Chapter 1
We Are All Connected to Facebook . . . by Facebook!

Arnold Roosendaal

1.1 Introduction

Tracking and tracing users over the web is a valuable tool for profiling purposes. Based on revealed interests, web users can be targeted for personalized advertisements. Companies that earn their revenues from targeted advertising have a huge interest in using these techniques. It is therefore not surprising that the way these techniques are exploited becomes more and more sophisticated.

The use of cookies and third-party cookies to recognize and track and trace web users is not a new concept (see Dwyer 2009; Martin et al. 2003). Usually, cookies are placed on the user's web browser without any direct visibility. A cookie is a small text file and the process of placing it on the browser is executed without user interaction. The presence and origin of the cookies is not revealed until a user checks his cookies via his browser options. In order to let third-parties place cookies, they have to be allowed to place content on a website. The content is requested from the web server of the third party and is delivered along with a cookie. When a site is visited again, the cookie is sent along in the request for the content. This allows content providers to 'remember' preferences of web users, such as language settings or purchasing history, and to provide the web content according to these preferences. A web browser is recognized through the cookie, which allows the web activity to be monitored.

In order to gain as much reach over the web as possible, the technologies for tracking have become very sophisticated. Sophistication can, however, also be in the presentation of a tracking tool. For instance, Facebook offers content providers to place a Like button on their website. This button is a tool which allows Facebook members to indicate that they like a certain website or item on a website. By clicking the button, a link to the item is placed on their Facebook profile page. In addition, the number of visitors who 'liked' something is indicated next to the button. For content

A. Roosendaal (✉)
Tilburg Institute for Law, Technology, and Society (TILT),
Tilburg University, Tilburg, The Netherlands
e-mail: a.p.c.roosendaal@tilburguniversity.edu

S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*,
DOI 10.1007/978-94-007-2903-2_1,

providers, the Like button can thus function as an important business tool, because website visitors can contribute to attracting more visitors to a website. This makes the tool valuable for content providers, which is also reflected by the fast increase in web coverage of the Like button. However, even though presented as a nice feature for content providers, the Like button is also used to send cookies and to track and trace web users, regardless of whether they actually use the button. The browsing behavior of individuals can be connected to their Facebook account. If a user has no Facebook account, a separate set of data concerning individual browsing behavior can be created. When a user creates an account later on, the data can be connected to the newly established profile page.

The practice of massively collecting data concerning individual web behavior is an important phenomenon in the Internet realm. It hugely affects the way companies, people, and privacy mutually relate to each other and, at a fundamental level, it influences the abilities of individuals to construct their own identities. The fact that individuals value their privacy and object to these practices also becomes clear from the class action law suit against Facebook, which was filed in California.[1]

In this chapter, the effects on privacy and identity of individuals resulting from hideous tracking technologies will be described. First, a further introduction to the Facebook Like button and its value will be given in Sect. 1.2. In Sect. 1.3, the technical process of placing and replacing cookies with the help of the button will be described, as well as how this facilitates profiling. Subsequently, the way this practice affects the privacy of individuals will be discussed in Sect. 1.4, and finally a conclusion will be drawn in Sect. 1.5.

1.2 The Facebook Like Button

The Facebook Like button is an image displaying a thumbs-up symbol accompanied by the word 'Like.' According to Facebook, "[t]he Like button lets a user share your content with friends on Facebook. When the user clicks the Like button on your site, a story appears in the user's friends' News Feed with a link back to your website."[2] Anyone can display the button on his website by simply implementing the code which is available for free. The button can thus be used by content providers to have web users promote content and create links on their Facebook profile pages. When clicking the Like button, a login field opens in a pop-up window to log on to Facebook. Logging on results in the creation of the link on the Facebook profile page. When a user is already logged on to Facebook, the creation takes place immediately.

In April 2010, at their f8 conference, Facebook announced Instant Personalizer and Social Plugins, two services that allowed partners to leverage the social graph—the information about a user's relationships on the site that the user makes available

[1] Ung vs. Facebook, Class action complaint, Superior Court of the State of California, County of Santa Clara, Case No. 111CV200467, filed 05/09/2011.

[2] "Like Button—Facebook Developers," accessed 22 March 2011, http://developers.facebook.com/docs/reference/plugins/like.

to the system—and provide a channel for sharing information between Facebook and third parties. For example, websites could implement a Like button on their own pages that enables users to share content from that site with their connections on Facebook (boyd and Hargittai 2010). The value of displaying the Like button on a website becomes clear from the statistics. Sites that have added such social plugins from Facebook reported increases in traffic in excess of 200%. Besides, the time spent and the number of articles read on websites with Like buttons also increased by over 80%.[3] The button represents 12.9% of the distribution of third-party widgets.[4] It also appears that, within months, the use of social plugins had reached millions of sites.[5] The penetration rate of the Like button in the top 10,000 websites reached over 4% in the first six months after its introduction,[6] and it is likely that it will continue to grow.

While the Like button can help content providers to generate traffic to their websites, it is also a tool for Facebook members to add information about their interests to their personal profile page. Thus, it fits perfectly in the ongoing trend of social networking sites like Facebook encouraging members to share personal information.[7] Obviously, for sharing items from the web, the Like button is a very useful tool, because it allows direct linking without having to copy and paste complete URLs and the content is made up in a readable manner automatically.

1.3 Cookies, Recognition, and Identification

As indicated, there are numerous third parties which deliver content to websites and place cookies. Usually, the function of these third parties is to provide website providers with content such as advertisements or specific functionalities like maps or videos. A piece of content is delivered from the servers of the third party and can be sent together with the cookie. The cookies can be used to generate information on the number of visitors and which items on a website attracted the most attention. In this way, third parties can provide a service to the website provider. A web user is usually not aware of this. He just types in the URL of the website he wants to visit and the

[3] "The Value of a Liker—Facebook," accessed 22 March 2011, http://www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797.

[4] "Facebook Like Box Usage Statistics," accessed 22 March 2011, http://trends.builtwith.com/widgets/Facebook-Like-Box.

[5] "Facebook Stats Likers," accessed 29 Sept. 2010, http://www.insidefacebook.com/2010/09/29/facebook-stats-likers/.

[6] "Facebook Like Usage Statistics," accessed 22 March 2011, http://trends.builtwith.com/widgets/Facebook-Like.

[7] There are, however, more privacy friendly initiatives which focus on audience segregation and controlled disclosure of personal information. For instance, Clique allows users to have several 'faces' in one account. See http://clique.primelife.eu/. This social networking site is one of the results of the EU FP7 PrimeLife project.

page is loaded. That the loading of the page involves numerous HTTP requests[8] for content from the servers of the visited websites and often several third-party servers is a process which takes place behind the scenes. Or, in more popular terms: that is where the magic happens!

A cookie is placed on the web user's computer via his browser. Each cookie is connected to a web server, so only the server from which the cookie was sent has access to the cookie. The provider of a website does not have access to other cookies placed by third parties via his website. Once a cookie is available on the user's computer, this cookie will be sent together with the HTTP request in each later request for content from the server which installed the cookie. The HTTP request also includes data on the referrer, which is the website on which the content will be displayed. Since the referrer data is always included, third parties can follow exactly which sites a user visits. When data concerning web visits are combined based on the unique cookie, the browsing history of a web user can be mapped. The content is needed to load a page so, for tracking purposes, it is irrelevant whether a user actually clicks a piece of content or not, or whether the content is clickable at all.

1.3.1 Scenarios

The Facebook Like button is also a piece of third-party content. The website provider does not directly place an image of this button on his website. In fact, the button is a piece of HTML code which includes the request to the Facebook server to provide the image when the website is loaded. This implies that the button can be used to set third-party cookies or to recognize them as well. A few different scenarios can be distinguished: (1) a web user has a Facebook account, (2) a web user does not have an account, (3) a web user becomes a member of Facebook, and (4) a member deletes his account. These scenarios have been tested in a practical experiment using Techcrunch.com, CNN.com, and Gizmodo.com.

1.3.1.1 The Web User Has a Facebook Account

The first option is a scenario in which the web user has a Facebook account. When the account is created, Facebook issues a cookie, containing a unique user ID, to the computer of the user. This cookie facilitates the display of a username in the login field at returning visits. When accessing Facebook from another device, a temporary cookie is issued, which is replaced by a cookie with the same ID after logging on to the account. In this way, different devices can be linked to one account and thus one user. Every time the user visits the Facebook website, the cookie is sent together

[8] HTTP stands for Hyper Text Transfer Protocol, the programming language used for internet traffic. An HTTP request is a request for a specific piece of content sent from the user's computer to a web server. The web server replies by sending the requested content. If the content is not available, the reply includes an error code.

```
GET
/plugins/like.php?href=http%3A%2F%2Fwww.facebook.com%2FGizmodo&layout=button_co
unt&show_faces=false&width=200&action=like&colorscheme=light&height=21 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.2.10) Gecko/20100914
Firefox/3.6.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://gizmodo.com/
Cookie: datr=yjPATCXPQuDBLU_J5ZfRsJpd; lu=TgbyaYN2Obo-F4fEBiQTGtwQ;
locale=en_GB; x-
referer=http%3A%2F%2Fwww.facebook.com%2Fhome.php%23%2Fhome.php;
cur_max_lag=20; c_user=100001XXXXXXXXX; sct=1287731574; sid=0;
xs=55dcbdfe4719c2693d477d0c0dd83ab6
Cache-Control: max-age=0
```

Fig. 1.1 The HTTP GET request for the Like button on Gizmodo.com, including the cookie with user ID (anonymized by the author)

with the HTTP request for the site. As a result, Facebook already knows who wants to log in before the actual login has taken place.

However, the cookie is not only sent to the Facebook servers when a member logs on, but also on every occasion when content such as the Like button has to be provided from the Facebook servers (Fig. 1.1). Thus, every single time a website containing the Like button is visited; Facebook receives information concerning the user, including his unique ID, via the cookie. If the user actually clicks the button, he has to provide his Facebook login details, and a message about the 'Like' is posted on his profile page.

Users are often not aware of the fact that data about the user are sent to Facebook regardless of whether the Like button is actually clicked. The cookie contains the unique user ID and thus allows information on browsing behavior to be connected to the account. Even though the user is not involved, Facebook can collect far more individual data than the data made available on the profile page only.

Below is an example of a request for the Like button where the cookie including a unique user ID is sent along.

In this scenario, there is a link between the Internet user and Facebook because there is an account. Now, consider a scenario where there is no membership link.

1.3.1.2 The Web User Does Not Have a Facebook Account[9]

If a user does not have a Facebook account, there is no cookie and no user ID available. A visit to, for example, Techcrunch.com includes an HTTP GET request

[9] This scenario does not apply anymore since Facebook changed its systems after the publication of my initial research findings (Roosendaal 2010). In a communication to the Hamburg Data Protection Authority (Germany) Facebook stated that the tracking of nonusers was the result of a 'bug' in their software development kit.

1. Set-Cookie: datr=ckviTDm3989eNbvw6xMhAWle; expires=Thu, 15-Nov-2012 09:14:26 GMT; path=/; domain=.facebook.com
2. Set-Cookie: datr=ckviTC8tNJ-1ZKqCu_Srlga7; expires=Thu, 15-Nov-2012 09:14:26 GMT; path=/; domain=.facebook.com

Fig. 1.2 A cookie issued via Facebook extern login status (1) and one via Facebook Connect (2) on Gizmodo.com

for the Like button. However, in this scenario, when the button is provided, no cookie is issued. Thus, it seems that the Like button itself is not used to issue cookies. However, when a site is visited which includes Facebook Connect (for instance Gizmodo.com), this application does issue a cookie (Fig. 1.2). From that moment on, visits to other websites which display the Like button result in a request for the Like button to the Facebook server including the cookie. An important part of the process depends on visiting a site which has implemented Facebook Connect. The chance of visiting such a site is considerable. Within a year from its launch in December 2008, Facebook Connect was used on almost 1 million websites and in March 2009 over 40 million unique visitors of Facebook Connect implementations were registered (Burbary 2009). The number of implementations increases exponentially, so the likelihood of accessing such a website is increasing at a fast pace as well.

As indicated, after visiting a website on which Facebook Connect has been implemented, the request for the Like button includes a cookie. This cookie has an expiration date two years from the moment it was issued. However, by browsing across websites, additional cookies can be placed on the user's computer and these can be added later on in new requests. Not all cookies are used in this way. For instance, a cookie issued via the extern login status plugin is not included in later requests.

Based on the cookie, the entire web behavior of an individual user can be followed. Every site that includes some kind of Facebook content will initiate an interaction with the Facebook servers, disclosing information about the visited website together with the cookie.

1.3.1.3 A User Becomes a Facebook Member

It is possible that a web user already has a personal set of data collected by Facebook, based on the mechanism described above. The question is what happens if this user creates a Facebook account. In that case, he first has to go to the Facebook homepage (login page). The cookie on the user's computer is sent to Facebook in the request for the web page to be loaded. The server responds and issues a few new cookies. These new cookies are temporary ones, or session cookies. When the account is actually created, a unique ID number is issued and sent in a cookie. The connection between this ID cookie and the old cookie is made behind the scenes by Facebook's servers. This means that the entire historical information of the user can be connected to the newly created Facebook account. From this moment on, all subsequent requests for Facebook content are accompanied with the unique user ID cookie.

If a user deletes all his cookies, the process starts from the beginning with Facebook Connect placing a new cookie when a site containing Facebook Connect is visited. From the moment on that the user accesses his Facebook account, or connects to this account by clicking the Like button and providing username and password, this cookie is replaced by a cookie containing the unique user ID that belongs to the account.

1.3.1.4 A User Deletes His Facebook Account

A last possibility is that an existing Facebook member decides to exit the network. In this case, the user can delete his account. Facebook offers an easy process to deactivate an account. Deactivation, however, is not similar to deletion. In fact, when an account is deactivated, the account and all its contents are only made unavailable to the network community. The entire account is kept by Facebook just in case the user decides to rejoin the network. In that case, the complete account, including all connections and contents can be reactivated. Clearly, during the inactivity of an account, Facebook is still able to connect data to the account in a way similar to when the account was active.

There is also an option to really delete an account. The deletion process includes a specific request to Facebook that takes two weeks to process. If the account is accessed in this period, the deletion process is stopped. After 14 days, accessing the account is no longer possible and the contents can no longer be retrieved. Whether Facebook keeps any information or even the entire account, probably disconnected from the login credentials, is unclear. However, even if the account is really deleted, the web user can still be tracked and the browsing data can still be connected to an individual data set. This means that, after deleting the account, all services which were connected to Facebook, for instance, by using the Facebook account to sign up, have to be disconnected as well and cookies have to be deleted. Once everything is cleared and disconnected, the web user can be considered to be someone who does not have a Facebook account and the scenario earlier described applies.

1.3.2 Recognition and Identification

Facebook uses cookies for recognition. Web users can be recognized whenever they visit a site with a piece of Facebook content. Facebook members are identified as individual account holders, because the cookie includes their unique user identification number. When different devices are used to access Facebook, such as a home computer, a laptop, or a smart phone, these devices are recognized as belonging all to the same individual, so all web interaction from these different devices is connected as well. Individuals who do not have a Facebook account are recognized as well. Their browsing behavior, however, is not connected to a Facebook account; besides, recognition is machine based and separated for every single device. Since there is

no unique user ID in the cookie resulting from a log-on to Facebook, the different devices cannot be connected solely on the basis of the cookies. Single devices can be quite reliable, however, even though they can be used by different persons. More and more devices, such as laptops and smart phones, become personal and are usually used by one single individual. This implies that information collected based on the cookies and browsing behavior results in a very personal profile. Obviously, Facebook can use this to provide their members with targeted advertisements. The information collected about the browsing behavior of nonmembers probably provides a larger sample for profiling and targeting purposes.

The Facebook Like button is not the only button which frequently appears on websites to facilitate sharing or promoting content. Other examples are Twitter's Tweet button, the Digg button, and Google's Buzz, but there are differences. As described above, Facebook Connect is the system that actually issues a cookie the first time. From that moment on, the cookie is sent together with all HTTP requests for content, so also when the Like button is uploaded onto a page. Thus, an additional system is used to initiate the cookie exchange. Twitter, for instance, does not have such a system. The Tweet button does not always send a cookie when the button is requested from the Twitter servers. Only if someone visits the Twitter homepage is a cookie issued which is used in future interactions with the servers, similarly as with the Like button. Logging on or even having a Twitter account is not necessary. A small but important difference with the Like button is that there is at least supposed to be some link to Twitter, because the web user has visited this website. For Facebook, this is not necessary at all, which implies that individuals who consciously choose not to participate in Facebook are still tracked and traced by Facebook. Even if someone does not connect to Facebook himself, Facebook makes the connection.

Another important difference is that Facebook can trace the browsing behavior to member accounts. These accounts are, usually, quite rich concerning disclosed information, but the Like button as exploited by Facebook allows far more information to be collected about individual members than the information disclosed on the personal profile page. Thus, people who have an account, but do not want to disclose much information are still profiled more extensively. Their browsing behavior discloses much information concerning personal interests, and this information can also be collected by Facebook and connected to the individual account. In the end, consciousness in disclosing information, either by not participating on Facebook or by very limited disclosure of personal information, is not sufficient to escape Facebook's tentacles.

An additional point of attention lies in the function Facebook is exploiting as an identity provider. An increasing amount of websites offers the possibility to register or log on with Facebook credentials.[10] The username and password are consequently used at places other than on Facebook only. Obviously, the services that provide this possibility are linked to Facebook as well. However, a more pressing issue is the fact that, for some web services, logging on is *only* possible with a Facebook account. This means that, without a Facebook account, accessing or using the services is simply

[10] For instance: www.slideshare.net.

impossible. If the amount of web services requiring a Facebook account increases, web users will become more dependent on Facebook as an identity provider so users can indirectly be forced to create an account.

1.4 Privacy Implications

The way the Like button is exploited and used to monitor web behavior of individual Internet users raises privacy concerns. In this section, it will be explained how privacy is affected and why this is troublesome. An important starting point in this respect is the link between privacy and identity. The construction of an own identity is only possible when an individual has some privacy. Keeping things private, or at least for some people, enables an individual to present himself in a way he wants and to set long term goals to achieve. Thus, privacy is instrumental to individual identity construction. Because privacy also enables the free and unrestricted determination of goals to achieve by the individual, it is also directly instrumental to individual autonomy. In this chapter, however, the focus will be on privacy and identity.

1.4.1 Privacy and Identity

Making choices and defining wishes and desires is closely related to identity. Identity is who you are as an individual and how you want to be seen by others, so it has an internal and an external element. The internal element can be described as how human beings acquire a sense of self (Hekman 2004, 22). The external element relates to social interaction with others. This interaction, however, is not always similar. When an individual wants to express himself and wants to present himself differently in different roles or contexts, control over data concerning him is a necessary condition. This is where privacy comes in. Agre defines privacy as freedom from unreasonable constraints on constructing identity and control over aspects of identity projected onto the world (Agre and Rotenberg 1997, 7). The world can be the world in general, but usually the world is divided into different contexts which are seen as separate audiences to which a certain (partial) identity or aspect of identity is projected. As Hekman puts it: "I am social in interaction with *specific* others, and understanding identity must attend to both the general (social) and the specific (individual). In other words, we are all embedded but we are all embedded differently at different locations" (Hekman 2004, 23). When approaching identity from a privacy perspective, the external element is the main focus. This is also reflected in Agre's definition where he speaks of projecting onto the world.

In the light of the foregoing, the two main aspects of privacy are informational self-determination and contextual integrity. Before delving into these particular aspects of privacy two open terms in Agre's definition will be briefly discussed. These terms are 'identity construction' and 'unreasonable constraints.'

1.4.1.1 Identity Construction

An important aspect of identity construction is role-playing (Goffman 1959); an individual plays a certain role in social interaction and the role and interaction give clues about the expected behavior of the individual. Depending on how the individual wants to be seen by others, he can decide to behave in accordance with expected behavior or to behave more or less idiosyncratically. This form of self-expression can help to change the way an individual is perceived by others.

A related aspect is audience segregation (Goffman 1959). Individuals tailor their behavior depending on their audience. For instance, the way a person behaves towards family members differs from his behavior in a working context. There are different partial identities for different contexts. An individual is thus always known by his audience as the identity that is shown in the specific context.

When data originating from different roles or contexts are collected and combined by one party, like Facebook, the individual is no longer able to keep roles and contexts separated. As a result, the individual is restricted in his ability to construct an own individual identity or partial identity. This will be further discussed in Sect. 4.2 below.

Given these main aspects of identity construction, it is now time to discuss what constraints on this construction may be unreasonable.

1.4.1.2 Reasonable and Unreasonable Constraints

The fact that the Agre/Rotenberg definition of privacy contains an element called unreasonable constraints implicitly indicates that there are reasonable constraints as well. In practice, I believe there is a sliding scale and that some constraints are definitely reasonable, some are definitely unreasonable, and the major part of constraints is somewhere in between. How reasonable or unreasonable a constraint actually is may depend on the specific circumstances in which there is a constraint. Because the infringement on privacy is taking place without the individual being informed, the reasonableness should be tested from the perspective of the individual user who is affected in his privacy and autonomy by the use of tracking technologies. The individual loses control over his personal data.[11]

Reasonable constraints can be defined as constraints that are defendable or foreseeable for the individual. Being able to predict a constraint or just knowing about it beforehand as well as being able to give grounds for the constraint is an indicator of a reasonable constraint. A clear example can be found in limits that are laid down in law, such as the limitations on fundamental rights. In specific circumstances, for example, involving public order or national security, fundamental rights may be restricted. This means that disclosing personal data to prevent an attack on the national

[11] Another reason to take the individual perspective is that privacy and data protection legislation is based on the privacy interest of individuals. Taking the perspective of a commercial company would come to a weighing of interests (conform Article 7(f) of the Data Protection Directive (Directive 95/46/EC)) and, thus, legally imply an assumption that the commercial business interest is a valid interest. At least, this assumption cannot be made in general.

government is a constraint, because the individual himself does not really have a say in this, but the constraint is reasonable given specific circumstances in which other interests should prevail. Another example directly in the field of data protection is the grounds for legitimate processing of personal data as laid down in the EU Data Protection Directive. Except for the ground of consent, these are constraints related to specific situations or interests where something else prevails over the privacy interest of the data subject. Clearly, the constraints are dictated by the need to maneuver within the rules of the given context.

Unlike reasonable constraints, unreasonable constraints are either not foreseeable or not communicated beforehand, or not defendable, or both. Obviously, even unexpected constraints may be reasonable in the light of specific circumstances. The necessary condition then is that the constraint has to be defendable. For a constraint to be defendable an objective perspective should be adopted, rather than the subjective perspective of the concerned individual.

Taking the example of Facebook, the requirement of using a real name to create a personal profile page may be reasonable. The aim of the social network site (SNS) is to create and maintain networks and find people with whom there is some relationship. Obviously, a name is very helpful in this context. However, taking the perspective of the SNS as a medium to connect people who share a particular interest, the name may be less relevant, but the details of these interests are the most important. In this respect, requiring the use of a real name may be considered to be an unreasonable constraint, because it disables the option to create a partial identity which is not deemed to be known to an individual's friends or family. For instance, when you are highly interested in Disney movies, but do not want your family to know this, looking for other people with the same interest would only require the characteristic of "liking Disney movies" to be known. The real name of the people with whom the interest is shared is of no concern. This constraint is therefore neither completely reasonable nor completely unreasonable.

Another example is when Facebook would require the disclosure of a telephone number. This is not in any way necessary for the function of Facebook and therefore irrelevant for the context to make it a default. As a result, the required disclosure is not objectively defendable as a constraint. In general, default sharing of unnecessary data as well as default disclosure to other contexts can be said to be unreasonable. It hinders identity construction in context and thus limits the individual in creating an identity free from unreasonable constraints.

Having described how conscious, sometimes forced, disclosure of data can be an unreasonable constraint on a person's construction of his identity, it is only a small step towards arguing that invisible data collection, such as is the case with the Like button, can be an unreasonable constraint. In fact, rather than the individual himself, Facebook is building an identity. If the data concern an individual who has a Facebook account, the data complement the data posted on the profile by the individual himself. The fact that the data are combined, however, remains invisible, in contrast to, for instance, wall posts by other Facebook members. The individual has no insight in the data collection, which makes it impossible to construct a separate or different identity.

1.4.2 Privacy Aspects

Privacy can be distinguished into different dimensions. Common distinctions are between spatial, relational, communicational, and informational privacy.[12] Informational privacy relates to the protection of personal data and has two main components. The first, which is at the core of the right to privacy, is being free from attention of others and not being watched. The second element comes into play once a third party has information and the individual wants to control the use and dissemination of this information (Lloyd 2008, 7). This element concerns the context to which information belongs. A focus on informational privacy can easily be defended. Obviously, many aspects of an individual's life are captured in data, which implies that information from the other dimensions becomes part of informational privacy as well. Information concerning home environment (smart metering), relationships (social networking sites), and body (medical files) is made compatible with the informational dimension. In the context of informational privacy then, data protection can be seen as an intermediate value, since data protection facilitates privacy. When talking about data, the two abovementioned elements of informational privacy have to be discussed in more detail. I will call these elements informational self-determination and contextual integrity, respectively.

1.4.2.1 Informational Self-determination

Informational self-determination is related to the control of a person over his personal data. In this approach, the individual controls his own personal data and information. However, Rouvroy and Poullet state that informational self-determination means "that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said [to be] 'self-determined"' (Rouvroy and Poullet 2009, 51). This approach focuses on the identity aspect and in fact underscores the determination aspect of the 'informational self' rather than the self-determination of information concerning the individual. From that perspective, restricting individual self-determination to control data and deciding what can be done with personal data is far too narrow. Schwarz calls this the 'autonomy trap' and indicates that the "organization of information privacy through individual control of personal data rests on a view of autonomy as a given, pre-existing quality" (Schwartz 1999). However, the problem is that, in the information age, individual self-determination itself is shaped by the processing of personal data. How personal data are used determines the terms under which an individual participates in social and political life. For instance, "the act of clicking through a 'consent' screen on a website may be considered by some observers to be

[12] There have been several efforts define the concept of privacy clearly and concisely. The definition will not be discussed here. For those interested in the discussion and efforts, see, for instance, the valuable work done by Parent (1983), who approaches the concept from different views and disciplines, and the extensive work by Solove (2002, 2006, 2008).

an exercise of self-reliant choice. Yet, this screen can contain boilerplate language that permits all further processing and transmission of one's personal data" (Schwartz 1999). In the end, the autonomy trap refers to a specific form of individual choice being "locked-in." Even though it seems that the individual himself has control over the disclosure of his data simply because he performs a certain action like clicking a button, the control is actually with another party, namely the party who requires the button to be clicked before a certain performance takes place and who decides what conditions are linked to the button being clicked.

The freedom to disclose what you want and to whom you want relates to autonomy and is an active component of privacy. It stresses the action of disclosure initiated by the individual. A passive component lies in the freedom from being monitored or analyzed and can be related to privacy in the sense of being left alone.[13] Next to the active and passive components, there are control mechanisms. These controls can be *ex post*, like access to data and the option to change or to delete them, or *ex ante*, in the mechanism of informed consent. This informed consent can also relate to keeping things to yourself and the mere consideration of whether or not to disclose data.

All components that are of importance for informational self-determination are bound to contexts. The importance of context will be described in the light of contextual integrity.

1.4.2.2 Contextual Integrity

The concept of contextual integrity in informational privacy originates from Nissenbaum (2004), who defines it as "compatibility with presiding norms of information appropriateness and distribution." She specifies the concept by articulating variables which can help determine whether a particular action is a violation of privacy, such as "the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination." Thus, contextual integrity means that information has to be kept within a context and that the way the data are treated has to be in compliance with the general rules and specific agreements concerning that context.

In contextual integrity the emphasis is on the freedom to decide to *whom* an individual discloses information. Evidently, data are usually disclosed within a specific context and to the people that belong in this context. In this respect it is important to understand that disclosing information in a way which makes it accessible to everyone, for instance, by posting something in a public space on the Internet, does not always mean that it is intended to be disclosed to and be made available for use by everyone. A distinction has to be made between the intended audience and the actual audience. The intended audience is the people that belong to the context in

[13] This distinction between active and passive components is inspired by Isaiah Berlin's theory on positive and negative freedoms (Berlin 1958).

which the information is disclosed. The actual audience is the people who in fact have access to the disclosed information, regardless of whether they belong to the specific context in which the information is disclosed.

As can be derived from the variables given by Nissenbaum, purpose binding is an important component. It means that the disclosure of information and its further processing is bound to a specific purpose. This purpose has to be defined before the processing of data takes place. Further dissemination of data, probably to another context, has to be in accordance with the indicated purpose for which the data were disclosed. However, in principle dissemination out of the initial context is not allowed when contextual integrity is the norm. A new context means a new purpose and a new audience.

Someone may browse the web in various contexts: it may be for professional purposes, such as searching for work-related information, or for private purposes, for example, searching for information about a disease a person is suffering from.[14] Obviously, when information about web behavior related to all the different purposes is sent to Facebook, the contexts and purposes change. This implies that the norms that belong to the initial context no longer apply either, resulting in a conflict with contextual integrity.

The fact that the context in which information is processed changes is one thing, but another important issue is at stake here. The collected information is combined with other information by Facebook. As a result, all information is connected and mixed up, so that contexts are collapsed. The distinction between contexts and the consciously or intuitively created boundaries between different contexts are lifted. In the end, the individual can no longer create his own personal identity and cannot even keep partial identities separated. Facebook's Like button interferes with privacy aspects of informational self-determination and contextual integrity and, ultimately, limits individuals in their construction of a personal identity.

1.5 Conclusion and Outlook

This chapter described the purpose and use of the Facebook Like button and how the technical process behind the button works. Four scenarios gave insight into how Facebook is able to monitor individual web behavior, even of nonmembers of the SNS. The scenarios showed that there is no escape from Facebook. The roll-out of the Like button and the potential advantages for web content providers has led to a high implementation rate of the feature. Facebook has a potential connection with everyone, given the fact that actual use of the button is not necessary for it to send information about the web user to Facebook.

Privacy protection is instrumental to the protection of personal identities. Individuals have to be able to construct their own personal identities, free from unreasonable

[14] In this respect, the public outcry on the Like button being available at the website of the National Health Service (NHS) in the UK is a case in point (see, Kirk 2010).

constraints. Forced disclosure of data which, on top of that, may be irrelevant for the purpose for which data sharing takes place may be an unreasonable constraint. This is closely related to informational self-determination and contextual integrity. An individual has to be able to control the disclosure and use of his personal data. If data are disclosed, this has to be done according to the norms and rules that belong to the context in which disclosure takes place and the data may not be disclosed outside the given context. If these conditions are not fulfilled, identity construction is no longer free from unreasonable constraints.

Applying the above to the Facebook Like button shows that there are constraints on the construction of identity. Facebook collects data concerning individual web users and can use these data to construct profiles. In particular, if a web user has a Facebook account, the data can be linked to this account based on the unique identifier that is sent along with the cookie in the HTTP request for the Like button. This implies that Facebook collects far more data than the data disclosed by its members. Moreover, Facebook collects huge amounts of data concerning individuals who do not have a Facebook account at all. As a result, individuals cannot create their own personal identities and cannot keep partial identities within a context.

Even though data collection concerning browsing behavior of web users via third-party cookies is nothing new, the Facebook Like button brings up some slightly different issues. These issues are strongly related to Facebook as a platform and to the presentation of the Like button. As indicated, the presentation of the button as a tool for Facebook members to share the web pages and items they like suggests that actual use of the button is necessary to set up communication with Facebook. Besides, nonmembers will think that they are not involved with Facebook in any case. This is obviously not true.

The other issue, related to the platform Facebook, is also very important. Facebook is a SNS which allows members to share their personal data with other members. These data can contain biographical data, but also pictures, videos, interests, and so on. Even though there is an initial choice on whether to participate in the network or not, there is also some social pressure to create an account.[15] Once you have an account, Facebook tries to let you share more and more data. The introduction of social media plugins, of which the Like button is one, formed a new development in this context. The plugins try to encourage individuals to connect all their web activity, subscriptions, and accounts to their Facebook account. Thus, on the one hand, Facebook possesses extensive information sets of all its members and can supplement these with additional information collected via third-party cookies, even if members do not attach things they like to their account pages. On the other hand, Facebook is trying to become the real digital identity of individuals for all contexts and interactions.

[15] Compare the famous quote by Skyler, 18: "If you're not on MySpace, you don't exist!" (Quote posted by her mother Kathy Sierra at http://headrush.typepad.com/creating passionate users/2006/03/ultrafast relea.html , no longer available (cf. boyd 2008).

Because Facebook has thoroughly embedded itself into the personal lives and identities of individuals, its impact reaches much further than the impact of 'traditional' third-party cookies, which are often used for targeted advertisements only. If an individual is not connected to Facebook, Facebook will make the connection instead.

The Facebook Like button is a case making very clear how changes in society and technology change the character of privacy concerns. The Internet has become central to daily life and social media are focused on sharing of personal information. However, the providers of social media are commercial companies which generate profits from the use of personal data. At the same time, these companies succeed in broadening their impact by connecting to other web services and increasing their coverage over the web. It is simply not possible for a web user to escape from being monitored once his browser connects to the Internet, whether the user has a formally established relationship with some services or not.

A related development is the technological trend towards the 'Internet of things' in which the connection to the web is ubiquitous and data are collected everywhere. This development implies that the notion of consent as we know it now becomes unworkable as a central concept in personal data processing. This trend calls for policy changes concerning privacy and data processing, while the need for a workable web environment remains essential. To find proper ways of regulating privacy in an era of ubiquitous information collection and in a society where connectivity is the standard is very challenging. Nevertheless, in light of personal identities, individual autonomy, and privacy, it is of the utmost importance to consider these issues at short notice. For the moment, commercial companies are leading the way with their own interest as a top priority.

References

Agre, Philip E., and Marc Rotenberg. 1997. *Technology and privacy: The new landscape*. Cambridge: MIT Press.

Berlin, Isaiah. 1958. *Two concepts of liberty*. Oxford: Clarendon Press.

boyd, danah. 2008. Why youth heart social network sites: The role of networked publics in teenage social life. In *Youth, identity, and digital media*, ed. David Buckingham, 119–142. Cambridge: MIT Press.

boyd, danah, and Eszter Hargittai. 2010. Facebook privacy settings: Who cares? *First Monday* 15: 8.

Burbary, Ken. 2009. Five reasons companies should be integrating social media with Facebook connect. http://www.kenburbary.com/2009/08/five-reasons-companies-should-be-integrating-social-media-with-facebook-connect/. Accessed 20 Aug 2009.

Dwyer, Catherine A. 2009. Behavioral targeting: A case study of consumer tracking on Levis.Com. Paper presented at the 15th American Conference on Information Systems, San Francisco, California.

Goffman, Erving. 1959. *The presentation of self in everyday life*. Garden City: Doubleday & Company.

Hekman, Susan J. 2004. *Private selves, public identities: Reconsidering identity politics*. University Park: The Pennsylvania State Univ. Press.

Kirk, J. 2010. NHS link to Facebook raises privacy concerns. http://www.pcworld.com/businesscenter/article/211711/nhs_link_to_facebook_raises_privacy_concerns.html. Accessed 7 Dec 2011.

Lloyd, Ian J. 2008. *Information technology law*. Oxford: Oxford Univ. Press.

Martin, David, Hailin Wu, and Adil Alsaid. 2003. Hidden surveillance by web sites: Web bugs in contemporary use. *Communications of the ACM* 46 (12): 258–264.

Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79: 119–158.

Parent, William A. 1983. Privacy, morality, and the law. *Philosophy and Public Affairs* 12 (4): 269–288.

Roosendaal, Arnold. 2010. Facebook tracks and traces everyone: Like this! Tilburg Law School Research Paper No. 03/2011. http://ssrn.com/abstract=1717563. Accessed 30 Nov 2010.

Rouvroy, Antoinette, and Yves Poullet. 2009. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In *Reinventing Data Protection*, ed. Serge Gutwirth et al. 45–76. Berlin: Springer.

Schwartz, Paul M. 1999. Privacy and democracy in cyberspace. *Vanderbilt Law Review* 52: 1609–1701.

Solove, Daniel J. 2002. Conceptualizing privacy. *California Law Review* 90 (4): 1087–1156.

Solove, Daniel J. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (3): 477–560.

Solove, Daniel J. 2008. *Understanding privacy*. Cambridge/London: Harvard Univ. Press.