Social Networking: The Application of the Data Protection Framework Revisited

REBECCA WONG*

This article will revisit the social media issues in the context of the Data Protection legislative framework and the extent to which the notion of 'data controller' could extend to individuals. The main contribution is that the discussion will add to the debate on the blurring of the distinctions drawn between public and private spheres and whether what is published on social media should be deemed to be private or in the public domain. This paper will revisit the concept of 'data controller' in the context of social media and consider the extent to which users are entitled to the 'privacy' of data they share on a social media platform. It will also cover some of the forthcoming changes introduced under the proposed Data Protection Regulation including the 'right to be forgotten'.

Introduction

In 2007,[1] I examined the emerging development of social media in the context of the data protection legislative framework and the extent to which the notion of 'data controller' could extend to individuals. In other words, the application of the Data Protection Directive 95/46/EC (DPD) could apply to individuals for posting information about others on social media such as Facebook. Although the data protection framework did not envisage extending

* Senior Lecturer, Nottingham Law School (email: r.wong@ntu.ac.uk).

[1] Rebecca Wong, 'Social Networking: A Conceptual Analysis of a Data Controller' (2009) 14 Communications Law 142. Original working paper: 'Social Networking: Anybody is a Data Controller' (2008) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668> accessed 28 August 2014.

its breadth, the Art. 29 Working Party on data protection published an opinion making it clear that users would only be responsible in so far that it goes beyond the private purposes category such as acting on behalf of a company or association or using the social networking site to promote charitable or political aims.[2]

This paper will revisit some of these issues and consider whether there have been any significant developments since then. For the purposes of this study, this paper will consider the legal frameworks in the UK, Germany Sweden, and to a limited extent, Norway.

Background

The main statutory provision that deals with the application of the DPD is Art. 4—application of the directive. This provides that Art. 4(1)(a) of the DPD and corresponding national laws implementing the DPD apply to activities of an establishment of the controller on the territory of the European Union member state, or where the data controller had used equipment to process the data of an individual, thus falling within the scope of Art. 4(1)(c). To exemplify this, consider the example of MySpace, whom has its headquarters in and is domiciled in California. This means that the DPD would not be applicable. However, if they process or use equipment within a member state of the EU, then they could be deemed to be processing personal data and thus fall within the scope of the DPD.[3] The question that then arises is, who is the data controller in this scenario? MySpace or its users? First, MySpace if it processes data of its users. The complexity then arises when users use data belonging to other users—who owns this data? For instance, a photograph may be more difficult to ascertain. Who owns the photograph? The

[2] Art. 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 5/2009 on Online Social Networking* (WP 163, 2009) para 3.1.1 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf> accessed 14 November 2014.

[3] This is likely to change under the forthcoming Data Protection Regulation which provides that the Regulation will apply where the processing of activities are related to (a) the offering of goods or services to such data subjects in the Union or (b) the monitoring of their behaviour (Art. 3).

Copyright, Designs and Patents Act would indicate that it was the photographer who owns the photograph. The DPD, however, places responsibility on the data controller to ensure that any processing of personal information is carried out in accordance with the DPD.

It was originally thought that the DPD would not apply to a social networking site (SNS) environment given its historical background and the opinions of the Data Protection Commissioners. However, the Art. 29 Working Party, responsible for providing guidance on the application of the data protection laws decided in 2009 (by issuing an opinion to that effect)[4] that the household exemption under Art. 3 of the DPD applies and therefore SNS users would not be considered to be data controllers unless they fall under narrow exceptions where activities were used to promote charitable or political aims. According to the Art. 29 Working Party, if the SNS user acts on behalf of a company or association or uses the SNS to promote commercial, political or charitable goals, Art. 3 exception would not apply as it would go beyond the definition of personal or household exemption.[5] It was further acknowledged by the Art. 29 Working Party that even if Art. 3 exception did not apply, the other exception under Art. 9 of the DPD—journalistic, artistic and literary purposes—may apply.[6] SNS and application providers, however, within a SNS environment would be considered to be 'data controllers' under the DPD. Perhaps, the main difficulty is being able to draw a clear boundary between individuals acting in their private capacity and those who adopt additional roles which may go beyond the private use exception in a SNS environment. It could be argued that private use is becoming more difficult for users who have two roles both in their professional and private capacity and that therefore, this provision becomes unworkable in practice. A further note to add is that the Art. 29 Working Party does not hold the view that images are unlikely to be sensitive data unless the data reveals sensitive data about the individuals.[7] It does, however, take the view

[4] Art. 29 Working Party (n 2).

[5] ibid 6.

[6] ibid.

[7] ibid.

that sensitive personal data[8] may be published with the express consent of the individual.

UK

The main provision that deals with the exception is s. 36 of the Data Protection Act 1998. Although it has slightly different wording from the DPD, the Information Commissioner's Office (ICO) has taken the view that social networking falls outside the scope of the UK DPA 1998. In 2007, there were relatively few complaints made against social networks[9] and it was not clear whether this could be due to the slow progress by SNS users or rather the mechanisms of complaints were easily resolved.

The case of *Applause Stores Production and Firsht v Raphael*[10] was the first case in the UK dealing with SNS and a fictitious profile. This was based primarily on a defamation claim and concerned an individual businessman who had found that the defendant (D) had posted a fake profile of the claimant and made defamatory remarks concerning his creditworthiness and his company on Facebook. This led to a court action resulting in an award for damages of £15,000 in libel damages and £2,000 for privacy damages.

In *Bryce v Barber*[11] the High Court had ruled that the claimant was entitled to damages of £10,000 for defamatory material posted on his Facebook profile, including an accusation that the claimant was a paedophile. Indeed, Rider argued that the widespread use and

[8] Sensitive data is defined as 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life'.

[9] Wong (n 1).

[10] [2008] EWHC 1781 (QB).

[11] *Bryce v Barber* (HC, 27 July 2010) unreported. See Deborah Rider, 'Social Networks: *Bryce v Barber*' (2010) 10(4) E-Commerce Law Reports 12-13. See also Ashley Hurst, 'Social Media and Reputation: When to Take Legal Action' (*Olswang*, 25 November 2010) and The Telegraph, 'Law Student Wins £10,000 after Being Branded a Paedophile on Facebook' *The Telegraph* (28 July 2010) <www.telegraph.co.uk/technology/facebook/7912731/Law-student-wins-10000-after-being-branded-a-paedophile-on-Facebook.html> accessed 14 November 2014.

availability of material posted on the internet could influence the amount of damages awarded by the courts.[12] Although this case was based on defamation, it could be argued that the information held on Facebook was inaccurate and could have been easily removed if a request was made directly to Facebook. However, this case does highlight the problems that may exist in an SNS with users posting information about others (X) which may portray them (X) in a different light.

In *J19 v Facebook Ireland*,[13] an interim injunction was discharged against Facebook for being imprecise and unclear and placed a disproportionate burden on Facebook to monitor all the content on the web pages it hosted. Facebook had published photographs and information about J without his permission describing J as a 'sectarian parade organiser' and a 'loyalist bigot'. Members of the public added further threatening comments on the website. An interim injunction was granted preventing Facebook from placing on its website photos of J, his name, address and personal details. Facebook removed the data and appealed successfully against the injunction. The court held that the injunction was not precise and J could seek further remedies from the court. There was insufficient evidence that J could establish a breach of Art. 2 ECHR. What this case indicates, however, is the relative ease with which information can be posted on Facebook. Although the claimant had used legal remedies (not under the DPA 1998) to remove this information, it further highlighted the need for SNS such as Facebook to act swiftly in removing information that is likely to be defamatory of an individual or reveal private information about an individual before it gets out of hand.

In July 2014,[14] the author requested information on the number of complaints that were made against SNS such as Facebook, Google, LinkedIn, Pipl, etc. Although the cases recorded date back to 2012, their enormous number (exceeding 100 since 2012) meant that it was not possible to evaluate all the data and, therefore, the statistics

[12] ibid (Rider).

[13] [2013] NIQB 113.

[14] Freedom Of Information Act (FOIA) request to the ICO (18 July 2014) (correspondence on file with the author).

date from 2014, the current year.[15] It should also be added that complaints raised were not only on the above complainants but included other organisations. The cases were categorised according the specific sector ('internet', 'retail', 'media', 'general'). Therefore, only cases dating since April 2014 were considered.

ICO

Organisations (April 2014 –August 2014)

Google	6
Facebook	4
LinkedIn	0
Pipl	0
Twitter	0
Other	67

As indicated above, the legal cases against social media have been very few, despite the focus in the academic literature.[16] However, when considering the concept of breach of privacy, the misuse of personal information or the law of confidence is used rather than the Data Protection Act 1998, where a direct complaint before the UK Information Commissioner or the rights provided under the UK DPA 1998 would be appropriate.

Finally, there is one further point to add in relation to the private purposes exemption. In response to the forthcoming Data Protection Regulation,[17] and in particular Art. 2 (material scope) on 'processing

[15] The number refers to the number of complaints made, but not whether there were valid grounds or the types of queries referred to.

[16] This is not an exhaustive list, but see Amedeo F Cappuccio, 'The Private Nature of Information' [2014] 2 IPQ 159 and Nicole A Moreham, 'Beyond Information: Physical Privacy in English Law' (2014) 73 CLJ 350—this is not to suggest that the privacy is not relevant, but that data protection is not considered or examined.

[17] ICO, *Proposed New EU General Data Protection Regulation: Article by Article Analysis Paper* (12 February 2013) <http://ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_

by a natural person without any gainful interest in the course of its own exclusively personal or household activity', the ICO took the view that in some contexts processing personal data for gainful interest could still be in the course of a person's exclusively personal or household activity, such as setting up a website to sell unwanted birthday presents.[18] According to the ICO, wording such as 'in pursuit of a commercial objective' could be non-personal.[19] The ICO further added that they did not agree with the *Lindqvist* decision,[20] but accepted that open publication of personal data may be a contributing factor when deciding whether or not the processing was done for personal or household purposes. The ICO preferred clearer guidelines from the law and found that it was becoming more difficult to decide whether processing was done for personal or household purposes.[21]

The ICO's position therefore highlights the problems with applying the personal or household purposes exception and the level of disagreement with the *Lindqvist* decision. It is not certain how the personal or household purposes will apply in practice after the Data Protection Regulation is passed, but it indicates some reservations which need to be cleared, if there is to be any user confidence and certainty in the Data Protection Regulation whether online or not.

Germany

In Germany, the Federal Data Protection Act 2009 (BDSG)[22] governs the processing of personal data by private bodies and federal public

reports/ico_proposed_dp_regulation_analysis_paper_20130212_pdf.ashx> accessed 14 November 2014.

[18] ibid 3.

[19] ibid 4.

[20] Case C-101/01 *Bodil Lindqvist v Kammaråklagaren (Public Prosecutor), Jönköpning* (OJ C 118, 24 April 2001).

[21] ibid.

[22] Took effect from 1 September 2009, s 1(2) of the Federal Data Protection Act 2009 (BDSG) outlines the scope—public bodies of the Federation; public bodies of the Lander (state) where it is not covered by Lander bodies; federal law or act as judiciary bodies and administrative matters are not involved and private bodies. (The full text of the BDSG is available at

bodies whilst each state's data protection laws ('Länder') govern the processing of personal data by state bodies.[23] The German Telemedia Act 2007 applies to data processed in the context of online activities. The view of the Berlin Data Protection Commissioner in 2007 was that whether SNS users would qualify as 'data controllers' depended on the degree to which the data could be accessible to others. For instance, a photo album held on the server of social network provide accessible only to a subscriber would benefit from the exemption for 'purely personal or household activities'.[24]

The Art. 29 Working Party has since published an opinion on social networking sites and how the DPD applies.[25] While some developments have emerged since 2007, it is important to consider the opinion noted above. For example, the opinion outlines when the household exception would apply and addresses the issue of sensitive data as applied to the data protection framework[26]

<www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile> accessed 14 November 2014). See Jörg Hladjk, 'Changes to German Data Protection Law' (2010) 10(5) Privacy and Data Protection 10; Jones Day, 'Germany Strengthens Data Protection Act, Introduces Data Breach Notification' Jones Day (October 2009) <www.jonesday.com/files/Publication/943821c6-517f-495f-a753-a2a5e2c519cd/Presentation/PublicationAttachment/7917f187-78e1-487f-b00e-a519e5a22c23/Germany%20Strengthens%20Data.pdf> accessed 14 November 2014. See also: Privacy International, 'Germany: Legal Framework' (*Privacy International*, October 2010) <www.privacyinternational.org/reports/germany/i-legal-framework> accessed 14 November 2014.

[23] For an in-depth study into the German Federal Data Protection Act, see Anne-Marie Zell, 'Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field' (2014) 15(3) German Law Journal 461; David Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (UNC Press 1992); Spiros Simitis, *Bundesdatenschutzgesetz* (7th edn, Nomos 2011 (in German)); Christopher Klug, 'Book Review: Spiros Simitis, *Bundesdatenschutzgesetz*' (2012) 2(2) International Data Privacy Law 113.

[24] Wong (n 1), and also Daniel B Garrie and others, 'Data Protection: The Challenges Facing Social Networking' (2010) 6 Brigham International Law and Management Review 127, 138.

[25] Art. 29 Working Party (n 2).

[26] ibid.

In 2008, the German Federal Commissioner of Berlin, co-sponsored by other Data Protection Authorities[27] issued an opinion on privacy protection on social networking sites, making several recommendations.[28] The main recommendations were: that social networking sites should respect privacy standards where they operate their services; users should be informed of the processing of their personal information on an SNS; users should be given control over their SNS profile; privacy friendly default settings should be provided to users; security standards should be adhered to by SNS providers; users should be given access and the option to delete their user profile; users should be given the option to use pseudonyms; providers should ensure that third parties to do not bulk download of user's data; and user's data should not be accessible on search engines without the user's express and informed consent.

In 2009, the German Federal Commissioner for Data Protection and Freedom of Information, Peter Schaar, took the view that social networking sites were poorly protected by privacy policies and that they were not onboard with protecting user's data. [29] He recommended that an independent consumer agency should be created to evaluate social networks and give grades on their privacy policies, letting users know which SNS protects them best.

Very recently, in 2013, the Schleswig-Holstein Privacy Commissioner[30] outlined some of the challenges surrounding social

---

[27] The co-sponsors were the French CNIL, Italian Data Protection Authority, Dutch Data Protection Authority, New Zealand Privacy Commissioner and Swiss Federal Data Protection Commissioner.

[28] 30th International Conference on Data Protection and Privacy Commissioners, 'Resolution on Privacy Protection in Social Network Services' (*BfDI*, 17 October 2008) <www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2008SocialNetwork.pdf?__blob=publicationFile> accessed 25 August 2014.

[29] Federal Commissioner for Data Protection and Freedom of Information, 'Data Protection Commissioner Warns over Social Networking Sites' (*BfDI*, 4 January 2010) <www.bfdi.bund.de/EN/PublicRelations/SpeechesAndInterviews/Artikel/271209ArtikelDeutscheWelle.html> accessed 25 August 2014.

[30] Thilo Weichert, 'Current Data Protection Challenges in Social Networks' (*Datenschutz Zentrum*, 19 November 2013)

networks and privacy arising from complaints about Google and Facebook and the application of German data protection laws, which are described below.[31]

In 2012, an informal group ('Dusseldorf Circle') of Data Protection Authorities within Germany examined the application of data protection laws to SNSs in Germany.[32] Although the resolution was not binding, it gave an insight on how German data protection laws would apply. According to Niemann, the application of German data protection laws to social networking sites had been quite controversial.[33] Providers outside the European Economic Area (EEA) were subject to the German data protection laws where personal data was collected by accessing users' data on computers in Germany. The German data protection laws would still apply to organisations unless it can be shown that it was established in a different country within the EEA. It emphasised that organisations could not circumvent the data protection rules by setting up an establishment in another EEA country, so some control over the SNS within the establishment had to be shown if it were to fall outside of German data protection rules. The German data protection rules continue to apply to organisations where data processing took place outside the EEA but where one EEA establishment could be identified as a data controller. The Dusseldorf Circle further pointed

<www.datenschutzzentrum.de/vortraege/20131119-weichert-data-protection-social-networks.html> accessed 14 November 2014.

[31] ibid.

[32] Fabirn Niemann, 'German Data Protection Authorities Broaden Application of German Data Protection Law to Foreign Social Networks and Attack the Use of Social Plugins and Fanpages' (*Mondaq*, 17 April 2012) <www.mondaq.com/x/170870/Social+Media/German+Data+Protection+Authorities+Broaden+Application+Of+German> accessed 14 November 2014; German Federal Data Protection Commissioner, 'Social Networking Resolution' (*BfDI*, 8 December 2011) <www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.html?nn=409242> accessed 25 August 2014. (See more on the Dusseldorf Group at <www.bfdi.bund.de/DE/Entschliessungen/entschlie%C3%9Fungen_node.html> accessed 25 August 2014, and the Dusseldorf Group Resolutions at <www.bfdi.bund.de/DE/Entschliessungen/DuesseldorferKreis/DKreis_node.html> accessed 25 August 2014.

[33] ibid (Niemann).

out that the use of social plugins (on sites such as Facebook and Google) or fanpages were responsible for safeguarding user's privacy. In particular, social plugins by German website providers would be illegal where they triggered the transfer of personal data to an SNS provider. Consent was required from the user before data could be collected using a social plugin. German websites should ensure they have knowledge of the use of social plugins in order to inform their users. Otherwise, the Dusseldorf Circle discourages the use of social plugins by German websites.[34] Although the scale of social plugin use on websites is generally unknown,[35] it is quite clear that there is some reservation expressed by the German Data Protection Authorities on the potential harm that can be caused by the transfer of personal data from websites onto SNS using this plugins.

In two separate legal developments the subject of Facebook was once again raised, primarily on the application of German data protection law and the extent to which users' data are protected in Germany.

The court in Schleswig-Holstein held that German data protection laws did not apply to Facebook because its headquarters were in Ireland.[36] The case concerned a decision by the Schleswig-Holstein Data Protection Authority (ULD), when it issued its policy against Facebook for not allowing users to use pseudonyms on the social

[34] ibid.

[35] Facebook, 'Social Plugins and Your Privacy' <https://en-gb.facebook.com/help/340599879348142/> accessed 25 August 2014.

[36] Carlo Piltz, '*Facebook Ireland Ltd/Facebook Inc v Independent Data Protection Authority of Schleswig-Holstein, Germany*—Facebook is Not Subject to German Data Protection Law' (2013) 3(3) International Data Privacy Law 210; Schleswig-Holstein Data Protection Authority, 'OVG Schleswig-Holstein: For Facebook, German Data Protection Laws Do Not Apply' (*Datenschutz Zentrum*, 24 March 2013) <www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg-en.htm> accessed 14 November 2014; Natasha Lomas, 'Facebook Wins Court Challenge in Germany Against Its Real Name Policy' (*TechCrunch*, 15 February 2013) <http://techcrunch.com/2013/02/15/facebook-wins-court-challenge-in-germany-against-its-real-names-policy/> accessed 14 November 2014; Louise Osborne, 'German State Fights Facebook over Alleged Privacy Violations' *The Guardian* (London, 4 January 2013) <www.theguardian.com/world/2013/jan/04/facebook-germany-data-protection> accessed 14 November 2014.

networking site based on s. 13(6) of the Telemedia Act,[37] contending that it eroded user's online freedom.

By contrast, the High Court of Berlin ruled in 2014 that Facebook was subject to data protection laws. In this case, the German Consumer Organisation (VZBV) had brought a claim against Facebook for breaching German consumer laws by sending emails without user's consent.[38] The tool used was the Facebook 'Friend Finder'. Users who agreed with Facebook terms and conditions would give permission to Facebook search through contact details and send user's friends invites, if they had not registered with Facebook. Agreeing with the terms and conditions also meant that the data could be shared with third parties. The High Court of Berlin held that users were not informed. Facebook had not complied with the data protection laws when using non-user's data to distribute advertising material.[39] The key issue was whether German laws applied or whether the Irish Data Protection law applied. According to the Berlin Court, Facebook—an American based business—was responsible for the processing and there was very little evidence provided that the data was being handled by the Irish headquarters.

[37] s 13(6) of the German Telemedia Act states that providers of Telemedia Services (including websites) are required to provide users with the opportunity to remain anonymous or use a pseudonym while using a regulated service. For further analysis, see Marcus Schreibauer and Jan Spittka, 'German Court Holds Presence of Irish Subsidiary Precludes Application of German Data Protection Law to Facebook' (*Hogan Lovells*, 1 March 2013) <www.hldataprotection.com/2013/03/articles/consumer-privacy/german-court-holds-presence-of-irish-subsidiary-precludes-application-of-german-data-protection-law-to-facebook/> accessed 14 November 2014; Henning Krieg, 'German Telemedia Act Introduces New Rules for New Media' (*Bird & Bird*, 5 March 2007) <www.twobirds.com/en/news/articles/2007/german-tele-media-act-new-rules> accessed 14 November 2014; and Centre for German Legal Information, 'German Telemedia Act 2007 (English Translation)' (*CGerLI*, 26 February 2007) <www.cgerli.org/fileadmin/user_upload/interne_Dokumente/Legislation/Telemedia_Act__TMA_.pdf> accessed 14 November 2014.

[38] Out-Law News, 'Facebook Subject to Data Protection Rules, says Berlin Court' (*Out-Law News*, 26 February 2014) <www.out-law.com/en/articles/2014/february/facebook-subject-to-german-data-protection-rules-says-berlin-court/> accessed 14 November 2014.

[39] ibid.

It centred on the application of Art. 4(1)(c) whereby if equipment was used in Germany, then it would fall within the German Federal Data Protection Act. Cookies were installed on the devices of German users and, therefore, the Berlin Court held that the German Federal Data Protection Act applied. It is not clear whether an appeal would be lodged before the German Supreme Court.[40]

Finally, one further legal development is a further appeal which was decided on the 4th September by the German Administrative court by the Schleswig-Holstein Data Protection Authority against Facebook on the use of pseudonyms following the Berlin Court ruling. The German Administration Court delivered its judgment and it was decided that Facebook fan operators are not regarded as data controllers as they are not responsible for the technical and legal aspects of Facebook. It is not clear whether the ULD will appeal against this decision, but it is likely to heighten tensions between the Data Protection Authorities of Germany and Ireland, and it is not clear why the German Court did not make a preliminary ruling reference directly to the Court of Justice of the European Union (CJEU) on this point as it raises a significant issue in terms of how the Data Protection Directive is applied.[41]

Although the issue of social networking and the individual as a 'data controller' was not considered to any extent, these recent case developments serve as an example of the nature and complexity of SNSs in Germany and highlight the difficulties in terms of the practical application of data protection rules to an SNS located within the EU but outside the EU Member States.

---

[40] ibid.

[41] Many thanks for the Schleswig-Holstein Data Protection Authority (ULD) for guidance on this (on file with the author, dated 29 August 2014). See also John O'Connor, 'German Court Ruling on Facebook's Personal Data Gives Legal Certainty to Irish Data Controllers' (*Lexology*, 12 September 2014) <www.lexology.com/library/detail.aspx?g=a0fa6f1a-32b8-4bc4-b980-ecf86a1d9eb9> accessed 14 November 2014; and ULD, 'OVG Judgment on Facebook Fan Pages in Need of Revision' (*Datenschutz Zentrum*, 29 September 2014 <www.datenschutzzentrum.de/artikel/770-ULD-OVG-Urteil-zu-Facebook-Fanpages-revisionsbeduerftig.html> accessed 14 November 2014.

Sweden

The Swedish Personal Data Act 1998 governs the protection of personal data within Sweden and was recently amended in 2007 to include the misuse-orientated approach.[42] This means that data that is unstructured would fall outside the scope of the Swedish Personal Data Act. The guidelines provided by the Swedish data inspectorate provide that processing of data in unstructured material such as email messages or texts published on the internet would be exempted and should not offend individuals ('violation of the integrity' of the individual), such as breaching confidentiality, defaming an individual or compiling information about an individual for no specific reason.[43] As this is exempted in Sweden, it is different from the EU approach on Data Protection whereby all forms of data processing fall within the scope of the Data Protection Directive unless the exemptions under Art. 3(2) processing (for private household purposes) or Art. 9 (artistic, journalistic and literary requirements) apply.[44] It further decriminalises breaches of data security through mere negligence, though gross negligence could still fall within the Swedish Personal Data Act.

Swedish Study into Social Networking 2011

The Swedish Data Inspectorate Board carried out a study on social networking sites in 2011, primarily focusing on young people's attitudes towards privacy. The sample group included youth between the ages of 15-18 (N=522).[45] What follows is a summary of some of

[42] Swedish Personal Data Act Amendments 2007, SFS 2006:398.

[43] Swedish Data Inspectorate, *Personal Data Protection* (4th revised edn, Swedish Ministry of Justice 2006) 14 <www.regeringen.se/content/1/c6/07/43/63/0ea2c0eb.pdf> accessed 14 November 2014.

[44] For a background into the misuse-orientated approach, see Sören Öman, 'Trends in Data Protection Law' (2010) 56 Scandinavian Studies in Law 209, <www.sorenoman.se/documents/2769.pdf> accessed 14 November 2014.

[45] Kairos Future/Swedish Data Inspection Board, 'Young People and Privacy 2011' (*Swedish Data Inspection Board*, January 2011) <www.datainspektionen.se/Documents/rapport-young-people-and-privacy-2011.pdf> accessed 26 August 2014.

the findings. Given the limited nature of this paper, only the salient points on social networking are considered.[46] The study found that more and more young people were using SNSs and the most widely used was Facebook.[47]

The information that young people considered 'private' included, but were not limited to: who they were 'in love with', their personal finances and where they lived. Political opinion and religious beliefs were thought to be less sensitive.[48] Similarly, information about which school they attended, or the town or country they came from, were less sensitive. In 2010, over 90% surveyed had posted photos of themselves online, almost 50% had uploaded videos of themselves and almost 90% had written comments about themselves with their names attached. In terms of awareness, over 60% surveyed had thought about privacy issues and how they handle private information and approximately 40% avoided writing certain things online that would cause problems later in life.[49]

[46] Please note that the author does not represent the views of the Swedish Data Protection Inspectorate Board and the results are used in the context of this study into social networking and the application of the Data Protection Directive and relevant data protection laws.

[47] Swedish Data Inspection Board (n 43) 3.

[48] ibid.

[49] Ibid 7.

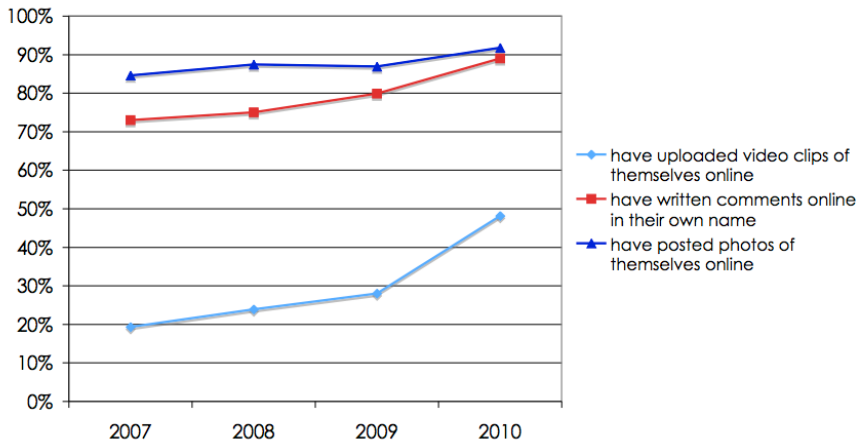


Figure 2. Risky behaviour on the Internet is increasing.

Developments in technology and the growth of online communities where people can share information about themselves give a lot of pleasure to many young people. At the same time this rapid development has major consequences for the ability to maintain privacy. The proportion of young people who say they have at some time regretted posting information about themselves online has risen since the last survey.

Figure 1: Risky behaviour on the internet

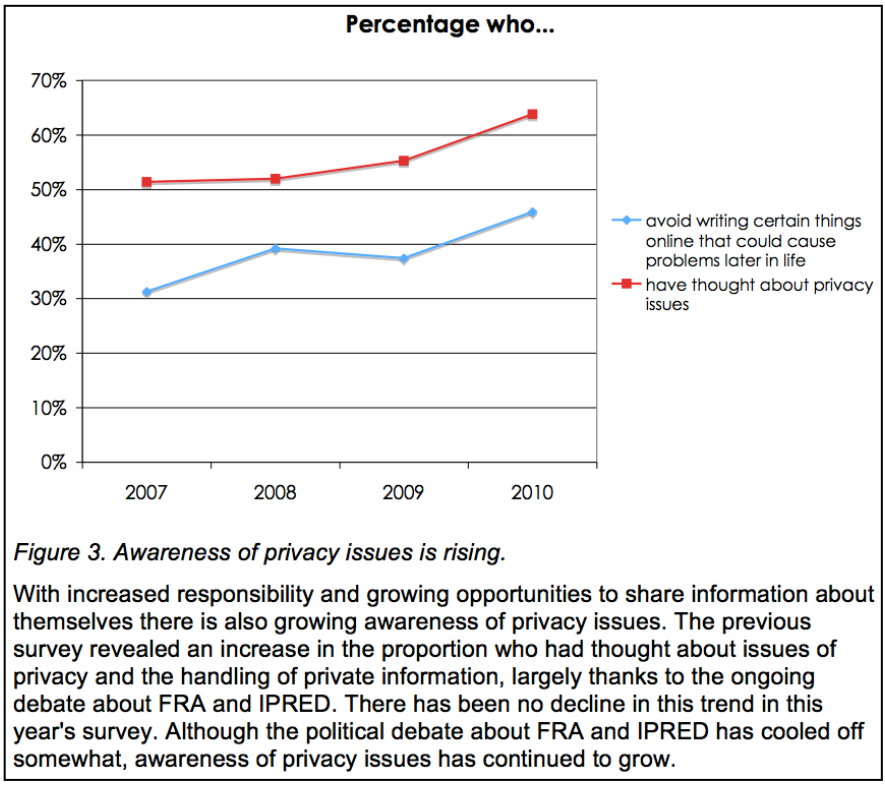


Figure 2: Awareness of privacy issues

FACEBOOK BY FAR THE MOST POPULAR SOCIAL NETWORK

The trend that is perhaps most likely to affect young people's attitudes to privacy is the growth of different types of social networks online. Figure 6 below shows the social networks that most young people belong to or visit once a week or more often.

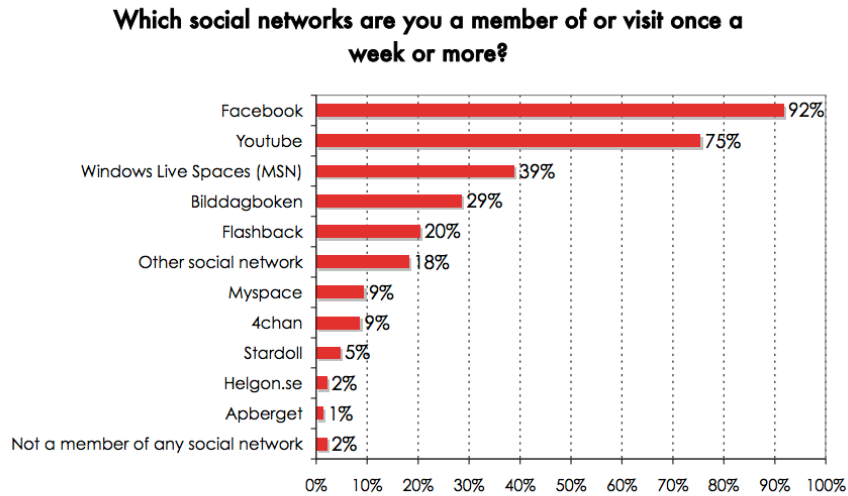
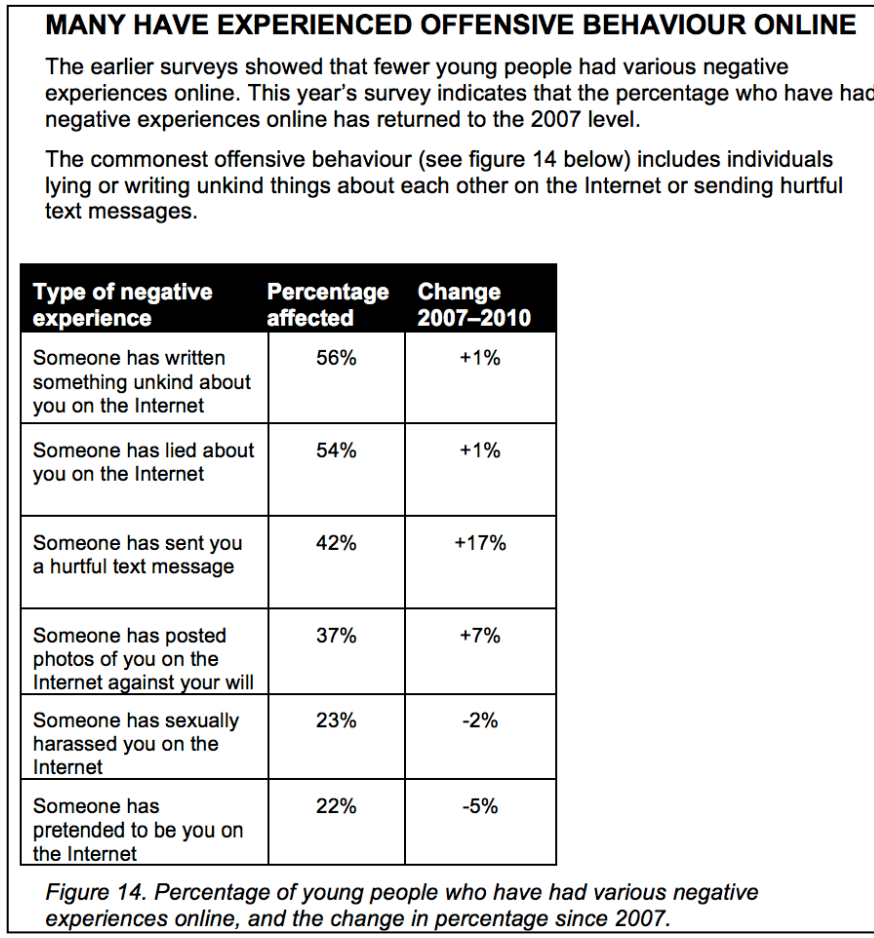


Figure 6. Percentage of young people who are members or visit various social networks once a week or more often.

Figure 3: Most used Social Networks

In terms of the most frequent use of SNSs, 92% surveyed were using Facebook more than once a week, whilst 75% were using Youtube.[50]

[50] ibid 10.



MANY HAVE EXPERIENCED OFFENSIVE BEHAVIOUR ONLINE

The earlier surveys showed that fewer young people had various negative experiences online. This year's survey indicates that the percentage who have had negative experiences online has returned to the 2007 level.

The commonest offensive behaviour (see figure 14 below) includes individuals lying or writing unkind things about each other on the Internet or sending hurtful text messages.

Type of negative experience	Percentage affected	Change 2007–2010
Someone has written something unkind about you on the Internet	56%	+1%
Someone has lied about you on the Internet	54%	+1%
Someone has sent you a hurtful text message	42%	+17%
Someone has posted photos of you on the Internet against your will	37%	+7%
Someone has sexually harassed you on the Internet	23%	-2%
Someone has pretended to be you on the Internet	22%	-5%

Figure 14. Percentage of young people who have had various negative experiences online, and the change in percentage since 2007.

Figure 4: Negative experiences online

In terms of negative experiences online, the survey found that the most common offensive behaviour was writing unkind things about each other on the internet. About 56% surveyed had experienced this. About half who were surveyed had experienced 'Facebook rape' where their Facebook had been hijacked by someone writing entries on their Facebook, whether harmless or not.[51]

[51] Ibid 17.

In terms of complaints procedure, 31% of complainants had ultimately won the removal of words, videos, and photos from the network, and 26% have had someone banned from the SNS.

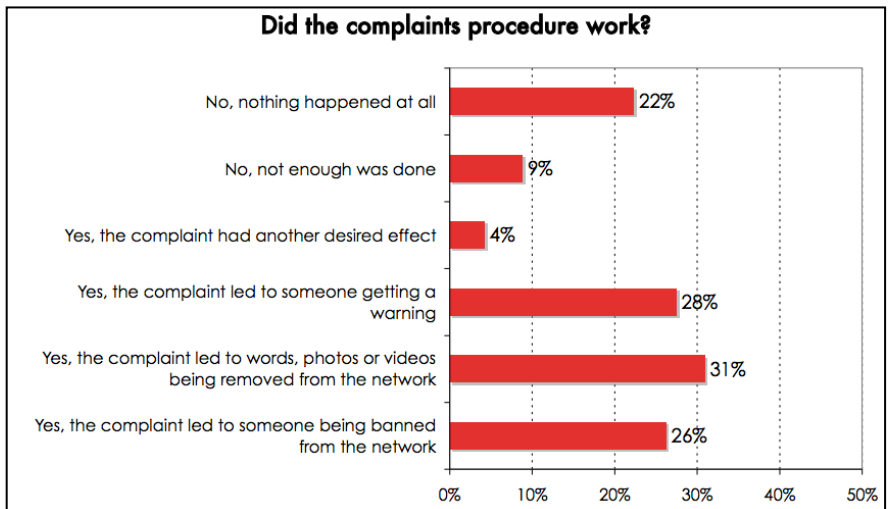


Figure 15. Percentage who feel that the complaints procedure works or does not work. More than one answer can be chosen, so the bars do not add up to 100%.

Complaints appear to be fairly effective (see Figure 15 above). In the previous study, the proportion who felt that nothing happened was lower, but the question was worded slightly differently. In general, the complaints procedure still has the desired effect, but may not always be as effective as desired.

Figure 5: Complaints procedure

VIEWS ON SENSITIVE INFORMATION REMAIN THE SAME

While previous sections have shown that significant changes in behaviour and attitudes have taken place over time, young people's views on what constitutes sensitive information are relatively unchanged.

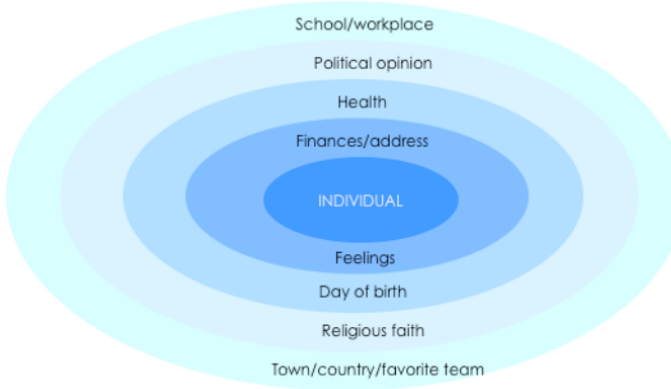


Figure 7. The private sphere for young people in 2010. The most sensitive information is closest to the centre.

The information young people consider most private is who they are in love with, their financial situation and, increasingly, where they live. Roughly a third of young people would consider disclosing this information to someone else. Around half would be willing to reveal information on health, their date of birth and political leaning. A large majority are willing to tell others about their favourite team, their religious faith, which school they go to or where they work, and what town or country they come from.

Figure 6: The private sphere for young people in 2010

The overall conclusion from the study was that although the sample was small, young people were presented with new communication opportunities which challenged them in how they should share and access information.[52]

[52] ibid 23. To date, other than the 2011 study, there have not been any recent studies carried out on SNSs.

Facebook

One significant development occurred in 2011, when the Nordic Data Protection Authority produced a case study into Facebook following a complaint made by the Norwegian Consumer Council.[53] This led to the Nordic Data Protection Authorities carrying out an investigation into the workings of Facebook, with specific focus on data protection issues. This is significant because the Swedish Data Inspection Board later submitted questions to Facebook, following the case study with the Nordic Data Protection Authority. The main findings from the study are as follows.

The study found that the privacy policy and statement of rights and responsibilities were wide. The wording of the clauses were vague and difficult to understand and, in particular, when processing user's IP addresses and tracking what web pages users see, they found that the scope of the policy did not result in effective outcomes. Additionally, the study found a lack of transparency regarding privacy procedures. For example, it was noted that by adding information to the personal profile, a user received an increase in customised adverts.[54] The use of social plugins generated more information about Facebook users when they are logged in and logged out and is relevant in the context of IP addresses. Information collected from non-users came from 'friend finder' and social plugins.[55]

The results of the study, however, led to more questions from the Nordic Data Protection Authorities directed towards Facebook on how Facebook works.[56] The questions focus on: who gains access or

[53] Atle Årnes, Jørgen Skorstad and Lars-Henrik Paarup Michelsen, 'Social Network Services and Privacy: A Case Study of Facebook' (*Persónuvernd*, 15 April 2011) <www.personuvernd.is/media/frettir/Microsoft-Word---11-00643-5-Part-I---Rapport_Facebook_2011-_april-2011_.pdf> accessed 14 November 2014; and Out-Law News, 'Norwegian Consumer Group Calls for Tighter Facebook Regulation' (*Out-Law News*, 2 June 2010) <www.out-law.com/page-11073> accessed 14 November 2014.

[54] ibid 4 (Årnes, Skorstad and Michelsen).

[55] ibid.

[56] 44 questions were raised to Facebook by the Nordic Data Protection Authorities (the Norwegian Data Inspectorate on behalf of: Norway, Sweden, Denmark (including the Faroe Islands), and Finland (including Åland)), see the Norwegian

collects personal information; what happens to the collection of personal data; what are the attitudes towards members' privacy settings; how much control does Facebook allow its members to have over these settings; and to what extent do Facebook or third parties allow users to change or reset settings on their Facebook profile. Facebook replied by writing that the user's name, email address and birth date were not public information and not shared with other business; however, an individual may grant access to the data when he or she added a third party application. When a person joins Facebook, his or her name, profile picture, networks, user ID and username are made publicly available and shared with Facebook trusted partners who have entered a contract with Facebook to provide instant personalisation services. No additional sharing of information in an indirect manner is provided.[57]

Facebook also gave the following reply in relation to the posting of information. A user who posts information on their Facebook profile ('wall') determines the scope of the audience for that piece of information. The contents of some of the posts are used by Facebook in their advertising of other promotional products. Facebook expressly mentioned that it did not share the content of user wall posts with other businesses and that users chose to share the content when they added a third party application. Users would decide what information was to be added to his or her profile—beyond the basic information. All information that the user chooses to add helps target better advertisements. In essence, Facebook argued that what personal data and information is made public is a matter of personal choice—a choice made by the user of the account. Indeed, in its

---

Data Protection Authority, 'What Happens with Personal Information in Facebook' (Norwegian Data Protection Authority, 18 January 2012) <www.datatilsynet.no/Global/english/Personal_information_Facebook.pdf> accessed 14 November 2014; and Norwegian Data Inspectorate, 'Social Network Services and Privacy' (Norwegian Data Protection Authority, 7 July 2011) <www.datatilsynet.no/Global/english/11_00643_5_Part_II_Questions_Facebook_DPA.pdf> accessed 14 November 2014.

[57] Letter from Richard Allan, Facebook's Director of Policy for Europe, Africa, and Middle East to Bjorn-Erik Thon, Director of the Data Inspectorate of Norway (September 2011) <www.datatilsynet.no/Global/english/Facebook_questions_answere2011.pdf> accessed 14 November 2014.

privacy policy, Facebook indicated that as this was a free service covering over 750 million users, to keep the service free it would show advertisements to users. Users have a contract with Facebook Ireland as a 'data controller' for the purposes of the DPD.[58]

On the question of IP addresses, Facebook adds that an impression log is created for all visits to a webpage. Facebook's policy would be to delete unique impression logs after 90 days. Facebook does not consider 90 days to be excessive and argues that such practices are in line with that of other websites. For instances, Facebook noted that they temporarily store unique impression logs which include IP addresses. The purpose of temporarily storing the impression logs, including IP addresses, is to monitor the technical performance of the 'like' button and to detect problems across particular networks. Facebook uses IP addresses to investigate security threats such as a denial of services attack. Facebook further adds that it does not automatically tag photos and that a user could disable the tagging feature on their privacy settings if he or she preferred.

Following the response, the details of Facebook were conveyed to the Irish Data Protection Commissioner to consider, as Facebook headquarters are based in Ireland and, therefore, Irish data protection laws apply. A response by the Norwegian Data Protection Authority was later written to the Consumer Council following their complaint.[59]

In a recent Norwegian case, a shopkeeper who had been recently robbed published on Facebook video surveillance footage of those who had committed the crime. The Norwegian Data Protection Authority considered this to be a violation of the Norwegian Data Protection Act and fined the shopkeeper. This received widespread coverage in the Norwegian Press.[60]

A second case concerned the publication of pictures and comments by an individual on Facebook. The issue centred on the right to speak freely on the internet and privacy. The Norwegian Data

[58] ibid.

[59] Grateful acknowledgements to the Norwegian Data Protection Authority for this information (on file with author, 27 August 2014).

[60] ibid. Case ref: 14/00538.

Protection Authority took the view that this was not a case of free speech and recommended that the data subject use 'delete me' for help or information to be deleted.[61]

In Sweden, the data inspectorate carried out a series of audits on Swedish organisations on the collection of personal information through Facebook.[62] Although this was not concerned with the processing operations of Facebook, the Swedish Data Inspectorate Board has since issued guidelines when processing personal information in Sweden.[63]

The developments that have emerged are similar to the German approach in terms of the application of the Nordic laws (if any) to SNSs. Whilst the DPD is expressly clear about Art. 4(1)(a) and the need for an 'establishment' before the data protection laws apply to the data controller, the approach from the Swedish Data Inspectorate is more focussed on the protection of the 'integrity' of the individual and, unless the data causes harm to the individual (misuse-orientated approach), the data protection laws do not apply.

---

[61] Case ref: 14/00888. See also 'Delete Me' website at <https://slettmeg.no> accessed 14 November, which was originally an initiative by the Norwegian Data Protection Authority and then moved to NorSIS <www.norsis.no> accessed 14 November 2014. According to the website, 'Slettmeg.no offers advice and guidance to people of all ages who find offending material about themselves on the internet. Offending material might be photos published without permission, fake profiles on different internet services, incorrect personal information or harassment. People who have published this information themselves, but regret it and want this information removed, may also get in touch with slettmeg.no for support.' Grateful acknowledgements to the Norwegian Data Protection Authority for this information (on file with the author, 27 August 2014).

[62] Årnes, Skorstad and Michelsen (n 53) 34.

[63] Swedish Data Inspection Board, 'Datainspektionen Granskar hur Facebook Anvands [Data Inspectorate Examines how Facebook is Used]' (*Swedish Data Inspection Board*, 26 March 2013) <www.datainspektionen.se/press/nyheter/2013/datainspektionen-granskar-hur-facebook-anvands/> accessed 14 November 2014; and 'Personuppgifter I Sociala Medier [Personal Information in Social Media]' (*Swedish Data Inspection Board*, May 2014) <www.datainspektionen.se/Documents/faktablad-sociala-medier.pdf> accessed 26 August 2014. See also Swedish Data Inspection Board, 'Frivilligt Integritets Skydd pa Internet [Voluntary Protection of Privacy on the Internet]' (*Swedish Data Inspection Board*, 1999) <http://bestall.datainspektionen.se/rapporter/frivilligt-integritetsskydd-pa-internet-beskrivning> accessed 26 August 2014.

Following a query to the Swedish Data Inspectorate, the author found that there was no record of statistics made on the number of complaints against Facebook, Google and other SNS. There is one case where an individual had posted naked pictures of other individuals on Instagram and this was reported to the Swedish Data Inspectorate leading to court action and resulted in fines to the individual.[64] Otherwise, there have been very few cases on the individual as a 'data controller'.

The studies carried out by the Swedish Data Inspectorate show increasing awareness of young people towards SNSs, particularly on the harmful effects that could result from putting information online. Although the study was carried out in 2011, it remains to be seen whether the mechanisms of the Swedish Personal Data Act and technical mechanisms online via internet browsers can safely protect users' personal information.

Google and the Right to be Forgotten

The key issue is to consider the extent to which individuals can erase data held on a public profile online, so whilst the recent CJEU's judgment deals with Google, it would be useful to see how this may apply to 'people search engines' that hold profiles of individuals publicly.

Whilst the principle of the right to be forgotten has received widespread academic attention—in regard to the applicability of the principle and how it will work in practice—the judgment dating back to May 2014 not only clarifies the application of the DPD to the internet, but the extent to which online users could request that information about themselves is removed.[65]

---

[64] Many thanks to the Swedish Data Inspectorate Authority for this information (on file with the author, 29 August 2014).

[65] Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD)* (OJ C 212/4, 13 May 2014). See elsewhere in this issue: Gloria González Fuster, 'Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) 2(2) Birkbeck Law Review 263. See also Meg Leta Ambrose, 'It's About Time: Privacy, Information Cycles and the Right to be Forgotten' (2013) 16 Stanford

By way of background, the applicant brought legal action against Google, requesting that search engine results about him from two printed issues in 1998 be removed.[66] One indicated that his property had been repossessed. The question on the application of the DPD to the internet was referred to the CJEU in an Art. 267 preliminary ruling reference by the Spanish Court. The CJEU gave its interpretation in May 2014. It held that the search engine operator had 'collected' data within Art. 2(b) of the DPD. The operator had 'retrieved', 'recorded' and 'organised' the data in question. Furthermore, the CJEU held that the operator was a 'data controller' within Art. 2(d) of the DPD and that it had to comply with the requirements with the DPD. As Google Spain was a subsidiary of Google Inc., on Spanish territory, it fell within the definition of an 'establishment' within Art. 4(1)(a). It was further noted that the right to be forgotten was not absolute and that it had to be balanced against other fundamental rights such as freedom of expression. What was interesting about the judgement was the responsibility of the search engine where it was held to be required to remove links to a web page published by third parties which contained information of a person from a list of results that were displayed after a search was made against a person's name online. The implications of this judgment are significant because they impose far-reaching implications—consequences for the extent to which information displayed by a search engine could or could not be accessible.

Following the judgement, Google received more than 12,000 requests to remove links within 24 hours.[67] As this judgement was

Technology Law Review 369; Jonathan Zittrain, 'Don't Force Google to "Forget"' *The New York Times* (New York, 14 May 2014) <www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0#> accessed 14 November 2014; Jef Ausloos, 'The "Right to be Forgotten"—Worth Remembering?' (2012) 28(2) CLSR 143; Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to be Forgotten" in Big Data Practice' (2011) 8(3) SCRIPT 229; Norberto Nuno Gomes de Andrade, 'Oblivion: The Right to be Different from Oneself—Reproposing the Right to be Forgotten' (1 February 2012) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033155> accessed 14 November 2014.

[66] ibid (*Google*).

[67] Samuel Gibbs, 'Google Hauled in by Europe over "Right to be Forgotten" Reaction' *The Guardian* (London, 24 July 2014)

likely to impact other search engines, Yahoo and Microsoft both indicated that they were reviewing their policies on displaying search engine results following the CJEU judgment.[68]

Recently, the United Kingdom House of Lords EU sub-committee has indicated that the CJEU judgement on Google was wrong and that the new Data Protection Regulation needed to invalidate the CJEU judgment. The House of Lords EU sub-committee took the view that the judgment was flawed. According to Baroness Prashar, 'we do not believe that individuals should have a right to have links to accurate and lawfully available information about them removed, simply because they do not like what is said.'[69] In its overall conclusion, the House of Lords Sub-committee took the view that the 1995 Directive and the CJEU's interpretation of the Directive 'reflected the current state of communications where global access to detailed personal information had become part of the way of life.'[70] It was not reasonable to allow data subjects to remove links to data where this was accurate or lawfully available. The right to be forgotten should be removed as it was misguided and unworkable in practice. The definition of a 'data controller' under the Data Protection Regulation needed to be amended to clarify that the term did not include ordinary users of search engines and that search engines should not be categorised as 'data controllers'.[71]

Whilst the CJEU has clarified the extent to which the DPD applies to search engines and precedes the Data Protection Regulation, the

<www.theguardian.com/technology/2014/jul/24/google-hauled-in-by-europe-over-right-to-be-forgotten-reaction> accessed 14 November 2014.

[68] Sam Schechner, 'Google Starts Removing Search Results under Europe's Right to be Forgotten' *The Wall Street Journal* (New York, 26 June 2014) <http://online.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023> accessed 14 November 2014.

[69] Liat Clark, 'Lords: Right to be Forgotten is Wrong, Unworkable and Unreasonable (*Wired*, 31 July 2014) <www.wired.co.uk/news/archive/2014-07/30/right-to-be-forgotten-is-wrong> accessed 14 November 2014. See also House of Lords European Union Committee, *EU Data Protection Law: A Right to be Forgotten?* (HL 2014-15, 40) <www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf> accessed 14 November 2014.

[70] ibid paras 60-65.

[71] ibid.

repercussions of this judgment are likely to impact search engine results where data can be easily displayed against the search of a name and linked to information to the individual if it is not accurate. It is not clear yet whether requests are likely to be made to search engines that are aimed at finding individuals, but the Google judgment is likely to be far-reaching and therefore the interpretation and application under the DPD and national data protection laws will be watched with much scrutiny by users and those likely to be affected by the CJEU judgment.

In a separate action, Max Schrems, an Austrian lawyer, has brought a case against Facebook following the Irish Data Protection Commissioner's investigation into Facebook.[72] This is a separate case and was commenced as the claimant did not completely agree with the previous outcomes reached by the Irish Data Protection Commissioner on Facebook. The main complaint, however, is with Facebook and whether it transferred data to the US. Schrems contended that by 'transferring user data to the United States, Facebook Ireland was facilitating the processing of such data by Facebook itself' and that 'While Facebook has self-certified by reference to the Safe Harbour principles.' Schrems further argued that there was 'no meaningful protection in US law or practice in respect of data so transferred so far as state surveillance was concerned.' Further still, Schrems maintained that

> the US law enforcement agencies could obtain access to such data without the need for a court order, or, at least, a court order showing probable cause that a particular data subject had engaged in illegal activities or stood possessed

[72] *Schrems v Data Protection Commissioner* [2014] IEHC 310; [2014] 3 CMLR 37 (text freely available at <www.europe-v-facebook.org/hcj.pdf> accessed 14 November 2014). See also The Guardian, 'Lawyer Suing Facebook Overwhelmed with Support Available' *The Guardian* (London, 6 August 2014) <www.theguardian.com/technology/2014/aug/06/facebook-privacy-action-austria-max-schrems> accessed 14 November 2014; and Bryan Cronan, 'Facebook Sued by Law Student Max Schrems for Privacy Violations' (*The Christian Science Monitor*, 1 August 2014) <www.csmonitor.com/Business/2014/0801/Facebook-sued-by-law-student-Max-Schrems-for-privacy-violations> accessed 14 November 2014.

> of information which would be of genuine interest to law enforcement bodies.[73]

In deciding the case, the Irish Court has referred certain questions to the CJEU. The main questions are as follows:

> Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?[74]

Although the judgment is likely to take at least another year before it is resolved, the High Court of Ireland was clear in noting that it was critical, when interpreting the DPD and the 2000 Commission decision on Safe Harbor, to re-examine this in the light of Art. 8 of the ECHR Charter and whether the 2000 Commission decision should be disregarded—which is why Art. 267 TFEU was crucial.[75] The implications of this case are likely to impact social networking and how information is held or transferred.

---

[73] ibid *Schrems* [29].

[74] ibid [71].

[75] Europe versus Facebook, 'European Court of Justice will decide over Facebook/Prism' (*Europe versus Facebook*, 18 June 2014) <www.europe-v-facebook.org/PRISM_pa_en.pdf> accessed 14 November 2014.

Conclusion

This paper began with an analysis of legal developments on SNSs since 2007 in the UK, Germany, Sweden and Norway (limited extent), and the application of Art. 3(2) of the DPD on private purposes and household exception. What can be identified is that there are different approaches adopted by the jurisdictions examined on the application of data protection rules to social media. This paper therefore contributed to the wider literature by considering the responses by the UK, German, Swedish and Norwegian Data Protection Authorities to recent developments.

Take, for instance, the UK ICO's profound disagreement with the scope of the forthcoming Data Protection Regulation and the CJEU's decision in *Lindqvist*, whilst other jurisdictions such as Germany and Norway have had to consider whether the data protection rules apply to Facebook and whether users' data were sufficiently protected. In Sweden, the attitudes of young people to social media in a recent study in 2011 revealed an increasing awareness amongst young people, but also challenges that these technologies presented on protecting privacy and how information is provided on social media sites. The legal remedies, however, still remain unclear. Furthermore, the approaches of different jurisdictions to the issue of data protection in social media are far from consistent.

This is further complicated by the recent CJEU judgment on Google to allow users to erase data on Google search engine results, yet the application and implication of the CJEU's judgment remains unclear.[76]

What is needed is further reinforcement and guidance on a) application or non-application of data protection rules to social media, b) when the rights to erase data could apply to people search engines as well as search engine results in general, c) academic and practitioner discussion into data protection rules online beyond the discussion on the aspects of 'privacy', and d) discussion on the

[76] As is further discussed in Gloria González Fuster's contribution to this issue. Gloria González Fuster, 'Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) 2(2) Birkbeck Law Review 263.

private and public spheres of social media and reasonable expectations for privacy online.

The forthcoming Data Protection Regulation is likely to be passed in 2015, if there are no further obstacles at EU level. The regulation would have to be applied uniformly and the renamed European Data Protection Board (ex Art. 29 Working Party) may need to revisit the guidelines it issued in 2009 on social media in light of the Data Protection Regulation to make clear when an SNS user could exercise their rights and have data removed without recourse to litigation which can be time-consuming and costly. Only then can there be confidence in the use of social media that respects the privacy rights of users.

The case of *Schrems*[77] is likely to propel the issue of social media into the spotlight and the CJEU's judgment will bring further insight and clarity on how the data protection rules will apply to social media and whether the current DPD will provide sufficient legal remedies (other than the Data Protection Regulation) to address privacy issues online. The application of the DPD, the protection of the user's privacy on social media is unlikely to go away and the aim of this paper is to raise awareness of how the legal developments have evolved since 2007 and consider what boundaries (if any) should be drawn to protect users' expectation of privacy online.

[77] *Schrems* (n 72).