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

Document type  Report / Conference level paper
Title  D6.3 - Guidelines for privacy-friendly default settings
Work Package  W6
Deliverable Number  D6.3
Editor(s)  J. Ausloos, KU Leuven
Dissemination level  Reviewer
Preparation date  21. December 2012
Version  1.0

Legal Notice
All information included in this document is subject to change without notice. The Members of the IWT SBO SPION project make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IWT SBO SPION project shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.
The IWT SBO SPION Project

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Participant name</th>
<th>Country</th>
<th>Department</th>
<th>Participant role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KU Leuven</td>
<td>BE</td>
<td>COSIC/ESAT</td>
<td>Coordinator</td>
</tr>
<tr>
<td>2</td>
<td>KU Leuven</td>
<td>BE</td>
<td>DISTRINET</td>
<td>Partner</td>
</tr>
<tr>
<td>3</td>
<td>KU Leuven</td>
<td>BE</td>
<td>DTAI</td>
<td>Partner</td>
</tr>
<tr>
<td>4</td>
<td>KU Leuven</td>
<td>BE</td>
<td>ICRI</td>
<td>Partner</td>
</tr>
<tr>
<td>5</td>
<td>Vrije Universiteit Brussel</td>
<td>BE</td>
<td>SMIT</td>
<td>Partner</td>
</tr>
<tr>
<td>6</td>
<td>University of Ghent</td>
<td>BE</td>
<td>OWK</td>
<td>Partner</td>
</tr>
<tr>
<td>7</td>
<td>Carnegie Melon University</td>
<td>USA</td>
<td>Heinz</td>
<td>Partner</td>
</tr>
</tbody>
</table>

Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Jef Ausloos (Author)</td>
<td>KU Leuven, ICRI</td>
</tr>
<tr>
<td>2  Eva Lievens (Co-Promotor)</td>
<td>KU Leuven, ICRI</td>
</tr>
<tr>
<td>3  Els Kindt (Supervisor)</td>
<td>KU Leuven, ICRI</td>
</tr>
<tr>
<td>4  Jos Dumortier (Promotor)</td>
<td>KU Leuven, ICRI</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction......................................................................................................................4

2. What are Default Settings?...............................................................................................5
   2.1 Code is Law................................................................................................................5
   2.2 Default Privacy Settings..............................................................................................6
       a Settings .........................................................................................................................6
       b Default Settings ...........................................................................................................7
   2.3 Use Cases..................................................................................................................8
       a Geo-Location Data .........................................................................................................8
       b Facial Recognition .........................................................................................................10
       c Do Not Track ...............................................................................................................11

3. Purpose and Meaning of Default Settings .....................................................................13
   3.1 The importance of settings .......................................................................................13
       a Control .........................................................................................................................13
       b Transparency ..............................................................................................................14
       c Fair and Lawful Processing – Increasing Accountability ..............................................15
   3.2 The importance of Default settings ..........................................................................15
       a Settings are not Used ..................................................................................................15
       b Privacy Paradox ..........................................................................................................17
       c Fairness Principle .......................................................................................................17
       d Societal Values ...........................................................................................................19
       e Privacy by Design/Default .........................................................................................20
   3.3 Challenges ................................................................................................................21
       a Nature of Social Networks ........................................................................................21
       b The bigger picture ......................................................................................................22
       c Conflicting (Corporate) Interests ................................................................................23
   3.4 Quest for the Perfect Default .....................................................................................23
       a To Change or not to Change ......................................................................................24
           i Complexity ...............................................................................................................24
           ii Fundamental Values ..............................................................................................24
           iii Conclusion ............................................................................................................25
       b Setting the Default ...................................................................................................25
           i Personal attributes .................................................................................................27
           ii Purpose and Nature of Data (Processing) ..............................................................27
           iii Conclusion ............................................................................................................29

4. Implementation ...............................................................................................................29
   4.1 Law ..........................................................................................................................30
       a Data Protection ...........................................................................................................30
           i Fairness ....................................................................................................................30
           ii Consent/legitimacy of processing .........................................................................30
           iii Obligation to Inform ............................................................................................31
           iv Security ..................................................................................................................31
           v Towards a ‘Privacy by Default’ Provision? ............................................................32
       b Consumer protection ................................................................................................32
           i USA .........................................................................................................................33
           ii Europe ....................................................................................................................34
   4.2 Self-Regulation? .........................................................................................................35

5. Conclusion ......................................................................................................................36
1. Introduction

In 2010, Matt McKeon put online a great visualisation of how Facebook’s privacy default settings had changed since 2005.¹ It becomes very clear that the social network site² evolved from a rather closed down policy to an environment where almost all information is public by default. In the early days, for example, the only information that was visible to other Facebook users (not friends) included the name, picture, gender and networks of the individual. In April 2010, this had evolved to the public availability (even to non-Facebook users) of wall posts, photos, likes, friends and other profile data. This evolution is part of a deliberate choice by CEO Mark Zuckerberg, who believes that managing one’s privacy and personal data demonstrates a ‘lack of integrity’. Subsequent public outcry made clear that his opinion was far from universal and lead to some important changes to Facebook’s privacy policy.³

Especially in a social networking environment⁴, people expect some degree of control over their privacy and personal data. Privacy settings are a potentially important and useful tool to empower social network users. Controlling one’s social interactions and flow of personal information through technical settings, however, is not very intuitive. It will therefore be important that such settings have pre-selected values that respect the privacy of the social network’s users. The Article 29 Working Party⁵, in its opinion on online social networking, has explicitly stated that “robust security and privacy-friendly default settings are [...] the ideal starting point with regard to all services on offer.”⁶

This paper will try to elucidate the concept of ‘default privacy settings’ and the underestimated role it can have on the protection of individuals’ privacy and personal data protection on social networks. In the first Chapter, the scope and meaning of ‘default settings' itself will be examined. Once the reader has a better idea what can be understood as a ‘privacy default setting’, the following Chapter will thoroughly evaluate their rationale. After assessing its pros and cons, this Chapter ends with a modest attempt to suggest how default privacy settings should be determined. Finally,

---

² Hereafter referred to as: SNS.
⁵ The Article 29 Working Party is an advisory body of the European Commission. It is composed of data protection commissioners from all European Member States and a representative from the European Commission. The Working Party is independent and acts as an advisory body. It seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection issues. For more information, see: ec.europa.eu/justice/data-protection/article-29. The Article 29 Working Party will be referred to as the ‘Working Party’ or ‘WP’ throughout the rest of this paper.
the last Chapter will examine what constitutes the legal basis of privacy-friendly default settings.

2. What are Default Settings?

2.1 Code is Law

Code is Law. Postulated by Lawrence Lessig almost a decade and a half ago, this phrase has become a true proverb in Internet policy scholarship. According to Lessig, code (architecture, programming language, etc.) has an inherently regulating quality, directing the actions of its users. He argues that this so-called ‘west coast code’ is at least as important as ‘east law code’ in regulating individuals in the information society.

Evidently there are some important differences between these two forms of regulation. Code or architected design usually appears to individuals as a fait accompli. It is not the product of a (preferably) democratic process as is the case for traditional Law. More importantly, a priori Code cannot be sidestepped as easily as legal rules. In other words, people are chained by what the relevant code allows them to do. With regard to legal provisions, individuals will generally have the possibility to ignore them when they deem them illegitimate. This does not usually occur as laws are (normally) the product of a democratic process and ideally reflect the norms and values of society. Code, however, lacks this inherent quality and is subject to the coder’s intentions. To put it in the words of Tien:

“Architectural regulations are at the extreme perceived more as conditions than as rules to be followed or disobeyed consciously. Unlike ordinary sanction-backed rules, architecture achieves compliance by default rather than through active enforcement.”

Generally, code also lacks the transparency of legal provisions, making it harder to understand the underlying rationale and (intended) effects. Even benign decisions can have a big – and not necessarily intended – impact. It is, therefore, of utmost importance to recognize the influence of code over people’s behaviour, particularly in a social networking environment where every action happens within the network’s algorithmic confines.

Perhaps even more important, in this context, is how code can be used as a way to have a positive impact on users’ rights. With regard to the protection of privacy and personal data more specifically, the presence of appropriate settings plays an incredibly important role in empowering users. When clear and meaningful, privacy settings do allow individuals to maintain some control over their personal data. However, the mere provision of settings alone is often deemed insufficient. The

---

7 Lawrence Lessig, Code: And Other Laws of Cyberspace (Basic Books, 1999).
8 Referring to the geographic location of where most of this code is written.
9 Referring to legislative texts.
10 Lee Tien, “Architectural Regulation and the Evolution of Social Norms,” Yale JL & Tech. 7 (2004): 11–12. The author continues: “To the extent that legitimacy and public deliberation are integral to our notion of law, the surreptitious enactment and enforcement of norms via architecture should give us pause.”
creation of privacy-friendly default settings has been pushed forward as an important way in which code can guide individual behaviour in a fair and legitimate way.

2.2 Default Privacy Settings

a Settings

Privacy Settings

In the context of this deliverable, privacy settings can broadly be defined as *all technical options and elements that (can) decide how data flows on the social network*. In other words, settings exist where a concrete, technical decision is or can be made. It is important to note that who decides on these settings and the ease of changing them is irrelevant in this definition. From an end-user’s perspective though, a distinction can be made between wired-in settings and adjustable settings.

Wired-In Settings

In the development of a social network, thousands of decisions are made with regard to how data will flow. These decisions do not involve end-users, but are taken – deliberately or not – by the developers. When operational, most of these choices are given facts to end-users, determining their behaviour on the network.

Facebook’s timeline, for example, is a feature of the service that has been consciously developed in certain ways and has a direct impact on how people use the service. Furthermore, Facebook has stated that certain types of information (such as name, profile picture, network, gender and username) will always be publicly available.11 The fixed nature of wired-in settings is also demonstrated by the fact that most commercial SNS do not allow individuals to control what data they (do not) share with the service provider itself (though they usually do allow users to tweak what data is shared with other users (infra)).

Put briefly, wired-in settings cannot be altered by the end-user and are therefore not often considered to be privacy settings *stricto sensu*. It is important to remember, though, that they are settings nonetheless as a decision is/can be made.

Adjustable Settings

Settings that can be adjusted by end-users are the category that people usually refer to when talking about ‘privacy settings’. This category covers all options and tools end-users have in order to control what happens to their personal data. One of the most obvious examples is the ability to decide whom you share your data with. Privacy settings on social networks can generally be divided into two sub-categories. On the one hand there are settings allowing individuals to fine-tune their relationship vis-à-vis other users of the network. On the other hand, a large chunk of settings allow individuals to manage their relationship with the social network provider and other third party data controllers and processors. With regard to the latter category, settings often have as their main purpose to obtain the individual’s consent to process his/her personal data. As to the relationship between the data subject and social

---

11 Facebook Data Use Policy, [http://www.facebook.com/about/privacy/your-info](http://www.facebook.com/about/privacy/your-info) (last visited: December 5th, 2012).
network provider, privacy settings either regulate access to data, or how it can be used.

b Default Settings

“a software default is a pre-selected option adopted by the software when no alternative is specified by the user.”12

Dynamic nature

Privacy settings panes always come with a certain set of pre-selected values (even if they are entirely empty), usually referred to as the ‘default settings’. Settings can evolve over time, and with them defaults may change as well. For example, Facebook introduced more fine-grained control over users’ profiles. But, at the same time, the social network also increased the visibility of accounts and made most of users’ profiles public by default. On top of this, accounts also became indexable by search engines.13 Researcher Matt McKeon made a graph in 2010, clearly demonstrating the evolution of Facebook’s default privacy settings towards increased public exposure.14

Third Parties

Defaults can also influence what third parties the social network user will interact with. Twitter users, for example, are free to choose between different URL shorteners and image hosting services, but will generally rely on Twitter’s default partners. Depending on the third party’s privacy policy, this can have a considerable impact on users’ privacy, not to mention potential anti-trust issues.15

Default v Wired-In

It is important to distinguish default settings from wired-in settings. As described supra, wired-in privacy settings cannot be changed directly by the user of the social network, whereas default settings necessarily imply there is an option (for the user) to change them. In the context of social networking sites more specifically, default settings can take a variety of different shapes and forms. They do not necessarily relate to binary switches only (e.g. on/off), but can also apply to passwords16 and or

14 McKeon, “The Evolution of Privacy on Facebook.”
15 In many countries, Microsoft has been the subject of such investigations with regard to preferential treatment of web browsers, search engines, etc. See: Shah and Kesan, “Setting Online Policy with Software Defaults,” 990.
16 In an attempt to simplify configuration procedures, technology and service providers sometimes set a default password and/or username. A straight-forward and rather innocent example are WiFi settings (network name and/or password). But seemingly innocent cases might lead to reprehensible situations, as was illustrated in the Edutech case a few years back. The company (Edutech) had installed cameras monitoring the girls’ locker room in a Tennessee Middle School. Because the default passwords for these cameras were well-known and had not been changed, ‘anyone could access the camera and view the footage through the Internet’. See: Ibid.
automatically generated usernames. As mentioned in the previous paragraph, default settings might change over time. When a Facebook user, for example, does not explicitly (un)check the box 'keep me logged in', the box will become checked by default when the same user logs in from the same computer three times in a row.\(^\text{17}\)

**Penalty Defaults**

When there is a strong need for clear choice and/or consent, the SNS might also opt for a so-called ‘penalty default’. This means that the user cannot continue without making a clear decision. In other words, he/she is forced to inform him/herself and make a conscious decision. Unsurprisingly, penalty defaults are most relevant in situations where end-users are un-/misinformed or lacking technical sophistication. In order to be effective, they should be easily adaptable.\(^\text{18}\) In practice, penalty defaults will often take the shape of a setting that has no pre-selected value yet. A classic example can be found on many websites where the user is required to submit a country (of delivery, of residence, etc.).

**Conclusion**

Clearly default settings can take many different shapes depending on the relevant settings the end-user has at his/her disposal (forms, tick-boxes, sliders, etc.). The value of these defaults (even in case of 'penalty defaults'), is the product of the social network's self-interest – which also includes responding to end-users' concerns – and external (data protection) regulation. On top of their vague and heterogeneous nature, practice has demonstrated that default settings can change over time (supra). The least that can be said is that default privacy settings on social networks constitute a contentious issue that has not been the subject of much debate yet. The goal of this deliverable is to lift the veil and elucidate the practicability of privacy friendly default settings on social networks. But before examining their implementation, it will be necessary to evaluate the benefits and drawbacks of default settings.

**2.3 Use Cases**

This part will describe three cases in which (default) settings play an important role as to protecting the privacy of individuals on social networks. They will referred to throughout the rest of this paper and serve as illustrations to the rather abstract parts.

\textbf{a Geo-Location Data}

The strong increase of mobile, Internet enabled devices has led to the development of a wide variety of location-based services. The actual location of a smartphone, tablet or portable computer can provide a lot of added value to the user, as well as be useful to the (social network) service provider.

---


\(^{18}\) Shah and Kesan, “Setting Online Policy with Software Defaults,” 999–1000. The authors’ use of the word 'defaults' differs from the meaning of default settings in this deliverable and bears more resemblance to 'adjustable settings' (supra).
Netflix (an online VOD service), for example, regulates access depending on the location where you are accessing the service from. When an American Netflix customer travels to the UK, he will be offered different content depending on the relevant licensing deals in the UK. When traveling to other countries, the customer might not even be able to access the service at all together. Location data is also amply used by (international) websites in order to set the default language. When accessing Google in France, for example, the user will be referred to Google.fr and be addressed in French. Examples of location data serving end-users are legion. With regard to social networks in particular, many services have incorporated the ability to share your location, find friends, give (sight-seeing or restaurant) recommendations, etc.

Location data can be obtained in a variety of ways, each with different levels of accuracy (e.g.: WiFi access points; GPS; via wireless carriers; location providers; or location aggregators). Although geo-location data does not fall within the ‘special categories of data’, mentioned in the Data Protection Directive, it concerns potentially sensitive and intrusive information nonetheless. When obtained through ‘always on’ mobile phones in particular, this data will closely mirror the individual’s movements and activities. Though not applicable to social networks in particular (only to electronic communication services, such as mobile phone operators), the European ePrivacy Directive explicitly states that the ‘processing of such [precise location] data for value added services should only be allowed where subscribers have given their consent’. Arguably, social network providers have an important responsibility with regard to this data as well, particularly when it is shared with third parties on their platform. This might be translated into appropriate tools for data subjects to control the use of their data, combined with privacy friendly defaults.

The issue of location data emphasizes the difference between settings regulating access to personal data and settings regulating how the data can be used (supra). As a first step, appropriate settings might give the data subject the ability to control whether his/her location data is shared. Secondly, settings will enable the data subject

---


22 "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

23 Soltani, Testimony on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy, 2. The author continues: “The location of a mobile device at any given moment may not be particularly sensitive; However, the historical trail of past locations can reveal much about its user’s behavior.”


25 Recital 35. The text continues: “Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.”

26 Opinion on Geolocation, 13.
to manage how the personal data is used. In some situations, the end-user might not be able to control access to his/her location data (in a meaningful way). A device’s location might be derived from its WiFi access point or through local cache files already. And a Wall Street Journal Survey of 2011 demonstrated that almost half of the 101 most popular iOS and Android apps transmitted the phone’s location data to third parties.

A great example of the second category of settings (regulating use) can be found, yet again, in Facebook’s geographic network policy. In 2007, it was brought to light that people were included in a certain geographic network by default. At the same time, visibility defaults were also set to ‘anyone within your network’. As a consequence, most of your data became viewable by anyone else in ‘your (geographical) network’ (at the time this networks were huge already: NY more than 421,000 and London more than 1.2 million).

b Facial Recognition

Facial recognition is the automatic processing of digital images, that contain the faces of individuals for the purpose of identification, authentication/verification or categorisation of those individuals.

At the All Things Digital (D9) Conference in May 2011, Eric Schmidt (Google’s CEO) expressed his concern about the facial recognition technology capabilities Google had developed. “As far as I know,” Schmidt said, “it’s the only technology Google has built and, after looking at it, we decided to stop.” Such statements, especially from the man who is known for his bold anti-privacy statements, clearly demonstrate the contentious and potentially dangerous nature of this emerging technology.

In short this technology makes it possible to identify individuals, based on their facial features. As with location data, this generates a lot of potential uses for individuals, such as security or organising a photo library. Issues arise, however, when facial

---

28 For more information, see: blogs.wsj.com/wtk-mobile.
32 For example: “If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.” See: Richard Esquerra, “Google CEO Eric Schmidt Dismisses the Importance of Privacy,” Electronic Frontier Foundation - Deeplinks, December 10, 2009, eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.
33 The Article 29 Working Party, has identified six different steps in the process of facial recognition: (1) Image Acquisition; (2) Face Detection; (3) Normalisation; (4) Feature Extraction; (5) Enrolment; (6) Comparison. See: Opinion on Facial Recognition, 2.
recognition technology is used by others (often without the individual even being aware of it).\textsuperscript{34} 

Facebook for example, tagged people automatically in pictures uploaded to the platform. Meanwhile, the social network has changed this by asking prior consent. Nonetheless, tag suggestions will still appear at the top of the user’s page.\textsuperscript{35} And even though people might opt not to tag themselves on certain pictures, Facebook will still perform apply the technology internally. This illustrates, yet again, the difference between adjustable settings (option (not) to tag) and wired-in settings (Facebook recognising faces). It must be said, however, that in the 2012 re-audit by the Irish DPA, Facebook appeared to delete ‘facial profiles’ when users disabled tag suggestions entirely.\textsuperscript{36}

Because of the ‘particular risks involved with biometric data’, the Article 29 Working Party has recently declared that prior informed consent is required for facial recognition processing. But, in practice, it will only be possible to obtain consent (or verify if consent has been obtained already) after a face has been ‘recognised’ already. The working party has affirmed that such processing should be allowed and is justified by a legitimate interest (art.7(f) DPD, or 6(1)(f) of the DP Regulation Proposal).\textsuperscript{37}

Facial recognition technology allows a link to be made between physical and virtual identities or vice versa (dubbed Face-to-Data or F2D).\textsuperscript{38} With off the shelf technology, someone could easily take a picture of a person in a bar and discover that person’s identity through publicly available pictures on the Internet. Or one could even imagine cross-referencing (profile) pictures that are used across different platforms, discovering real identities behind pseudonymous accounts.\textsuperscript{39} As a matter of fact, researchers at Carnegie Mellon University have demonstrated the feasibility of this in practice.\textsuperscript{40} Nevertheless, as a few important privacy law scholars recently stated, “a widespread private use of F2D may contribute little to society while presenting a significant risk of potential harm to privacy.”\textsuperscript{41}

c Do Not Track

“Do Not Track is a technology and policy proposal that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms.”\textsuperscript{42}

---


\textsuperscript{35} Irish Data Protection Commissioner, Facebook Ireland Report of Re-audit, 8; 36–37.

\textsuperscript{36} Ibid., 36–37.

\textsuperscript{37} Opinion on Facial Recognition, 5.

\textsuperscript{38} Christopher Kuner et al., “Face-to-data—another Developing Privacy Threat?,” International Data Protection Law (December 6, 2012), http://idpl.oxfordjournals.org/content/early/2012/12/05/idplips032.

\textsuperscript{39} Also see: Edwards and Brown, “Data Control and Social Networking,” 13.

\textsuperscript{40} For more information, see: http://www.heinz.cmu.edu/~acquisti/research.htm.

\textsuperscript{41} Kuner et al., “Face-to-data—another Developing Privacy Threat?,” 2.

\textsuperscript{42} donottrackkus
Do Not Track (‘DNT’) is the product of a collaborative effort between a group of researchers, civil society organisations and technology companies, reacting against the exponential increase of online tracking. Today, people are being tracked across the Internet in a wide variety of ways (cookies, HTML5 storage, pixels, beacons, fingerprinting...). In a 2009 survey, it turned out that Google is tracking Internet users on around 88% of websites. Social plug-ins are proliferating on many websites as well. Facebook’s COO Sheryl Sandberg, for example, declared that “10,000 new websites integrate with Facebook every day”. In 2007, so-called flash- or respawning cookies were discovered. When an individual deleted cookies, these flash cookies would make them reappear. It has also become clear that many tracking entities use multiple technologies simultaneously to track people. When people delete or change one of them (e.g. delete cookies or use a different browser) there will still be other trackers that can identify the individual and make the deleted tracker respawn.

In short, Do Not Track constitutes a standard that would signal the Internet user’s wish not to be tracked. At the moment, such a ‘centralised opt-out of online behavioural tracking’ depends to a great extent on the benevolence of tracking entities. On top of that, end-users should also have the opportunity to signal a DNT preference. Put differently, in order for Do Not Track to work, browsers (and/or other channels through which people access the Internet) as well as online tracking entities are required to implement the standard in their technology. Most web browsers have implemented a DoNotTrack button and one company (Sitecom) has even released a router that supports DNT. Microsoft announced that it would enable DNT by default in Internet Explorer 10 on all future Windows 8 devices. Finally, the US Federal Trade Commission is currently investigating to what extent Do Not Track can/should be legally enforceable. And although initially a US focused initiative, the European Commission is looking into the merits of DNT as well.

---

43 Ashkan Soltani, Travis Pinnick, and Joshua Gomez, Know Privacy (California: UC Berkeley, School of Information, June 1, 2009), 27, knowprivacy.org.

The Article 29 Working Party has also expressed its enthusiasm for Do Not Track. See: Article 29 Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural
3. Purpose and Meaning of Default Settings

3.1 The importance of settings

"[O]n SNSs the notion of consent fails as a gatekeeper protecting the privacy of users."

Before evaluating the importance of default settings, this part will focus on the rationale behind privacy settings in general. As described elaborately in the previous deliverable, ‘consent’ is generally seen as a justification for data processing. Interpreted as such, this ‘artificial procedural justification’ offers a wild card to data controllers as to what can be done with the data. Arguably, fairness should be reinstated. This happens, among other things, through proper privacy settings. These allow the individual to exercise more control, increase transparency and enhance the lawfulness and fairness of the processing altogether.

a Control

Probably the most important and straightforward reason for privacy settings to exist on social networks is to enable the user to control his/her personal data. The digitisation of (personal) information, has removed all of its spatial as well as temporal boundaries. On top of that, technology nowadays allows for the collection of virtually every kind of data imaginable. In other words, the idiom ‘information wants to be free’, often used as a slogan criticising the copyright industry, is also relevant with regard to personal data. But, because of the underlying fundamental values of privacy and personal data protection, some boundaries – artificial as the may be – should be put in place. Privacy settings enabling the data subject to control the flow of his/her personal data constitute such limitations. As with other information/intellectual rights, however, these limitations should not be absolute and a careful balance will have to be found. This balance should take into account the data subject’s ability to control, as well as other individuals’ fundamental rights (to control their data, to freedom of expression, etc.) and the corporate interests of the social network itself. In practice, this could mean, for example, that privacy settings enable a SNS user to delete a picture uploaded by him/herself (A), but cannot have it removed if uploaded by someone else (B). Intermediate solutions in this situation could be that A can restrict access to the picture, blur his/her face, (un)tag it, etc.

Offering users the ability to control their personal data is often interpreted quite broadly. In order for this control to be meaningful, it is important that the social network provider offers a clear, simple and logical privacy settings pane that can easily be manipulated by the end user. As an example of the contrary, Facebook makes it hard to dissociate oneself from liked pages in bulk. One cannot simply remove all


51 Edwards and Brown, “Data Control and Social Networking,” 19.
53 Ibid.
'likes' with one click, but has to 'unlike' each individual page via a click-through pane. Another often-recurring problem on existing social networks is that users are often with an all-or-nothing choice when third parties request access to their personal data.\(^5^4\) Finally, the strong differences between control panels on different social networks, and even within the same SNS but on different operating systems/platforms (variety of mobile as well as desktop OS's). Particularly on mobile devices, granular permissions are not typically made available.\(^5^5\)

Recent research seems to suggest that SNS users are becoming more pro-active in managing their accounts (unfriending, deleting pictures or comments, etc).\(^5^6\) Over half of social networking users (58\%) in a 2012 Pew Study, claimed to have closed down their profile so that only friends can see it.\(^5^7\) In the same study, however, half of users (48\%) said to have difficulties managing the privacy controls (although only 2\% said the privacy settings were 'very difficult'). Educated users expressed more difficulties in managing privacy settings and female users (67\%) and teens (62\%) generally control their privacy settings more conservatively.\(^5^8\)

b Transparency

Privacy settings do not just enable the individual to better control the flow of personal data on the social network, they also make them more visible. An elaborate – though clear – set of adjustable privacy settings necessarily implies transparency about the data flows that can be tweaked. After all, how can the end-user control his/her personal data without knowing what it might be used for? Google, for example, compiles its location databases by ‘crowdsourcing’ their customer’s devices. Although consumers do have the option to opt-out, background collection and transmission is usually enabled by default.\(^5^9\) As a matter of fact, few people are even aware of this at all. Unintended disclosure of personal data is often the consequence of the misconception that social network sites are private – rather than public – spaces.\(^6^0\) Clear and precise privacy settings can elucidate different levels of visibility and positively influence end-users’ expectations of privacy protection.

Under the European data protection regime, social networks are obliged to provide a certain amount of information to their end-users (art.10 et seq. DPD). Usually, this requirement is dealt with through legalese privacy policies that are rarely read by anyone. Instead of this legal fiction, a more effective ‘notice and choice’ system might consist of a clear setting-up procedure. During this procedure, the user is educated about the different functionalities and can make meaningful decisions instead of the binary all-or-nothing approach in the current consent regime.

\(^{5^4}\) Edwards and Brown, “Data Control and Social Networking,” 11.
\(^{5^5}\) Soltani, Testimony on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy, 8–9.
\(^{5^6}\) Edwards and Brown, “Data Control and Social Networking,” 11.
\(^{5^7}\) Madden, Privacy Management on Social Media Sites, 2–3.
\(^{5^8}\) Ibid., 2–3; 7.
\(^{5^9}\) Soltani, Testimony on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy, 4–5.
\(^{6^0}\) Edwards and Brown, “Data Control and Social Networking,” 17.
c Fair and Lawful Processing – Increasing Accountability

According to the European data protection framework, all data processing must be fair and lawful (art.6(1)(a) DPD). This obligation can be read as an important motivation for social networks to provide adequate privacy settings. As has been argued amply by many scholars, the protection of Internet users’ privacy should not be the product of a contractual agreement, but should be ‘contextually-driven [and] consumer expectations-oriented’.61 The proposal for a new data protection Regulation by the European Commission in January 2012 has included some extra obligations with regard to the data controller’s responsibility and data protection by design/default (art.22-23).62 These clearly illustrate the intention to increase ‘fairness’ and ‘reasonableness’ and not just rely on the binary consent framework which only provides a priori protection.

As will appear infra, fairness is a criterion that is not just exclusive to data protection law, but also appears in the context of consumer protection rules. Because of the absence of a general data protection framework in the USA, this is often the only effective way to go after unacceptable practices by social network providers. In 2011, for example, Facebook settled with the FTC in a case concerning its 2009 privacy settings changes (suddenly making public certain parts of users’ profiles such as profile picture, birthday, friends list, etc.).63

Put briefly, in order for social networks to comply with consumer protection and data protection rules (infra), they should – among other things – ensure the presence of adequate privacy settings. The fairness principle forces social networks to protect personal data more methodically/rigorously and restrains them from acquitting themselves through the use of ‘notice and consent’ alone.

3.2 The importance of Default settings

The previous part demonstrated the importance for social network sites empowering their users through privacy settings panes. But, merely providing privacy settings only goes that far. In order to be truly privacy friendly, these settings will need to have proper default values.

a Settings are not Used

A lot of research has been done on how SNS users manipulate their privacy settings, if at all. Although results vary, the common trend seems to be that a majority of people does not change the default privacy settings of their social network. One 2007 study – conducted by security firm Sophos – asserted that 75% of users never changed their

---


default settings. In 2009, for example, Facebook’s Chief Privacy Officer (Chris Kelly) said that only 20% changed their privacy settings. This was confirmed in 2010 by the information and privacy Commissioner in Ontario Canada. Yet another 2009 study found that between 55 and 90% of social network users does not change their default settings for viewing of profile information. It must be said, however, that more recent research has suggested that social network users are becoming increasingly pro-active with regard to the management of their privacy settings.

The numbers mentioned before should be take with a pinch of salt. The relatively low percentages of people changing default settings depend on a lot of factors and it is hard to discern what they actually mean. First of all, the default values of privacy settings might actually be agreeable to social network users. It is important not to forget that publicity and sharing data is exactly what constitutes the nature of a social network. Back in the early days of Facebook (2005), for example, Gross and Acquisti demonstrated that only 1,2% of users changed the searchability default of their profile. And only 0,06% had changed the default of their profile (set to visible to anyone). On the other hand, the low numbers might also be a consequence of the complexity of privacy settings. Several studies have demonstrated that the functions and actual impact of privacy settings are often unclear to users. People generally visit social network sites as diversion and are not inclined to deal with the cumbersome process of managing privacy settings. Moreover, it has been claimed that few users are even aware of the existence of privacy settings that can be tweaked. And if users are aware of their existence, they often lack the (technical) knowledge to make a proper risk assessment.

So, put briefly, although most social networks do provide extensive privacy controls, only few users do change the initial settings. Due to this fact, whatever the reason, it is important that the default values of these settings are privacy friendly.

68 Madden, Privacy Management on Social Media Sites. Also see supra, 3.1.a. The Importance of Settings – Control.
71 Ibid., 7.
72 Paul Marks, “Social Networks Must Heed the Human Element,” New Scientist 206, no. 2763 (June 5, 2010): 19–19. The author explains that the massive overload of privacy settings on many social networks make it impossible for the average user to manage them properly.
73 Ibid., 22.
Related to the previous point, another important observation many scholars (in different disciplines) have written about is the so-called ‘privacy paradox’.\(^\text{74}\) In short, the privacy paradox refers to the apparent contradiction between an individual’s privacy concerns and their actual (online) behaviour. When asked, most people seem to agree that they want their privacy and personal data to be protected as much as possible. But on the other hand, most social network users behave quite carelessly with regard to their personal data. In his research, \textsc{Acquisti} has also demonstrated what he calls a ‘control paradox’.\(^\text{75}\) He shows that when given (the illusion of) more control over the publication of their private information, privacy concerns decrease and individuals will be more likely to publish (sensitive) information.

It goes beyond the scope of this paper to discuss the details of these paradoxes. What they make apparent is that in general, people do not tend to behave in privacy protective ways. Also made clear is that this behaviour does not necessarily reflect people’s desire to have their privacy and personal data protected. Especially with regard to social interactions, managing privacy settings \textit{ex ante} is deeply alien to the human mind.\(^\text{76}\) People do not interpret privacy protection as controlling rigid access lists or permissions, but rather in terms of social roles and interaction.\(^\text{77}\) On social networks in particular, users tend to misperceive the platform as a private space, having the illusion of privacy.\(^\text{78}\) What can be drawn from the above is that the counter-intuitive nature of managing one’s privacy settings clearly demonstrates the importance of having privacy friendly default settings.

c \hspace{1em} \textbf{Fairness Principle}

A third, important ground for putting in place privacy-friendly default settings can be found in the fairness principle. Though still very vague and powerless in the current EU data protection framework, it seems that the concept will become more prominent in the future. As mentioned before (see \textit{supra}, Importance of Settings), policy makers have demonstrated the intention of strengthening the fairness principle and introduce some sort of proportionality principle as well. In the latest document for the modernisation of Council of Europe’s Convention 108\(^\text{79}\), an extra paragraph was added to article 5 on the legitimacy of data processing and quality of data: “Data

\(^{74}\) Patricia A \textsc{Norberg}, Daniel R \textsc{Horne}, and David A \textsc{Horne}, “The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors,” \textit{Journal of Consumer Affairs} 41, no. 1 (June 1, 2007): 100–126. Also see the many articles that were published as part of the 2012 Stanford Law Review Symposium on ‘The Privacy Paradox: Privacy and Its Conflicting Values’, available at: www.stanfordlawreview.org/symposia.


\(^{78}\) \textsc{Edwards} and \textsc{Brown}, “Data Control and Social Networking,” 8; 17.

processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, be they public or private interests, and the rights and freedoms at stake.”

The European Commission recently stated that data controllers (social networks) “must prove they need to keep the data rather than you having to prove that collecting your data is not necessary.”

These legislative efforts, complemented by audits and investigations into the privacy practices of major online social networks, seem to suggest a clear intention to hold these networks more accountable and induce better protection of privacy and personal data.

In general, default privacy settings on social networks seem to be rather permissive with regard to allowing access to strangers. The mere provision of extensive privacy settings, clearly does not guarantee the ‘privacy friendliness’ of social networks. As mentioned supra, end-users are often confused about the meaning and scope of privacy settings. This confusion ensuing from complex interfaces might – arguably – have a negative impact on the protection of users’ privacy. Even worse, SNS might well defend ever more privacy intrusive practices with the argument that they offer users the ability to adjust settings. In 2012, for example, Google decided to centralise all data gathered across its different services and social plug-ins, arguing that users maintain control. One could easily question the practical impact of this ‘user empowerment’ (even when users are given more control), if default settings are privacy-unfriendly. Moreover, several social networks – Facebook in particular – have been criticised for constantly changing their (default) privacy settings, even though they increase user control.

Despite this scepticism vis-à-vis comprehensive privacy settings, it is crucial not to disregard their importance. Instead, more effort should be put in simplifying privacy panes. More importantly, the above also stresses the significance of fair and proportionate default settings that take into account all interests at stake.

---


85 This has been requested by the CNIL in its Review of the changes in Google’s privacy policy CNIL, “CNIL Review of Google’s New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data Across Services.”


d Societal Values

As has been mentioned in the previous part(s) on fairness, a privacy-friendly social network goes beyond the mere provision of fine-grained privacy settings alone. The primarily individualistic approach in the current data protection framework has failed to adequately protect people's privacy. Policy seems to evolve to increased accountability of data controllers/processors. In today's information society, there is a growing power imbalance between individuals and corporations processing personal data (e.g. social networks). In such an environment, it might make sense to reduce the responsibility of the individual to protect his/her own personal data and put in place some basic principles for data controllers/processors to follow. Such a paternalistic – 'European' – approach is particularly important in order to protect ignorant and/or vulnerable users (of social networks). The Council of Europe, in April 2012, has confirmed this fundamental societal value of protecting the weak in a social networking context: "In particular, children, especially teenagers, and other categories of vulnerable people, need guidance in order to be able to manage their profiles and understand the impact that the publication of information of a private nature could have, in order to prevent harm to themselves and others."99

Besides the protection of vulnerable social network users, proper default settings are also relevant with regard to so-called 'sensitive' or 'special categories of' data (art. 8 DPD). These categories of data in particular should be treated with extra care and protection. Conservative default settings can play a fundamental role in this regard.

Very recently, Facebook has specifically emphasised it does not target people based on religious, political or sexual orientation information in a person's profile. It is unclear, however, what the social network's policy is related to (default settings of) the use and sharing of this data for other purposes.

The importance of default settings goes beyond the protection of weak and vulnerable users. As mentioned before, privacy settings as such are not frequently used in practice. The fact that people often blindly accept and follow the default settings of a 'free' (social networking) service does not mean their privacy and personal data should not be adequately protected. Certain 'standards' for default settings might – it has been argued – have a considerable impact on individuals in general. Default settings are also interpreted as recommendations, guiding users. In this regard, they

---

88 Especially when they are aimed at children and inexperienced young users. See: Edwards and Brown, "Data Control and Social Networking," 18.

89 Committee of Ministers, Recommendation on the Protection of Human Rights with Regard to Social Networking Services Appendix, note 2.

90 This article refers to 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.' The Council of Europe has stated that an individual's search history (taken as a whole) might also constitute sensitive data (revealing racial origin, political/religious opinions, etc.) that warrant special protection under Article 6 of the Convention 108.


91 Irish Data Protection Commissioner, Facebook Ireland Report of Re-audit, 17.

do not just affect a person’s individual actions, but are also ‘shaping norms and creating culture’.

So put briefly, privacy friendly defaults are also relevant with regard to society as a whole. Not just to protect weak and vulnerable users, but also to avoid the erosion of fundamental values related to privacy. At this stage, it is worth reiterating five arguments that have been made in the previous deliverable.

(a) privacy is a societal good, and should therefore not be treated as a negotiable commodity;
(b) requiring individuals’ to ‘police their own privacy’ is a burden unfit for most;
(c) the efficacy of ‘notice & choice’ as a regulatory technique depends too heavily on rational choice fallacies;
(d) data subject consent should not serve as a waiver for privacy-intrusive practices; and
(e) requiring data subject consent inhibits socially beneficial re-use of information.

**e Privacy by Design/Default**

Last but not least, it is worth mentioning the Privacy by Design debate as an important rationale behind the creation of privacy friendly default settings. The Concept of Privacy by Design was popularised in privacy policy debates by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada. According to Cavoukian, privacy-preserving default settings are one of the seven privacy principles of ‘Privacy by Design.’ It is important that “[i]f an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.”

The principle of data protection by design and by default has been introduced in the proposal for a new Data Protection Regulation. Article 23 (emphasis added) specifies that:

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

---

94 Ibid., 7. The authors describe the perceived social value of ‘openness’ on social networks.
96 For a brief history about the concept, see: Ann Cavoukian, “Privacy by Design” (Information & Privacy Commissioner Ontario, Canada, 2009). ipc.on.ca/images/Resources/privacybydesign.pdf.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

[...]

From this (proposed) provision, the intention to increase accountability and responsibility of the data controller becomes apparent even more so. Privacy by design and default is not just another rule companies can simply tick away on their ‘privacy by design checklist’ for compliance reasons. It necessitates active and comprehensive measures that make a fair balance between the interests of the social network and those of its users (supra).

Finally, it is also worth mentioning the importance of the work that is being done in Human-Computer Interaction (HCI). A lot can be learned from HCI with regard to the designing process of (privacy) control panels on social networks. At the moment the surreptitious nature of software results in a large majority of users to accept it as a given fact, not meant to be controlled individually. HCI might help to identify the human needs and values on these networks and translate these into privacy-friendly and easy to manage (default) settings.

3.3 Challenges

The previous pages have tried to clarify what default privacy-settings are exactly and what its main rationales are in a social networking context. With this in mind, the following part will critically evaluate default settings and put them into perspective in the broader debate of privacy on social networks.

a Nature of Social Networks

To a certain extent, privacy-enhancing default-settings might be deemed contradictory to the inherent nature of social networks. People subscribe to social network platforms exactly because they want to share and publicise information. Danah Boyd’s research on social network usage by youngsters, for example, has demonstrated that ‘social factors undermine technical controls’. Putting in place restrictive default settings might frustrate users and even drive them away from the service. There is indeed a significant (some even claim irreconcilable) tension

---

99 Mulligan and King, “Bridging the Gap Between Privacy and Design,” 1019. The authors also refer to the related and emerging field of Values Sensitive Design (VSD).
between “the desire for reliable control over one’s information and the desire for unplanned social interaction.”

For example, a Facebook profile with its privacy settings set to maximum protection when created will not be visible to anyone. Arguably, this is not an ideal starting state. In a recent letter to the Irish Data Protection Authority, Facebook expressed its support for the Privacy by Design principle, but has doubts with Privacy by Default. According to the social network, this last principle does not take into account the ‘sharing ethos underpinning social network services.’ The Regulation, Facebook continues, ‘should have respect for the context in which data is collected and processed’.

Add to this the idea of privacy as contextual integrity and the practicability of privacy-friendly default settings becomes even more nonsensical. The term, coined by Helen Nissenbaum almost a decade ago, emphasises the importance of context – who can see the data, who will use it, will it be shared, what is the nature of the information, what is the relationship between the different parties, what are the larger institutional and social circumstance – when evaluating the sharing of (personal) information. Due to the sharing culture on social networks, establishing standard values is practically impossible as they will never be able to entirely capture the complexity and volatility of relationships. On top of that, privacy values also depend on the respective cultural/generational background, time period, location, etc. When interacting with peers, people tend to interpret their privacy in terms of ‘social rules and social roles’ instead of binary control panes.

**b The bigger picture**

It is important to remember that (default) settings are only a small part in the larger picture of ameliorating people’s privacy and personal data protection on social networks. The complex set of relationships and interactions that take place on social network platforms also make it very hard to establish standardised default settings for all users. The very idea of attempting to capture these context-dependent social nuances in technical controls is even said to be an oxymoron. Other elements – such as data minimisation, accountability, transparency, etc. – will probably play a more important role. Additionally, when people become too reliant on default settings for protecting their privacy, this might lead to ignorance, carelessness, and abuse by others.

Even when one has in place (default) privacy settings that are deemed adequate, the individual’s privacy and protection of personal data is still not guaranteed. As mentioned before (Do Not Track, supra), flash cookies and the like have as their main purpose to circumvent (default) privacy settings.

In August 2012, for example, Google was fined for violating “a Commission order by misrepresenting to Safari browser users how to avoid targeted advertising by

---

103 Edwards and Brown, “Data Control and Social Networking,” 22.
104 Facebook Ireland, ”Facebook’s Views on EU Data Protection Regulation” (Europe v Facebook, March 30, 2012), 4, http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf.
105 Nissenbaum, “Privacy as Contextual Integrity,” 154–155.
106 Ibid., 156.
In this case, Google had placed advertising tracking cookies on Safari browsers "despite telling users it would honour the default Safari privacy settings, which prevented the placement of such cookies." The collection and use of location data raises similar issues. Even though the operating system might provide privacy friendly (default) settings, third parties can still derive the device’s location whenever the its WiFi-radio is turned on (default on most smartphones, tablets and laptops).

In other words, even though an individual may have very advanced privacy controls with conservative default settings; this does not necessarily guarantee protection from third parties.

3.4 Quest for the Perfect Default

Put things into perspective – The previous two parts have evaluated the benefits and drawbacks of default privacy settings. It became clear that they only play a small role in the protection of an individual’s personal data and privacy on social networks. But despite the forces working against it (market incentives, nature of SNS, etc.), default settings still have considerable merits. In practice, however, it may not always be easy to determine what exactly ‘privacy-friendly default settings’ should look like. That is why, in the next few pages, a modest attempt will be made to set out some recommendations on how to construe these defaults.

---


113 Kuczerawy and Coudert, “Privacy Settings in Social Networking Sites,” 239.
a To Change or not to Change

Before evaluating what the default privacy settings should look like, it will be necessary to decide on whether the respective setting(s) should be wired-in or adjustable. As described supra, more (privacy settings) is not necessarily better (to protect personal data and privacy). There are two major justifications to opt for wired-in over adjustable settings: complexity of settings and fundamental values at stake.

i Complexity

An overabundance of adjustable privacy settings might lead to inertia and ignorance. When almost everything becomes customisable the more important settings (with regard to privacy) will get buried amid the trivial ones. The issues that are raised by an overabundance of choices have also been researched in the field of user customisation (computer science)114 and have been summarised by Shah and Kesān.115 First of all, a high number of (default) settings confuses and intimidates people.116 Secondly, designers are practically limited in the amount of defaults and presenting them in a useful manner without overloading the user interface. At a certain point, adding more defaults will reach a point of diminishing returns from the user’s perspective. SNS users, for example, might be interested in having the option to encrypt certain content on their profile. By contrast, users will probably not be interested in being offered choices regarding all the technical details behind the encryption process. On top of that, adding more options also exponentially increases the amount of potential configurations and thus the volume of code, making it a lot harder to audit.117 Finally, a highly adjustable privacy settings-pane might paradoxically lead to better identifiability (through fingerprinting).118

ii Fundamental Values

Privacy advocates often plead for the individual to have ever more control over his personal data. But, as became clear supra, more control does not necessarily equal better privacy. When certain fundamental (privacy) values or rights are at stake, the SNS should not offer the option to adjust, even if the default is privacy-preserving. Most users can easily be talked into changing the privacy-friendly defaults in return for small but instantaneous gratification.119 But, from a legal (and societal) standpoint,

116 With regard to security settings in particular, if the software engineer cannot even make up his mind (e.g. on which encryption tool to use), how is the end user supposed to make a decision? See: Roger Dingledine and Nick Mathewson, “Anonymity Loves Company: Usability and the Network Effect,” in Security and usability: designing secure systems that people can use, ed. Lorrie Faith Cranor and Simson Garfinkel (Beijing [u.a.]: O’Reilly, 2005), 552–553. Also see: Grimmelmann, “Saving Facebook,” 1185–1186.
118 Ibid., 553.
certain rights are simply not waivable. This may be particularly relevant with regard to minors. Arguably, location-based services should not even offer the option (to minors) to share their location with third parties and/or use it for behavioural tracking purposes. In other words, when the risks to privacy and personal data protection are imminent enough, wired-in settings might be preferable over adjustable settings (with or without privacy-friendly defaults).

\[iii\quad Conclusion\]

Summarising the above, it is worth mentioning four concrete factors that policy makers and social network providers should take into account when deciding on wired-in versus adjustable settings. First of all, the knowledge (relevant to the setting) of users should be evaluated. If there is a high likelihood that they are ignorant about the technical, legal or other implications of certain privacy settings, a wired-in solution might be preferable. Secondly, it should be possible to lay-out the settings in a clear, easy-to-use and well-organised way. If this is not the case, wired-in settings make more sense. Thirdly, wired-in settings might be preferable for those elements where there is little to no variety between users. For example, most users will probably agree on the importance of security. Preferences on the publicity of personal information might differ more widely. So, whereas the latter should be the subject of adjustable settings, security might, arguably, be wired-in. Finally, it should be examined whether there is a demand for adjustable settings in the first place. As mentioned in the ‘Complexity’ section, there is no added value in too much (trivial and/or technical) settings.

\[b\quad Setting the Default\]

Once the decision has been made to use adjustable (privacy) settings, the social network provider will have to decide on what their default value will be. Ideally, no action should be required from the SNS users for their privacy and personal data to be protected.

One of the key-factors for default settings to be considered privacy-friendly is that they fall within the user’s expectations. Determining these expectations will be challenging in practice, but necessary nonetheless. According to Shah and Kesan, the default should be based on what a well-informed end-user would choose if confronted with the relevant setting. This test is often called the ‘would have wanted standard’ and is derived from general contract law. According to this test, the default settings

\[\text{\small 120}\quad \text{Margaret Jane Radin, “Regulation by Contract, Regulation by Machine,” Journal of Institutional and Theoretical Economics 160, no. 1 (01 2004): 149–151. The author mentions three categories in particular: (1) rights related to legal enforcement; (2) human rights; (3) rights that are politically weak.}\]

\[\text{\small 121}\quad \text{Shah and Kesan, “Setting Online Policy with Software Defaults,” 1000.}\]

\[\text{\small 122}\quad \text{These factors are largely derived from: Ibid., 995–996.}\]

\[\text{\small 123}\quad \text{User’s likelihood of understanding should be measured against the most simple framing of the relevant setting. See the example mentioned in the ‘Complexity’ section, related to encryption settings.}\]

\[\text{\small 124}\quad \text{Ann Cavoukian, Privacy by Design and the Emerging Personal Data Ecosystem (Ontario, Canada: Information and Privacy Commissioner/Ontario, October 2012), 18, http://privacybydesign.ca/content/uploads/2012/10/phd-pde.pdf.}\]

\[\text{\small 125}\quad \text{Shah and Kesan, “Setting Online Policy with Software Defaults,” 1002.}\]
should be “what the parties would have bargained for if the costs of negotiating were sufficiently low”.126

General principles such as fairness and proportionality (supra) will also play an important role in setting the default. In the absence of specific legal requirements127, the social network will have to make this assessment by itself. But, this does not prevent a posteriori control by other (independent) bodies such as DPA's and/or Courts.128 In any case, the most recommended criterion to determine privacy-friendly default settings is to look at user expectations. Obviously, user expectations might be uninformed and/or manipulated. But the previous section (on wired-in versus adjustable settings) has already made clear that settings related to fundamental values and technical details should not be subject to choice in the first place. On top of that, social network providers will also be constrained by legal provisions (which will be amply discussed in Chapter 4 on Implementation).

The so-called Oxford Case129 is a classic illustration of how an individual’s expectations can be violated on social networks. This case concerns some Oxford students that had posted pictures of their post-exam parties (involving spraying each other with champagne, shaving foam and flour) onto Facebook. The University's proctors searched the social network for evidence and sanctioned some of the students. Students reacted in dismay and claimed this was a huge intrusion into their 'private sphere'. Arguably, Facebook should have put in place stricter default privacy settings so uploaded content is only visible to pre-selected contacts. Since this case occurred (2007) many similar cases have followed.130 Another example of how default settings can completely go against user expectations concerns Facebook’s group-policy changes in 2008. The network changed the default setting so that profiles became visible to everyone within the user’s default network. Consequently, profiles that were automatically included in the London network suddenly became visible to 2.1 million other Facebook users.131 In other words, being part

126 Shah and Kesan, “Setting Online Policy with Software Defaults,” 996. Also see the elucidating graph on p. 998.


128 Brendan, footnote 128: “In certain instances, the initial assessment made by the controller may be the subject of regulatory scrutiny even before the processing is initiated. Under the current framework, this may be the result of a ‘prior checking’ mechanism adopted pursuant to article 20 of the Directive. In the proposed regulation, it is similarly foreseen that certain forms of processing require prior consultation with and/or authorization by a supervisory authority. See in particular article 34 of the ‘Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’, Brussels, 25 January 2012, COM(2012) 11 final 2012/0011 (COD).”


130 Mayer-Schönberger quotes the – now well-known – ‘Drunken Pirate’ example, where a student teacher was denied her degree because of a photo she posted on MySpace. The photo was titled ‘Drunken Pirate’ and featured the student teacher with a pirate hat and plastic cup. See: Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press, 2011), 1 et seq.

of a group and/or a profile’s visibility to that group conflicts with user expectations and should not be the default. The main principle that personal information should only be visible to pre-selected contacts was re-confirmed by the Irish DPA\textsuperscript{132} as well as the Council of Europe\textsuperscript{133} and Article 29 WP.\textsuperscript{134}

These examples clearly illustrate that user expectations (and thus the recommendable ‘privacy friendly’ defaults) depend on a lot of different elements. These factors can generally be subdivided into two sub-categories: (1) personal attributes of the data subject and (2) the nature of the data and the purpose for which it is processed. Other elements that the SNS will have to take into account – mainly legal provisions, technical limitations and market incentives – will be evaluated in the chapter on implementation (infra).

\textit{i} \quad \textbf{Personal attributes}

As mentioned before, user expectations of how their privacy is protected will often depend on a variety of elements such as the culture, age, awareness, etc. Social networks are by nature very well placed to customise the default settings to the end-user. This will be particularly relevant with regard to default settings of minors (which should, arguably, be more restrictive\textsuperscript{135}). Nevertheless, it will be important not to differentiate too much either, as this might induce uncertainty. The main criterion should be whether noticeable differences in privacy expectations can be distinguished between large sub-sets of users.

\textit{ii} \quad \textbf{Purpose and Nature of Data (Processing)}

\textbf{Nature of the Data} – Expectations do not only differ depending on the individual’s personal background, but will also depend on the context,\textsuperscript{136} and type of information processed. Consequently, different types of (information) processing – such as facial recognition technology\textsuperscript{137}, geo-location data, the visibility of pictures – might be subject to different defaults. SNS should be extra cautious with regard to so-called ‘sensitive data’ (\textit{supra}). Arguably, this kind of data should not be shared by default.

\textsuperscript{132} Irish Data Protection Commissioner, \textit{Facebook Ireland Report of Re-audit}, 24.


\textsuperscript{136} Nissenbaum, “Privacy as Contextual Integrity”; Nissenbaum, \textit{Privacy in Context}.

\textsuperscript{137} According to the Article 29 WP, registered SNS users should not have their ‘reference template’ be enrolled in the identification database by default. This means that they cannot be automatically recognised (and subject to Tag suggest) when someone uploads a picture featuring that person.

The working party also specified that, when facial recognition is used as an ‘access control system’, an equally secure but less privacy intrusive alternative (e.g. strong password) should be available \textit{and} be the default.

\textit{See: Opinion on Facial Recognition, 5–6.}
Users’ expectations on what should(n’t) be considered sensitive data might vary too and will usually be broader than the categories mentioned in the Data Protection Directive (art.8). According to GRIMMELMANN, for example, end of relationship status updates should not be shared by default.138

ROLE OF THE SNS – End-users are often confused between two major roles of the social network provider. On the one hand the SNS acts as a mere agent under the authority of the user. The user decides on the use of the data and the social network provider merely acts as a technical facilitator, making the relevant actions possible. On the other hand, most SNS also process user data for their own purposes. This is the result of the typical social network business model, which generally relies on (behavioural) advertising as its main source of revenue. Users’ expectations of privacy protection will generally be different with regard to either one of these different roles. The second role in particular will raise most concerns.

The distinction between these two roles is epitomised in the social plug-in tracking debate. As mentioned supra (Do Not Track), SNS users are tracked by default on every website visited that has incorporated a relevant social plug-in, even when the user has previously logged out of the network. The social network provider mainly uses the data for its own purposes (behavioural marketing). These practices, especially when a user has deliberately logged out of the social network, seem to violate user expectations and should – arguably – be turned off by default.139 As a second example, it is worth referring to sensitive data (supra). Although social networks might not actively solicit this kind of data, there is a significant chance that users will upload such data on their own initiative. When this is the case, the argument could be made that the social network cannot use this data for its own purposes (obviously it will still process the data for the individual’s purposes).140

THIRD PARTY ACCESS – Many social networks have opened up their platform to third party developers. In general, third parties need to request access to your personal details. Usually consumers will only be able to use the service if they accept their data to be shared with this third party. Facebook has been criticised for their sharing settings not being fine-grained enough. The minimum amount of information that will be shared with the third party developer already includes the user ID, name, profile pic, gender, age range, locale, networks, list of friends and all public information.141 Arguably, these settings should be more granular. On top of that, default settings should limit the data being shared to what is absolutely necessary for the (third party) service to function.

A travel app, for example, should get access to location data, but not (necessarily) to the user’s relationship status. Apps containing age-restricted content should, by default, not have access to the exact age but only to the age range (e.g. under/over 18). It has also

138 The author describes it more eloquently, saying that “Breakups should be opt-in, not opt-out.” See: Grimmelmann, “Saving Facebook,” 1200.
139 Although one could still question the merit in this, “social networks have ample opportunity to collect consent from their members directly on their platform if they wish to conduct such tracking activities, having provided their users with clear and comprehensive information about this activity.” See: Opinion 05/2012 on Cloud Computing (Brussels: Article 29 Working Party, July 1, 2012), 9, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.
140 Luckily, Facebook announced it would not process sensitive data (mentioned in the DPD). See: Irish Data Protection Commissioner, Facebook Ireland Report of Re-audit, 17.
141 Irish Data Protection Commissioner, Facebook Ireland Report of Re-audit, 18–19.
been argued that social network profiles by default should not be indexable by (external) search engines.\textsuperscript{142}

It is also important to remember that the different roles of one controller (made in the previous paragraph) is equally relevant to third parties gaining access to the user’s personal data. In short, different relationships beget different expectations. According to the information commissioner from Ontario, Canada, a so-called ‘push model’ – in which the user decides what data is shared, when and with whom – will always be the most privacy friendly.\textsuperscript{143} In this line of thinking, several official bodies have advocated to limit the sharing of information only to self-selected contacts by default (see \textit{supra}).

\textit{iii Conclusion}

After having made the choice to put in place adjustable settings instead of wired-in settings (\textit{supra}), the social network will have to decide on the default values of these settings. The most user-friendly way to do so will be by evaluating and incorporating user expectations. This does not necessarily mean the social network provider should set all defaults to ‘maximum privacy’. Putting in place the most privacy preserving, closed down default settings when a profile is first set up seems contradictory to the very \textit{raison d’être} of social networks (\textit{supra}).\textsuperscript{144} After all, users subscribe to social network services in order to share and publish personal information.\textsuperscript{145}

As became clear from the above, identifying and understanding user expectations is not always an easy task. Common sense and general principles such as fairness and proportionality will often be a good starting point, but more work still needs to be done in order to systemise the interpretation of user expectations.\textsuperscript{146} The above tried to make a modest contribution to this challenge by identifying two major factors that can influence user expectations: personal attributes and context (or purpose and nature of data processing).

\section{4. Implementation}

The previous Chapter tried to provide a framework that could help determine privacy-friendly default settings on social networks. This Chapter will evaluate and


\textsuperscript{144} Kesan and Shah, "Setting Software Defaults," 7.

\textsuperscript{145} It must be said, however, that some have argued that having the most conservative default privacy settings, might well force users to learn how to make use of them before they moved on to networking. (…) It is unlikely, however, to be an option the SNS industry, or even users themselves, would favour.” See: Edwards and Brown, "Data Control and Social Networking," 22.

\textsuperscript{146} The field of Human Computer Interaction (HCI) might be very useful to this extent. Researchers would begin with a theory or framework that they think best captures the relationship between users and their potential privacy concerns and can refine it as appropriate after subjecting it to testing and analysis. See: Ibid., 1023-1024.
describe on what legal provisions and self-regulatory principles these settings can be based.

4.1 Law

a Data Protection

On a European level, there are two important documents that are relevant to default settings (from a data protection perspective): the Data Protection Directive (DPD) and the ePrivacy Directive. Early 2012, the European Commission issued a proposal for a new Data Protection Regulation, which would be directly applicable in all member states.**147** Put briefly, most of the personal data processing activities in a social networking context will fall under the scope of application of the DPD (art.2). The ePrivacy Directive’s scope of application is a bit narrower and will only cover certain aspects of the SNS’ activities.**148** This chapter will evaluate the concepts (in the above mentioned documents) that might form the legal basis of privacy friendly default settings on social networks.

i Fairness

The DPD explicitly prescribes that personal data must be processed fairly and lawfully (art.6(a))**149**. As mentioned supra, concepts such as fairness and proportionality are gaining more traction in policy debates (due to failure of consent framework to protect privacy and personal data in a satisfactory way). The same article in the DPD also sets down the purpose limitation principle, according to which personal data can only be processed for specified, explicit and legitimate purposes. These general and broad obligations aim to make the data controller (in casu, the social network provider) more accountable for its actions. Instead of making light of their obligations through the easily obtained consent of the data subject, they try to force the controller to put in place better safeguards. Privacy-friendly default settings, as defined supra, would undoubtedly be an efficient way to make data processing on social networks more fair, proportionate and limit undesired uses.

Default data retention periods, for example, might be based on the purpose limitation principle. In 2012 the Irish DPA recommended Facebook to delete by default all personal data received through social plug-ins within 90 days after a person has visited a website that includes such a plug-in. User-identifiable search logs should be removed by default after 6 months.**150**

ii Consent/legitimacy of processing

Social networks generally rely on consent to legitimise the use of personal data (art.7(a) DPD; art.6(1)(a) DP Reg.). Adjustable privacy settings in particular might serve as an additional way to obtain consent for certain specific types of uses of personal data. Because of their adjustability, settings can be understood as the

**147** The proposal is still being debated heavily and will be subject to many changes. For more information, see: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
**148** The ePrivacy Directive aims to protect privacy ‘with respect to the processing of personal data in the electronic communication sector’ (art1(1)). Types of data covered include: traffic data and location data.
**149** Article 5 in the Proposal for a new Data Protection Regulation.
expression of the user’s will. Consent obtained in this manner might even be considered more ‘specific and informed’ than ticking the box under a long and legalese privacy policy. This leads to the debate on opt-in versus opt-out consent, which goes beyond the scope of this deliverable.\textsuperscript{151} Suffice to say that when opt-in is required/preferred (e.g. sensitive data), the social network might opt for a penalty default (\textit{supra}) or a very privacy conservative default setting.

The Article 29 Working Party has indicated that consent (in the meaning of the DPD) cannot be obtained through pre-ticked boxes. This also applies to browser settings that accept tracking cookies by default. Since it was amended in 2009, the ePrivacy Directive (art.5(3)) requires an affirmative action in order to obtain consent for using (tracking) cookies.\textsuperscript{152} The Working Party did specify that explicit consent is \textit{not} required when visiting a website containing a social plug-in, \textit{and} the user is logged in on the SNS. On the other hand, social plug-ins cannot place tracking cookies when users have logged out of the social network or when the visitor is not a user of the social network at all. In any case, these cookies need to be session-cookies by default. When the SNS wishes to use them for additional purposes, separate consent must be obtained.\textsuperscript{153} The German e-zine Heise.de has implemented a practical technical solution on its website. Facebook's Like button is greyed out by default, and only becomes active (and sends data back to Facebook) when the user clicks on it.\textsuperscript{154} Finally, according to the Article 29 Working Party, permissive privacy default settings on social networks (e.g.: uploaded content is automatically shared with friends of friends) cannot be considered as unambiguous consent.

\textit{iii} \quad \textit{Obligation to Inform}

Social network providers – and data controllers in general – will have an obligation to provide certain information (such as the identity of the controller or purpose) to the individuals they are processing data from (Art. 10-11 DPD; Art. 11 \textit{et seq.} DP Reg Proposal). This obligation might (partly) be fulfilled by the use of penalty defaults (when the default value is zero). The user might, for example, be forced to make a decision on the third parties his/her personal data may be shared with.

\textit{iv} \quad \textit{Security}

Data controllers are also required to ‘implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing’ (art.17(1) DPD; art.30 DP Reg Proposal). Taking into account the costs and state of the art, these measures shall be appropriate with regard to the type of data (processing). This obligation of security can be seen as yet another legal ground for privacy-friendly default settings. After all,
the best way to prevent security flaws and data leaks is to limit the collection/sharing of personal data. Another way to implement this obligation is to encrypt all personal data (traffic) by default.

Currently, Facebook has a range of security measures/features turned on by default (e.g. log-in credentials, https, etc.). But the network also provides some extra security features to which the user can opt in (e.g.: login notifications; login approvals; active sessions; one-time passwords).\textsuperscript{155}

\textbf{v Towards a ‘Privacy by Default’ Provision?}

“[Social Network] Providers must take account of the principle of ‘privacy by default’, which means that the default settings should be those that provide the most privacy.”\textsuperscript{156}

The proposal for a new Data Protection Regulation, proposed by the Commission in January 2012, explicitly lays down a provision (Art. 23) on ‘Privacy by Design and Default’ (supra). Not only should social networks implement safeguards into the design from the ground up, “privacy-protecting default settings [...] should be the norm.”\textsuperscript{157} Although nothing more than a proposal (yet), the article clearly indicates the intent to introduce such an obligation in the next-generation legal framework on data protection. In recital 61\textsuperscript{158} of the proposed Regulation, the Commission further specifies that data controllers (social networks) should also “adopt internal policies and implement appropriate measures” as to ensure ‘privacy by default’. Finally, national DPA's will have the task to monitor data controller’s compliance with the principle (Art. 37(1)(c)).

Notwithstanding these general provisions, the proposal does not go any further as to how these ‘privacy-friendly default settings’ should look like in practice. If the provision survives the current revisions and is included in the final data protection reform package, more clarifications would be welcome.

\textbf{b Consumer protection}

At first sight it seems that the legal basis for privacy-friendly default settings is to be found in privacy and data protection law. But, (privacy) settings also constitute an important element in the (contractual) relationship between the individual and the social network provider. As a result, consumer protection rules may be applicable as well. Because of the existence of an elaborate data protection and privacy protection framework, this avenue has not really been developed in EU policy debates (yet). In

\textsuperscript{155} Irish Data Protection Commissioner, \textit{Facebook Ireland Report of Reaudit} ("FTR Solutions Report"), 10.
\textsuperscript{156} European Commission, “How Will the Data Protection Reform Affect Social Networks?”.
\textsuperscript{158} “The purpose of the recitals is to set out concise reasons for the chief provisions of the enacting terms, without reproducing or paraphrasing them. They shall not contain normative provisions or political exhortations.” For more information, see “Recitals,” \textit{Joint Practical Guide of the European Parliament, the Council and the Commission}, http://eur-lex.europa.eu/en/techleg/10.htm.
the USA, on the other hand, consumer protection rules have often been used in order to protect privacy and data protection (most likely because the country does not have a general data protection framework). Hence, it makes sense to briefly elucidate the situation in the USA before evaluating EU law.

i. USA

In the USA, the Federal Trade Commission (FTC) is the primary agency promoting and defending consumer protection. It is also the de facto agency for most consumer privacy related matters. Most recently, for example, it has strengthened the protection of children’s privacy on the Internet. One of the key powers of the FTC is to investigate and prevent unfair and deceptive trade practices. These investigations – and potential prosecutions – can be instigated by formal complaints by individuals and consumer organisations (among others).

In May 2010, the Electronic Privacy Information Center (EPIC) filed such a complaint. According to the Center, Facebook’s privacy policy changes constituted ‘unfair and deceptive acts and practices’. EPIC claimed that:

(a) Facebook disclosed users’ personal information to Microsoft, Yelp, and Pandora without first obtaining users’ consent;
(b) Facebook disclosed users’ information—including details concerning employment history, education, location, hometown, film preferences, music preferences, and reading preferences—to which users previously restricted access; and
(c) Facebook disclosed information to the public even when users elect to make that information available to friends only.

Additionally, EPIC also asserted that the material changes and misrepresentations in Facebook’s privacy policy are harmful to consumers. It was argued that data was disclosed and used for other purposes than consented to, falsely making consumers believe they are in control over their personal data.

---


160 Under US law, trade practices are unfair when they: (1) injure consumers; (2) violate established public policy; (3) are unethical or unscrupulous. To be considered as ‘injuring consumers’, the injury must be “substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.” See: Federal Trade Commission, “FTC Statement on Unfairness”, December 17, 1980, http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

161 To be regarded as deceptive: (1) practices must be a representation, omission or practice that is likely to mislead the consumer; (2) from the perspective of a consumer acting responsibly in the circumstances; and (3) the representation, omission or practice must be material (likely to affect the consumer’s choice and behaviour). See: Federal Trade Commission, “FTC Statement on Deception”, October 14, 1983, http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

162 Section 5 of the Federal Trade Commission Act (15 USC §45).

163 EPIC, “Before the FTC, In the Matter of Facebook Inc, Complaint, Request for Investigation, Injunction, and Other Relief.”

164 Ibid., 1.

165...and undermining the ability of users to avail themselves of the privacy protections promised by the company.” In: Ibid., note 140.
One of the contentious activities concerned a pop-up screen Facebook had presented to its users earlier that year. Users were informed that their profile could be linked to certain preselected (brand, music, movie, etc.) pages. A choice had to be made between the following three options: 'Link all to my profile'; 'Ask me Later'; and 'Choose Pages Individually'. The first option was made extra visible and the last option was written in a smaller, unnoticeable font. Some users were not even presented the choice, but only received an announcement that their profiles were matched to 'related pages' automatically (by default).166

Additionally, the adjustments users made with regard to the visibility of certain information, only applied to the profile page itself. In other words, Facebook would obscure the information when someone visits the user’s profile page, but the same information would still be disclosed elsewhere (e.g. friends’ pages, third party websites, etc.).167

In November 2011, the Federal Trade Commission came to a settlement with Facebook. In short, the social network will have to obtain prior consent from its users for changes in its privacy policy (opt-in) and it will be subject to periodical, independent review for the next 20 years.168 Facebook will not be allowed to put in place defaults that would clearly contradict users’ existing privacy configurations. Also, Facebook will have to implement ‘controls and procedures appropriate to [Facebook]’s size and complexity, the nature and scope of [Facebook]’s activities, and the sensitivity of the covered information’. Undoubtedly this settlement has an important impact on the determination of privacy-friendly default settings. Not just for Facebook, but for social networks in general.

**ii Europe**

As mentioned before, the need to protect personal data and privacy through consumer protection rules is less relevant in Europe, due to the extensive data protection (and privacy) legal framework in place already. Nevertheless, it might be interesting to briefly analyse to what extent consumer protection rules might be used as the legal basis for privacy-friendly default settings.

The key legislative document in the European Union is the ‘Unfair Commercial Practices Directive’ from 2005.169 This Directive includes a couple of provisions that might be relevant to default settings on social networks:

(a) Article 6: According to this article, a misleading practice contains false information and is ‘untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer’ (even if the information

---

166 Ibid., 9–12.
167 Ibid., 15.
is factually correct) and causes him/her to ‘take a transactional decision that
he would not have taken otherwise’.
(b) Article 7: A commercial practice can also be misleading if it omits material
information that the consumer needs to take an informed decision.
(c) Article 8: Commercial practices may be regarded as ‘aggressive’ when it
significantly impairs the average consumer’s freedom of choice through
(among other things) undue influence.

It does not require a lot of imagination to see how the practices of a social network
might fall under either one of these descriptions. Privacy-unfriendly default settings,
for example, could arguably be regarded as aggressive commercial practices (Art. 8).
When, in addition, these settings are well hidden and/or hard to adjust, they might
even be qualified as misleading (Art. 6-7). Consequently, users could – with the help
from consumer organisations that have the required means and resources – challenge
these practices before Court and benefit from the protective consumer law
framework.\footnote{Kuczeraw and Coudert, “Privacy Settings in Social Networking Sites,” 240.}

Finally it must be said that there are no known cases where SNS privacy (default)
settings were successfully challenged via the route of consumer protection law. This is
probably the result of the comprehensive data protection framework that constitutes
a more obvious avenue to dispute questionable privacy practices. Nevertheless,
consumer protection law constitutes an attractive alternative as it might lead to
pecuniary compensation. Only time will tell if European judges agree.

\subsection{4.2 Self-Regulation?}

Besides the law, self-regulation might also contribute to greater privacy-friendliness
of default settings. In April 2012, the Council of Europe explicitly stated that self- and
coreregulation \textit{can} be part of the solution.\footnote{Committee of Ministers, \textit{Recommendation on the Protection of Human Rights with Regard to Social
Networking Services}, note 6.} Shah and Kesan have even stated that policy
makers should avoid intervening and developers should rely on the ‘would
have wanted’ standard (\textit{supra}).\footnote{Shah and Kesan, “Setting Online Policy with Software Defaults,” 1004. The authors believe that legal
intervention is only justified when: a) the default’s topic is inappropriate; (b) when users lack
knowledge or ability to change important defaults; (c) defaults cause harm to third parties; (d) defaults
do not comport with existing law or policy.} Nevertheless, it is dangerous to rely on self-/co-
regulation too much, as the business models of most online social networks largely
depend on targeted advertisement (monetising personal information).\footnote{OECD, \textit{The Role of Internet Internet Intermediaries in Advancing Public Policy Objectives}, Workshop

A great example of these conflicting interests and why the market might ‘fail to
produce privacy friendly options for consumers’, can be read in a 2011 book by Douglas
Edwards, an ex Google-employee: ”What if we let users opt out of accepting our cookies
altogether? I liked that idea, but Marissa [Mayer] raised an interesting point. We would
clearly want to set the default as “accept Google’s cookies.” If we fully explained what that
meant to most users, however, they would probably prefer not to accept our cookie. So
our default setting would go against users’ wishes. Some people might call that evil, and
evil made Marissa uncomfortable. She was disturbed that our current cookie-setting
practices made the argument a reasonable one. She agreed that at the very least we


should have a page telling users how they could delete their cookies, whether set by
Google or by some other website.”

Nevertheless, voluntary (non-legal) efforts can still play an important role in
producing privacy-friendly (default) settings for users of social networks. In 2009, for
example, a group of major social networks set up a list of guidelines together with the
European Commission’s Social Networking Taskforce. One of them encouraged SNSs
to make profiles of minors unsearchable, set the visibility of their profiles to private
by default, etc.\(^\text{175}\) Do Not Track is also a great example of how a voluntary standard
can evolve into a sector-wide standard that ensures (to some extent) the privacy of
consumers.\(^\text{176}\) Although many browsers now include an option not to be tracked, this
box is not selected by default. Apple’s browser Safari does block third party cookies
by default though.

Finally, it should be stressed that privacy-friendly default settings do not necessarily
have to conflict with the social network’s business model. Such privacy-friendly SNSs
already exist, usually targeting privacy-conscious niches (e.g. gay people, religious
groups, etc.)

5. Conclusion

This paper tried to lift the veil on the often unclear and contentious subject of privacy-
friendly default settings. It became clear that default settings have an important role
to play with regard to the protection of privacy and data protection in a social
networking environment. Particularly on social networks, managing one’s privacy and
personal data feels unnatural and is ignored by many users. In order to avoid abuse of
this general passiveness, policy makers are developing general principles such as
fairness, proportionality and accountability. Proper default settings constitute a
straightforward and practical technique to make social networks more privacy
friendly without putting the onus on end-users too much. Existing legislation already
provides a legal basis for privacy-friendly default settings and the future data
protection framework (currently being debated) will strengthen this even further.
There is no doubt that the widespread use of privacy-friendly default settings on
social networks will be a challenging goal to achieve. Not in the least because many
SNS providers depend to a great extent on revenues generated through the use of


\(^{175}\) European Commission - Social Networking Task Force, “Safer Social Networking Principles for the
principles-eu.

\(^{176}\) Since W3C in December 2011, the Article 29 Working Party has been actively participating in the
debates to standardise the technology and meaning of DNT. See: *Opinion on Cookie Consent Exemption*,
10. European Commissioner Neelie Kroes has also addressed DNT in a recent speech. See: Kroes,
“Online Privacy and Online Business: An Update on Do Not Track.”

\(^{177}\) See for example kaioo.com, where privacy is seen as a key selling point: described at
iht.com/articles/2007/12/02/technology/network03.php.” Also see: Bebo, “a leading SNS for young
children, individually and manually vets the user profiles of every one of its young user base, to provide
their users’ personal data. Efforts will have to be made by policymakers, technologists and the sector itself. But if everyone works together, a constructive solution can definitely be found, satisfying both users and providers of social network services.