Nations, 1948) and in Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966). It is also part of numerous international and regional human rights treaties and conventions such as the European Convention on Human Rights (Council of Europe, 1950). The right to privacy protects *specific private domains* such as a person's body, family, home and correspondence and restricts the collection, use and exchange of personal data[3] about the individual, often referred to as informational privacy (Westin, 1967). A common denominator for the different areas of privacy is access control (Rössler, 2007). This includes *informational privacy* (control over

what others know about us); decisional privacy (control over private decisions and actions); and local privacy (control over a physical space). Individuals have a right to privacy not only in the private domain but also when acting in public spaces.

Within the member states of the Council of Europe the right to privacy is protected by Article 8 of the European Convention on Human Rights. The European Court of Human Rights has stated that while Article 8 essentially protects the individual against arbitrary interference by the state, there may be positive obligations inherent to an effective respect for privacy (K.U. v. Finland, 2 December 2008). As regards the internet, a state could arguably be liable in respect of third parties who store data on individuals (Council of Europe, October 2013). Up until now, the court has not resolved any cases dealing specifically with the collection, use and distribution of personal data by social media companies[4].

As with other human rights, the protection and enforcement of the right to privacy relies on national measures such as data protection laws and mechanisms of oversight. Contrary to most other regions, the EU countries are bound by a common Data Protection Directive (European Commission, 1995), which entail various provisions and safeguards concerning the capture and flow of personal information. In an increasingly digital world, however, numerous papers and civil society statements have warned against the erosion of informational privacy and called for globally applicable data protection standards[5]. The ongoing reform of the EU data protection regime (Dix, 2013; European Commission, 2014)[6], the White Paper on Consumer Data Privacy in a Networked World from the Obama Administration (The White House, 23 February 2012), and the revised OECD Privacy Framework (OECD, 2013) are all examples of current policy responses addressing this concern. In reaction to the revelations from former NSA-contractor Edward Snowden, the UN General Assembly in December 2013 adopted the first resolution on the right to privacy in the digital age (United Nations General Assembly, 18 December 2013), acknowledging that the right to privacy is under strong pressure.

3. ONLINE PRIVACY AND SOCIAL NETWORK SITES

In recent years, there has been an increasing focus on the way social media platforms handle personal data (Brandtzæg, Lüders et al., 2010; Raynes-Goldie, 2012; Bechmann, 2014), as well as the associated challenges related to the principle of user consent (Mantelero, 2014; Bechmann, 2014). In Europe, concern has been raised, for example, by the EU data protection authorities (Article 29 Data Protection Working Party, 22 June 2009), in the EU data protection reform package (Dix, 2013) by the Council of Europe (Council of Europe, April 2012), and by several of the national data protection authorities, not least of which the Irish (Irish Data Protection Commissioner, 21 September 2012). Some of the key concerns and recommendations from these bodies are highlighted below.

The Opinion from the EU data protection authorities (Article 29 Working Party) concerns the interrelation between the EU Data Protection Directive and social networking sites such as Facebook (Article 29 Data Protection Working Party, 22 June 2009). The opinion stresses that the Data Protection Directive applies to social network providers in most cases, even if their headquarters are located outside of the European Economic Area. Moreover, it iterates the obligation on social network sites to provide their users with clear information about the purposes and different ways in which they process personal data. The default settings of the service has to be privacy-friendly and allow users to specifically consent to any access to their profile's content. Also, users should be given an opt out option before their personal data is

made available to others. In the case of data being used for personalised advertisements, this requires a prior consent by the user. With regard to remedies, the social network sites should make available a tool for lodging complaints.

The EU data protection reform package reiterates several of the points raised above. One of the most controversial topics has been a proposed 'right to be forgotten'. The right implies that when there are no legitimate grounds for retaining personal information, the data has to be deleted. According to Peter Hustinx, the European Data Protection Supervisor, the data would be attributed some sort of expiration date[7]. Hustinx has stressed that in the online domain economic forces work against the individuals' right to privacy, hence there is a need to strengthen the request for data deletion. "From an economic perspective, it is more costly for a data controller to delete data than to keep them stored. The exercise of the rights of the individual therefore goes against the natural economic trend"[8]. Other elements of the reform package with an impact on social network sites include a right for individuals to transfer personal data from one service provider to another (data portability); stronger requirements on consent when required for data processing; and a request for 'privacy by design' and 'privacy impact assessment'. The latter implies risk analysis as part of new projects that may affect users right to privacy (European Commission, 2012).

The Council of Europe has addressed the privacy implications of social networking services in a recommendation from 2012 (Council of Europe, April 2012). The recommendation highlights two factors that threaten the right to private life. First, the lack of privacy-friendly default settings. Second, the lack of transparency about the purposes for which personal data is collected. To counter these threats a number of actions are proposed, many of which echo the concern raised at the EU level. For example, social network sites should provide users with explanations of the terms and conditions of their services in a form that is easily understandable; they should - by default - limit access by third parties to contacts identified by the user; and when allowing third party applications to access users' personal data, they should allow users to specifically consent to access to different kinds of data.

As a final and specific example, the Irish Data Protection Commissioner in 2011/2012 investigated Facebook's compliance with the European data protection law (Irish Data Protection Commissioner, 21 September 2012). The review came in response to allegations, such as the one formulated by Austrian law student Max Schrems, claiming that Facebook retained personal data after accounts had been deleted. The review focused on two aspects in particular. First, *user control* via, for instance, transparency as to how data is handled; control over settings; and ready access to personal data. Second, *limiting use of personal data* via, for example, limits to targeted advertising; no use of cookies and social plug-ins for profiling; face recognition and tagging, subject to informed consent; consistency between privacy policy and third-party applications; and clear retention periods for deletion of data.

In summary, the concern and recommendations raised in the above-mentioned sources focus on means of making it more transparent and easy for the user to limit access to their data - e.g. privacy-friendly policies and settings; and on making demands on the company that process and exchange personal data - e.g. a request for user consent prior to release targeted advertisement. Moreover users should have easy access to complaint mechanisms in case of alleged privacy breaches. Keeping in mind these concerns and recommendations, the following section presents a Danish study on how high-school students frame and manage their online privacy when participating in social media platforms.

4. METHODOLOGY

The present qualitative study was initiated by the consortium 'Digital Youth' (*Digitale Unge*), consisting of the Danish Media Council for Children and Young People, the Danish Consumer Council, Digital Identity, and the Danish Institute for Human Rights[9]. The study was a follow-up to a quantitative survey on youth, social media and privacy conducted by Digital Youth in February 2013 amongst 327 teens (12-18) and 404 adults (30-59) using a web-based questionnaire[10]. Based on the first survey, it was decided to focus in more detail on how youth respondents perceive and manage privacy and control over personal data in their social media practices. The study follows several related surveys - as mentioned in note ii.

The study was conducted in October 2013 and consisted of eleven focus group interviews carried out in six high-schools (*gymnasier*) located in the Copenhagen and Aarhus areas. The study included 68 students in total, with four to eight participants of mixed gender in each group. The students were in each case selected by one of the high school teachers who had asked around for students interested in the topic and willing to participate in the study. The interviews were audio recorded and lasted approximately one hour. They all followed a semi-structured interview guide (Thagaard, 2004; Kvale, 2008) focusing on three main themes. First, the role that social media platforms play in the everyday life of the respondents. Second, the strategies deployed to protect or control privacy, and third, the level of knowledge and awareness with regard to privacy and social media. The interviews were conducted in an open and explorative manner, allowing the respondents to elaborate on their experiences and interpretations of practice in relation to each theme.[11]

5. RESULTS FROM THE DANISH STUDY

THE ROLE OF SOCIAL MEDIA IN THE EVERYDAY LIFE OF THE RESPONDENTS

The first category of questions concerned the role that online media play in the respondents' lives. The respondents mentioned Facebook, Instagram, Twitter and Snapchat as widely used social media services, with Facebook as the key platform from which virtually all communication originates. All of the interviewed had a profile on Facebook and shared a common expectation of being reachable via Facebook: "*It is kind of expected that everyone has a Facebook profile. That you can communicate with everyone there.*" (17 year old girl). It was said that if you want to participate socially, you need to be on Facebook: "*There is a party at the school tomorrow. It might be announced on the school's website, but no one has checked it out there. Everyone is invited for an event on Facebook. So it's also used for practical information. For example that tickets can be bought on a website. And that is not mentioned on the school's website.*" (17 year old boy)

The respondents depicted themselves as "always on" via their smartphone, and described how Facebook was used for several purposes from entertainment, maintenance of social networks to 'staying updated ' on social events. Moreover, relationships with other people were also reinforced and confirmed via Facebook. For example as explained by several of the respondents "you are not truly a couple until it has been announced on Facebook". The respondents highlighted their personal investment into their social media profiles and how their Facebook profile has become an extension of themselves. As one 17 year old boy describes it, when

picturing the scenario of Facebook closing down one day: "*... it is kind of like you have invested so much time in it and so much focus on how you present yourself. And this is your friends. So it's kind of like a project. It's part of you. So it's a bit like not being able to talk. It's a tool of communication which is very integrated in you.*" But perhaps most importantly the respondents view their social media profiles as an integrated part of their identity: "*One's life is not just pictured on Facebook. It is Facebook.*" (17 year old boy) This is similar to findings from Bechmann's research amongst fifteen high school students (Bechmann, 2014), which suggests that Facebook has become so large and dominant a social platform - not least in Denmark - that people 'have to be on Facebook' in order to participate in social life.

STRATEGIES USED TO PROTECT AND CONTROL PRIVACY

The second group of questions concerned the strategies deployed to control privacy. In all of the groups there were commonly shared norms and boundaries on what is respectively good and bad behaviour in relation to sharing. Some of the mentioned examples of what not to share included emotional status updates about personal matters - parents' divorce, break up with girlfriends and boyfriends, etc. The respondents all used Facebook's 'privacy tools', for example, to create groups and to control access to their timelines, which is a chronological display of a user's history on Facebook. Yet they were also aware of the limits of these tools: "*And if there are some embarrassing pictures from some parties then I usually make them invisible to all, for example if someone tags a picture of me at a party where there has been an embarrassing situation. Then you can make it "not allowed on timeline". But I can't delete the picture.*" (16 year old boy)

Many of the respondents' activities on Facebook took place in thematic groups created for specific purposes and for invitees only. The groups usually reflected already established social contexts such as the class, the football team, etc. In addition to the privacy tools provided by Facebook, the respondents relied on shared social norms to manage their privacy. For example many described a 'filtering process' that pictures went through either before or after they were posted. Again, some pictures would not be posted on the Facebook timeline as they were deemed "not suitable for Facebook". Others would be deleted just after being posted if deemed unfit in comments by peers. As one 17 year old girl put it: "*But you also look at the picture yourself one more time and think if you would like it yourself to have it posted. (.) There are also pictures that are taken to look ugly just for fun. But in that case it doesn't even cross my mind to post it on Facebook. That is just not Facebook material.*" The sense of shared norms created an expectation among the respondents that they might control their social privacy: "*It is also a sort of unwritten rule that if you hint that something needs to be deleted, then the picture should be deleted. You can write "Yieks!" or "ehr". Or just "delete". Then it should be deleted within one minute. I mean, you see it immediately on your mobile and then you can write. Then it will be deleted quite quickly.*" (17 year old girl)

While users have a right to an effective remedy when their right to privacy is potentially violated, the above findings indicate that the respondents have limited knowledge of these privacy rights and how to address a potential privacy violation[12]. The study found, however, that the respondents feel somewhat protected by the sense of shared social norms, most notably the ability to have undesired content deleted.

LEVEL OF KNOWLEDGE AND AWARENESS WITH REGARD TO PRIVACY

The third theme focused on the respondents' level of knowledge regarding potential privacy risks. While the respondents were conscious of controlling their privacy in relation to friends and family, they had more difficulty in relating to privacy risks at state or company level. This is

similar to previous findings (Bechmann, 2014; boyd, 2014) stressing that youth are more concerned with controlling their data in relation to their social circles as compared to potential privacy risks towards the state or private companies. Some did talk about personal experiences discovering that one of their images have been used by others to create fake profiles or remembered to have been puzzled over how other people had found out information about them. Mostly the respondents found it hard to imagine that their personal data would be of interest to anyone. Frequently "surveillance" was described as something remote that would take place in 'totalitarian states' far away. "*I feel it's not a problem (ed. state surveillance). It's unpleasant when I think about it. But then I just want to look at Facebook again and then it does not matter*." (16 year old girl). In cases where the respondents were asked to think further about potential state surveillance, it was described as in principle 'not okay', 'uncanny' and 'uncomfortable': "*... Just the thought is indeed uncanny. If the state monitors you personally. They do not have the right to do that and they shouldn't have the right either." (16 year old boy). "It's a scary thought. But this only takes place in totalitarian places. But then again for instance in the United States right now where we have the NSA with Edward Snowden and all that. Where they spy on different people through social media and Google. It's not a very comforting thought*." (16 year old girl)

When asked specifically about the terms and conditions they had consented to, none of the interviewed had read them. Moreover, the majority had created their profiles at a time when they were under 13. "*You have heard that you probably should read those terms and conditions, because we do not know our rights. But we were very young when we created it. And then we just clicked yes." (17 year old girl). "I guess it doesn't matter to read it (terms and conditions) because if you want a profile then you need to accept them. It doesn't matter what it says*." (16 year old boy)

As discussed above, European data protection (as well as data protection regimes in other part of the world) is based on the principle of consent, indicating that the individual has a right to decide whether to share his/her personal information or not. The above findings indicate that the respondents perceive their consent to Facebook's terms of service as a 'tick in a box' needed in order to gain access to a crucial social infrastructure. None of the respondents had read the terms before consenting, and several stated that if the service was "doing bad stuff" they presumably would have heard about it.

THE STUDY: CONCLUSIONS AND PERSPECTIVES

The study revealed that the respondents were very conscious about controlling their privacy vis-à-vis their social circles, i.e., to protect their self-representation and flow of information amongst their peers. Contrary to this, privacy risks related to surveillance[13] and commercial use received limited attention. "*Maybe my messages are subject to surveillance, but what can they use it for? You decide for yourself, what to share*." (16 year old girl). The quote is indicative of a sentiment that many of the interviewed shared, namely that you exercise privacy control by decisions on what to share on Facebook and what not, yet once information is 'out there', your ability to exercise control is non-existent. Also, the respondents had limited knowledge of privacy and data protection as a right that the individual might claim. On the contrary several of the respondents expressed that by joining Facebook you sign off your rights, in particular related to your photos. Since Facebook is seen as the social infrastructure, the sense amongst the respondents was that in reality you have no choice but to accept Facebook's terms and conditions.

In the words of O'Reilly, Facebook is an archetypical example of a web 2.0 platform built around

user-provided data (O'Reilly, 2005:1). In Raynes-Goldie's empirical study of Facebook's business model the author concluded that the company's privacy policy is guided by a belief system which encourages 'radical transparency' and is at odds with conventional understandings of privacy. "Through Facebook's features, in-line with the O'Reilly's Web 2.0 revenue model as well as Wiener's notion of order as moral good, users convert their activities into structured, formal databases and code so that they can be surveilled, managed, searched, aggregated, mined, monetised and sold" (Raynes-Goldie, 2012: 154). Arguably, there is a fundamental disconnect between a business model where the free, unfettered flow of information is key to harnessing the commercial value of user data, and the value of privacy. As such, the above mentioned critique from regulatory bodies and data protection authorities comes as no surprise. On the contrary, it highlights a fundamental conflict between user control over personal data and Facebook's business model.

In recent years, companies such as Facebook increasingly speak to their human rights responsibility and endorse the UN Guiding Principles on Business and Human Rights (United Nations Human Rights Council, 21 March 2011). An often quoted example is the Global Network Initiative - to which Facebook is a member - that aims to strengthen internet companies' compliance with human rights standards on privacy and freedom of expression [14]. This commitment to privacy, however, is based on voluntary codes of conduct, thus it is largely up to the companies to decide on their data protection practices, with limited means of holding them accountable for adverse privacy impacts.

In summary, the above mentioned findings support many of the concerns addressed by the European Commission, the Council of Europe, and the Irish data protection authority in the previous section. The interviewed do not feel they have control over their data once submitted; they have not read the terms and conditions they have consented to; and they do not perceive privacy as a right they may claim, for example, via the Data Protection Agency. As such there is a discrepancy between the principle of user consent and the respondents' perceived lack of control over their personal data when participating in social media platforms.

6. CONCLUSION: ALTERNATIVES TO USER CONSENT?

The study highlights that a data protection regime built around the notion of user content do not adequately address the unequal power relation between a company perceived to provide a social infrastructure and users in demand of that service. In other words, the value of user consent as a data protection safeguard diminishes if users perceive no alternatives but to accept the terms and conditions of a given service.

Several scholars have argued that there is a need to fundamentally rethink the modalities of data protection. One of the alternative models is provided by Nissenbaum, who proposes the notion of contextual integrity as a normative framework built on the premise that different contexts carry different informational norms (Nissenbaum, 2010). In this approach a 'one-size-fits-all' privacy concept is replaced by a framework that places emphasis on the situational systems of rules governing information flows. Accordingly, the key challenge is to ensure that information flows appropriately, and to strengthen the individuals information control in various contexts. In consequence, privacy invasive behaviour is related to improper (out of context) sharing and use of personal information. Nissenbaum suggests to articulate the norms that are to guide specific online practices based on the well-known social situations that these practices resemble, such as information search or socialising with family and friends. As such, limitations in

information flows should not solely depend on user consent but rather on context-appropriate norms. “We must articulate a backdrop of context-specific substantive norms that constrain what information websites can collect, with whom they can share it, and under what conditions it can be shared” (Nissenbaum, 2011:32). The concept is suggested both as a framework for evaluating systems that process personal information, and when designing new systems. Applying such an approach to, for example, Facebook would require analysis on norms and rules guiding similar social situations and subsequently use these to prescribe the specific norms that Facebook should adhere to when processing personal data. An agreed norm about non-disclosure of other peoples contact information, for example, would imply that this was not allowed within the Facebook platform unless specifically requested by the person in question.

Other scholars have argued that in the era of ‘big data’ the principle of ‘privacy by consent’ has become increasingly meaningless and should be replaced by ‘privacy by accountability’ including stricter means of holding companies accountable for how they use data (Mayer-Schönberger, 2013:173-75). Mayer-Schönberger has argued that in the age of big data much of data’s value is in secondary uses that were not foreseen when the data was collected. Hence, data protection should place less emphasis on data collection and more on the subsequent uses of data. Data is no longer collected based on a specific purpose and an informed user consent, on the contrary, the purpose of collecting the data is frequently formulated in broad generic terms and accepted by the user with limited sense of what the consent implies. “The ability to capture personal data is often built deep into the tools we use every day, from Web sites to smartphone apps” (Ibid: xx). Coupled with the fact that personal data represents commercial value to an extent not previously seen, it makes no sense to rely on user content as the primary data protection mechanism, the argument goes. In consequence, Mayer-Schönberger suggests to focus on increased accountability for the companies that use data and to increase the power of data protection authorities as safeguards between the individual and data processing companies such as Facebook. In the words of Mayer-Schönberger; hold companies liable when harm to data subjects occurs, rather than limit their means of data collection. “I suggest to take the individual out of the equation and give data protection authorities much more teeth in order to enforce data protection law vis-a-vis companies”[15].

While alternative data protection schemes based on contextual integrity or stronger enforcement regimes may have immediate appeal, they both entail problems as well. The contextual integrity approach would require detailed analysis of a number of social contexts and situations, most likely associated with different norms across countries. As such it raised a number of challenges and provides limited guidance in relation to implementation. Moreover, it would require a complete rethinking of the current data protection regime. As for the accountability approach, this seems to ignore or downplay the fundamental disconnect between the commercial value that personal data hold for a company and the individuals’ right to privacy. Trusting that a principle of company accountability coupled with stronger enforcement mechanisms will be enough to safeguard the individual’s right to privacy seems overly optimistic in an age where personal data holds unprecedented commercial value, and where harvesting of personal data is the core of the online business model. Yet, the current model based on user consent is also not convincing as illustrated in this article. This is ironic, given the fact that the current data protection reform within the EU - as well as within the Council of Europe – remain anchored in precisely user consent, despite the decreasing relevance of this mechanism as a measure that will de facto preserve a right to user control over personal data in the online environment.

FOOTNOTES

1. Brin's book is not focused on youth practices as such but entails a general account of the proclaimed erosion of privacy. Brin argues that the right to privacy is outdated and contradict online social practices by which personal information is widely exposed and shared across various platforms. In response he suggests to deconstruct the entire notion of privacy and shift focus to accountability (Brin, 1998).

2. In a European context, related studies on online experiences and risks include the EC funded research project EU Kids Online (focus on kids), available at: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx; the EC funded research project CONSENT (focus on internet users more broadly), available at http://consent.law.muni.cz/view.php?cisloclanku=2013040002, and the Special Eurobarometer 359 from 2011 (TNS Opinion & Social, June 2011). Internationally, the Internet Society has conducted a Global Internet User Survey in 2012, which among other addresses how often users read the privacy policies of online services, available at: http://www.internetsociety.org/apps/surveyexplorer/online-privacy-and-identity/how-often-do-you-read-the-privacy-policies-of-websites-or-services-that-you-share-personal-information-with-17/. In a Danish context, Bechmann (Bechmann, 2014) has studied 'consent cultures' on Facebook amongst 15 high school students.

3. According to the Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data, 'personal data' is defined as any information relating to an identified or identifiable individual (Council of Europe, 1981).

4. The right to privacy is also stipulated in Article 7 and 8 of the EU Charter on Fundamental Rights, binding upon EU member states (The European Parliament, the European Council et al., 2007)

5. See, for example, the Madrid Privacy Declaration, that reaffirms international instruments for privacy protection and call for actions. The declaration is signed by a broad range of scholars and civil society organisations (Public Voice, 3 November 2009).

6. Retrieved August 10, 2014 from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf]/fn|, the modernisation of the Council of Europe's Convention on the Protection of Individuals with regard to Automatic Processing of Personal DataRetrieved August 10, 2014 from http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

7. See article 88 of the Opinion of the Data Protection Supervisor, 14 January 2011. Retrieved August 10, 2014 from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

8. Quote from article 84 of the Opinion of the Data Protection Supervisor, 14 January 2011. Retrieved August 10, 2014 from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

9. Digital Youth was created in 2013 as a platform for gathering knowledge and raising

awareness concerning youth practices and perceptions in relation to social media. See www.digitaleunge.dk Retrieved 14 August 2014. The author of this article is an employee of the Danish Institute for Human Rights.

10. The results of the quantitative survey are available (in Danish). Retrieved August 14, 2014 from http://digitaleunge.files.wordpress.com/2013/06/teenagere-deres-private-og-offentlige-liv-pc3a5-sociale-medier.pdf

11. The author participated in the study design, data collection and data analysis together with Werner Leth and Gry Hasselbach from the Danish Media Council. For a (Danish) report on the findings of the study please refer to (Jørgensen, Hasselbach et al. November 2013).

12. The right to remedy - stipulated in, for example, Article 13 of the European Convention of Human Rights - implies that remedies should be accessible, affordable and capable of providing appropriate redress (Council of Europe, 16 April 2014:6).

13. The principles are available. Retrieved August 10, 2014 from https://en.necessaryandproportionate.org/text

14. In 2014, the first independent audit of Google, Microsoft and Yahoo's compliance with GNI norms has been conducted. The assessment report of 8 January 2014 is available. Retrieved January 14, 2014 from http://globalnetworkinitiative.org/news/gni-report-finds-google-microsoft-and-yahoo-compliant-free-expression-and-privacy-principles

15. Response given by Viktor Mayer-Schönberger at "Big Data" research seminar, Copenhagen Business School, 18 September 2013.

REFERENCES

Article 29 Data Protection Working Party (June 22, 2009). *Opinion 5/2009 on online social networking*. Brussels: EC Justice.

Barnes, S. B. (2007). A privacy paradox: Social networking in the United States. *First Monday* 11(9).

Bechmann, A. (2014). Non-informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies* 11 (1): 21-38.

boyd, d. (2014). *It's complicated : the social lives of networked teens*. New Haven: Yale University Press.

Brandtzæg, P. B., Lüders, M., Skjetne, S.H. (2010). "Too many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites." *Journal of Human-Computer Interaction* 26 (11-12): 1006-1030.

Brin, D. (1998). *The Transparent Society*. New York: Perseus Books.

Bygrave, L.A. (2002). *Data Protection Law. Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague, London, New York.

Council of Europe (1950). *Convention on the Protection of Human Rights and Fundamental Freedoms*. Strasbourg: Council of Europe.

Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg: Council of Europe.

Council of Europe (April 16, 2014). *Recommendation of the Committee of Ministers to member states on a guide on human rights for Internet users*. Strasbourg: Council of Europe.

Council of Europe (April 2012). *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*. Strasbourg: Council of Europe.

Council of Europe (October 2013). *Factsheet - New technologies*. Strasbourg: Council of Europe, 7.

Dix, A. (2013). EU data protection reform opportunities and concerns. *Intereconomics* 48 (5): 268-285.

European Commission (1995). *EU Directive on Data Protection (95/46 EC)*. Brussels: EC.

European Commission (2012). *How will the data protection reform affect social networks?* Brussels: EC. Retrieved February 4, 2013, from http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

European Commission (2014). *Progress on EU data protection reform now irreversible following European Parliament vote*, MEMO/14/186 - 12/03/2014. Brussels, EC.

Irish Data Protection Commissioner (September 21, 2012). *Report of RE-Audit*. Portarlington: Irish Data Protection Commissioner.

Jørgensen, R. F., Hasselbach, G., Leth, V. (November 2013). *Unges private og offentlige liv på sociale medier* (Youths´ private and public life on social media). Copenhagen: Digital Youth.

Kirkpatrick, M. (January 9, 2010). *Facebook´s Zuckerberg Says The Age of Privacy is Over*. ReadWriteWeb. Retrieved July 10, 2014, from http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php.

Kosta, E. (2013). *Consent in European data protection law*. Leiden: Brill Nijhoff.

Kvale, S. (2008). *Interviews: an introduction to qualitative research interviewing*. London: SAGE.

Mantelero, A. (2014). Defining a new paradigm for data protection in the world of Big Data analytics. The Second ASE International conference on Big Data and Computning May 27-31, 2014. Stanford University, ASE@360 Open Scientific Digital Library.

Mayer-Schönberger, V. C. K. (2013). *Big data : a revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt: 173-175.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus, the journal of the American Academy of Arts & Sciences* 140 (4): 32-48, 32.

Nissenbaum, H. F. (2010). *Privacy in context : technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford Law Books.

O´Reilly, T. (2005). What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *O'Reilly*. Retrieved September 2, 2011, from http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

OECD (2013). *The OECD Privacy Framework*. Paris: OECD.

Public Voice (November 3, 2009). The Madrid Privacy Declaration - Global Privacy Standards for a Global World. *The Public Voice*. Retrieved September 2, 2011, from http://thepublicvoice.org/madrid-declaration/.

Raynes-Goldie, K. (2012). *Privacy in the Age of Facebook: Discourse, Architecture, Consequences*. Perth, Australia: Curtin University.

Rössler, B. (2007). The Value of Privacy. In G. Stocker and C. Schöpf (Eds.), *Goodbye privacy - Ars Electronica 2007*, p. 39-44. Ostfildern-Ruit: Hatje Cantz Verlag: 39-44, 26.

Snyder, D. (2007). The NSA's "*General Warrants: How the Founding Fathers Fought an 18th Century Version of the President's Illegal Domestic Spying*". Retrieved September 2, 2011, from http://www.eff.org/files/filenode/att/generalwarrantsmemo.pdf.

Solove, D. (2012). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126: 1880-1903.

Thagaard, T. (2004). *Systematic approaches and Empathy. An introduction to qualitative methods*. Copenhagen: Akademisk Forlag.

The European Parliament, the European Council, et al. (2007). *Charter of Fundamental Rights*

of the European Union. Brussels: EC.

The White House (February 23, 2012). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Washington: The White House.

TNS Opinion & Social (June 2011). *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*. Brussels: European Commission.

Tufekci, Z. (2007). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society Bulletin of Science, Technology & Society* 28(1): 20-36.

United Nations (1948). *The Universal Declaration of Human Rights*. New York: United Nations.

United Nations (1966). *International Covenant on Civil and Political Rights*. New York: United Nations.

United Nations General Assembly (December 18, 2013). *Resolution adopted by the General Assembly. The right to privacy in the digital age*. New York: United Nations.

United Nations Human Rights Council (March 21, 2011). *Report of the Special Representative John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*. New York: United Nations.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Winston, M. (2007). "Human Rights as Moral Rebellion and Social Construction. *Journal of Human Rights* 6 (3): 279-305.