A critical overview of the privacy debates regarding Facebook and an assessment of the "Anti-Facebook" social network, Diaspora*

Jennifer Cohen

690244

A Research report submitted in partial fulfilment of the requirements for the degree of Master of Arts in the field of Digital Arts, University of the Witwatersrand, Johannesburg

February 2013

Declaration

I declare that this report is my own unaided work. It is submitted for the degree of Master of Arts in the field of Digital Arts by coursework and research in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination at any other university.

Jennifer Cohen

_____

____day of ____ 2013

Acknowledgements

I would like to thank Christo Doherty, for his very helpful supervision and support.

Abstract

As the number of Facebook users across the globe reaches over a billion, more people continue to make even greater use of this social network to support their daily activities and relationships. As a result a large amount of personal information is being generated, all of which provides extensive insight about Facebook users. This information is frequently exposed to other individuals in unexpected ways and often with severe consequences such as shame, embarrassment, job loss, and sometimes even arrest. Additionally, this large collection of users' personal data is owned and stored by Facebook, which now exploits it for money through advertising, in continually changing and often bewildering ways.

This research paper aims to address the complex and often controversial debate around privacy invasions, specifically with regard to Facebook and the alternative social network site Diaspora*. It develops a rigorous conception of privacy relevant to online social networks, primarily using Helen Nissenbaum's framework of contextual integrity. This conception is made up of two dimensions: social privacy and institutional privacy. Social privacy generally covers *peer-to-peer* violations, while institutional privacy covers the relationship between Facebook and its users, specifically its practices regarding user data. These conceptions of privacy are used in conjunction with an analysis of Facebook's history and current privacy policy and features to determine the nature of privacy violations on Facebook, and the extent to which Facebook is accountable. This analysis occurs in the time frame since Facebook's inception in 2004 until June 2012, a month after its Initial Public Offering. As a comparative case study, the conception of social network privacy is used to assess the "Anti-Facebook" alternative social network Diaspora* to determine whether it successfully offers a better solution to social network privacy than Facebook does.

This paper concludes that violations of social privacy occur on Facebook primarily due to the collapsing and convergence of many different contexts. Institutional privacy is

violated by Facebook's continually changing, dense and bewildering data practices, which is exacerbated by the centralised nature of its user data store. Facebook is accountable for these violations principally because its default settings continually push towards increased information disclosure. This paper also concludes that this push is intentional, in light of Zuckerberg's fanaticism about making the world more transparent, and because of the commercial value of Facebook's huge personal data store.

This paper also concludes that Diaspora* offers some improved solutions to maintain online privacy, primarily because of the control of data it provides to its users and because of its potential to promote a heterogeneous landscape of social networks that do not need to commercially exploit user data. However, Diaspora* introduces some further risks to institutional privacy, and it is asserted in this paper that some social privacy issues are intrinsic to online social networks, and therefore difficult to avoid.

Table of Contents

List of Figures

Chapter One

1.1 Introduction

Today, almost every aspect of most of our lives is maintained online. All these activities breed information. On social networks, and Facebook in particular, a wide range of information is generated through the creation of accounts corresponding to one's real-world identity and through interactions with one's real-world friends, acquaintances, family, and work colleagues. Often this information is exposed to a range of unexpected audiences resulting in unintended consequences. It is additionally stored on Facebook servers for an indefinite amount of time and for often uncertain purposes. The state of personal information profusion and the opportunities to exploit it by individuals and Facebook itself have occurred swiftly with the fast, and at times volatile, development of Facebook over the last nine years. It has left us in a state of bewilderment and uncertainty, especially when it comes to the issues of privacy violations. This research paper aims to address the complex and controversial debate around privacy invasions, specifically with regard to Facebook. It will do so by developing a rigorous conception of privacy. It will apply this conception to Facebook by analysing its development as well as its current state of features and privacy policy to determine exactly what privacy violations occur; how and why they occur; and the extent to which Facebook is accountable for such violations. It will then also employ the conception of privacy to critically assess the effectiveness of a recent social network called Diaspora*, which was started as a reaction to the privacy violations occurring on Facebook, and is claimed to be a superior, privacy-preserving social network.

As will soon be elucidated, since its inception, Facebook has been in a continual state of flux, with changes to its features and privacy policy occurring regularly. For this reason, the time frame of the analysis was limited to Facebook's beginning in 2004 to June 2012. The closing date was chosen because it was a month after Facebook shares became available to

the public, which marked a significant milestone in its continual development, and additionally was the date the Facebook privacy policy had last been modified[1].

1.2. Towards a Conception of Social Network Privacy

In order to critically assess accusations of privacy violations directed at Facebook it is necessary to engage with a conception of privacy. The conception developed in this paper will be primarily based on the framework of Helen Nissenbaum, a professor of media culture and communication, as established in her book *Privacy in Context*[2], as well as supporting theories found in most of the literature reviewed. Arriving at a concise, universally applicable definition is, as Nissenbaum warns, a complex endeavour (2). Robert Post, a Yale law professor states "privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all" (2087). However, this does not mean it is a task to be abandoned completely, as the conception established in this chapter will be framed within (and thus limited to) the context of online social networks, and will be separated into two somewhat distinct dimensions – the context of social interactions between social network users, and the context of interactions between social network owners and their users. It has been stated that "agreement on a broad analytical definition of privacy in the abstract is difficult if not impossible. But discussions of the privacy implications of specific events and practices are easier to understand and discuss" (Waldo, Lin, and Millett 85). Furthermore, what will be produced in this chapter is not so much a precise definition as it is a distinct understanding of the requirements necessary to preserve privacy in the contexts just described. These conceptions will be applied to the next two chapters where the privacy policies and practices of two digital social networks, Facebook and Diaspora*, will be assessed and compared.

---

[1] As will be revealed in Chapter Four, Facebook subsequently revised their privacy policy in November 2012

[2] *Privacy in Context* was not only cited in Solove's book, but has been cited by many (over 400 on *Google Scholar)* scholarly articles and journals on the subject of information technology and privacy.

Before one can formulate a notion of privacy, it is necessary to examine how it has been commonly conceived, and how this conception has limited and confused evaluations of the legitimacy of various privacy violations. Therefore, this chapter first sets out to explain what privacy does **not** entail – it addresses previous or traditional notions of privacy that are insufficient in dealing with the complexities and nuances of privacy issues both in general and within the context of today's Information Age. The next section dispels commonly argued reasons for not needing privacy, which have often been raised with regard to Facebook practices, and which have thwarted a meaningful analysis of potential violations. Once this foundation has been established, the impacts of privacy loss are described. These impacts are explained in terms of potential consequences as established by many scholars in relation to a general notion of privacy (in contexts greater than online social networks). Additionally, examples of actual consequences experienced by social network users are provided. Finally, the conceptions of social network privacy are elucidated.

As alluded to earlier, it is now necessary to point out the two distinct dimensions of Facebook issues that will be dealt with in this paper. The first dimension is related to the harvesting and commercial exploitation of user data by Facebook itself (i.e. its data practices) and the second is associated with violations that result from users disclosing their own information on social networks, as well as others disclosing information about a particular user. Kate Raynes-Goldie terms these two dimensions of privacy "institutional privacy" and "social privacy" respectively (Raynes-Goldie). Throughout the rest of this paper these two terms will be used in this way.

1.3. What Privacy is Not

1.3.1. Public vs. Private

A common conception of privacy (both in legal and philosophical terms) assumes that everything is divided into two separate realms – a public one and a private one. The private

realm is usually confined to “the familial, the personal, or intimate relations”, while the public realm “signals civic action...beyond the home and the personal” (Nissenbaum 90). In this binary view of privacy any information that is placed in public view has no claim to privacy protection (Solove 163). This conception is dealt with in most of the literature. Helen Nissenbaum, in *Privacy in Context* uses the term “public/private dichotomy” (89–102), while Daniel J. Solove refers to it as the “secrecy paradigm” (*The Digital Person* 43). Despite the common conception, we often in fact expect and require privacy when in public. This expectation is often illustrated by the example of our expectations when having a conversation in a restaurant. In this context, even though we are in a public location and our conversation may be audible to those around us, we still expect others not to listen in (Solove, *The Future* 166). As Danah Boyd and Alice Marwick stress - “Engaging in public life does not entail throwing privacy out the window” (25). Additionally, Solove states that most of our personal information exists in records that are outside of our “secret” realm and it is almost impossible to “live life as an Information Age ghost, leaving no trail or residue” (*The Digital Person* 8). To participate in society today, both in the online and the offline world (e.g. banking both online and offline, shopping with credit cards, voting), it is inevitable that we generate personal information, and that this information is stored in external databases beyond our own “private” physical or virtual repositories.

The legitimacy of requiring privacy specifically within private realms was acknowledged in 1890 in a highly influential article that appeared in the *Harvard Law Review* by Samuel Warren and Louis Brandeis. The article entitled “The Right to Privacy” has been credited as fundamental in the establishment of a “comprehensive legal right to privacy” (Nissenbaum 1). It was written in response to the newly invented instantaneous camera and the increasingly invasive nature of the press. In this paper Warren and Brandeis assert that “instantaneous photographs and newspaper enterprise have invaded the sacred precincts of

private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" (195 -196). Because one's images could be captured without one's consent and from far away, Brandeis and Warren acknowledged that one should be able to sue for non-consensual photography (Solove, *The Future* 190). Although Warren and Brandeis focused on the "precincts of private and domestic life", they insightfully acknowledged the danger of the abilities of technologies (in their case photography and the press) to disrupt and blur the distinctions of public and private realms. Whether a photograph is taken in private or in public, "there is a difference between what is captured in the fading memories of only a few people and what is broadcast to a worldwide audience" (Solove, *The Future* 163). Solove is asserting here that the persistence and publication capacities technologies allow can drastically change the nature of what occurs in public, and so, more than ever, people should be provided with protection outside of the traditionally private realm. Furthermore, as Nissenbaum stresses, what we could once expect in the public realm has been drastically changed by these (photographic and press) technologies: "In the period before such technologies were common, people could count on going unnoticed and unknown in public arenas; they could count on disinterest in the myriad scattered details about them" (117).

With the further advancement of modern technology (e.g. mobile phone cameras, closed circuit television cameras) the public privacy requirement is even more significant. As Solove states: "Today data is gathered about us at every turn. Surveillance cameras are sprouting up everywhere. There are twenty-four-hour surveillance cameras in public linked to websites for anybody to view" (Solove, *The Future* 163). Additionally, since the emergence of the World Wide Web and most recently social networks, more of our daily activities are conducted online. The nature of the online realm (allowing even greater persistence and publication than photography and the press) introduces even more challenges to our

understanding of and expectations for the notion of "public" and the consequences of activities within it. This will be discussed in depth in the next chapter.

1.3.2. Big Brother and Invasion Conceptions

Another common conception of privacy issues that has been raised more recently in relation to online social networks (and online technology in general) is what Solove terms the "Big Brother Metaphor". George Orwell's famous novel *1984* is often referred to when talking about privacy invasions and surveillance issues. However, Solove feels that this metaphor focuses too much on the concept of surveillance by a centralized malevolent entity. This concept does not sufficiently tackle the kind of surveillance that occurs between Facebook and its users when collecting their generally innocuous information (*The Digital Person* 35). It additionally does not deal with the kind of peer-to-peer surveillance occurring on Facebook. As the next section will reveal, surveillance may indeed be an issue in both social and institutional contexts but focusing on this issue alone limits the assessment of other significant violations that may occur.

Solove also debunks what he terms the "Invasion Conception". This notion assumes that a violation occurs only when a person is directly injured by the perpetrator's invasion (*The Digital Person* 8). The problem with this conception is that digital dossiers[3] and many information revelations in the social context do not commonly invade privacy in a direct or explicit manner. Often our information is aggregated at different stages and connected across databases for different, mostly harmless purposes, which would not be a valid violation in terms of this invasion conception (Solove, *The Digital Person* 8). Solove also goes on to discuss what he terms the "aggregation effect" which he explains as "information breeds information" (*The Digital Person* 44). Individual pieces of information may seem harmless

[3] A dossier is a "collection of detailed data about an individual" (Solove, *The Digital Person* 1). Solove explains that today there are "hundreds of companies that are constructing gigantic (digital) databases of psychological profiles, amassing data about an individual's race, gender, income, hobbies, and purchases" (*The Digital Person* 2)

but, when combined and interpolated, can amount to meaningful insights about a person. Furthermore, in *Privacy Lost*, David Holtzman stresses that "web searching and blogging are impulsive, and although each instance may not be revealing, collectively searches and blog entries paint a detailed picture of a person's opinions and interests" (12). The analysis of Facebook's privacy policy in the next chapter will reveal the extent of the information that Facebook acquires from most users, and that may as a result be available to other individuals. The section that follows shortly in this chapter will reveal the problems that may arise as a result of this "aggregation effect".

1.4. Dispelling Reasons for Not Needing Privacy

1.4.1 Nothing to Hide

Often as a result of the simplistic or inaccurate notions of privacy (discussed in the previous section), it is argued that we in fact do not need privacy at all. One of these arguments is what Solove terms "Nothing to Hide"("'I've Got Nothing to Hide'" 748), which assumes that people only require privacy if they are doing something illicit or illegal (Boyd and Marwick 17). Nissenbaum echoes this observation when she explains that often it is argued that privacy "is more likely a cover for the freedom to do wrong" (Nissenbaum 76). In fact, Eric Schmidt, CEO of Google, made this exact argument in response to concerns over Google's data tracking practises, stating that, "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Mick). However, Solove states that the basis of this argument incorrectly assumes that privacy is solely about concealing wrongs ("'I've Got Nothing to Hide'" 764). As this chapter will show, specifically in the next section ("Consequences of Diminished Privacy"), the preservation of privacy serves many other significant values above the ability to perform illicit activities without getting caught.

1.4.2. Lack of Privacy Concerns

Another opinion voiced frequently is that people no longer care about privacy and therefore do not need it. Supposedly Facebook users have succumbed to exhibitionist behaviour and have discarded all concerns over their privacy in the process (Peterson 3). In 2010 Mark Zuckerberg, founder of Facebook, expressed his belief that the desire for privacy as a social norm is disappearing. Zuckerberg stated that "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time" (qtd. in Johnson).

The economics columnist for the *Washington Post*, Robert J. Samuelson believes that the Internet and social networks specifically have introduced what he calls "mass exhibitionism" and that their popularity "contradicts the belief that people fear the Internet will violate their right to privacy". Samuelson asserts that people's obsession with fame and "spilling their guts" as shown in crass reality television shows like "Jerry Springer", has been facilitated en masse by social networks and that "millions of Americans are gleefully discarding -- or at least cheerfully compromising -- their right to privacy. They're posting personal and intimate stuff in places where thousands or millions can see it" (Samuelson).

Anita Allen, an American privacy law expert, also asserts in her paper "Coercing Privacy" that from as early as 1999 people no longer care for privacy. She states that "one detects signs of an erosion of the taste for and expectation of privacy" (728). Allen suggests that such "erosion of privacy" could be due to technologies that make it easier for individuals to disclose and publicise information and for institutions to track and commercialise such disclosures (730). Like Samuelson, she also attributes exhibitionist tendencies to explain the privacy erosion, again asserting that the Web has facilitated and encouraged such tendencies

(731). Allen uses Jennicam[4], a website that existed from 1996 to 2003 and created by Jennifer Ringley to publicise every part of her life via a webcam, as an extreme example of the increase in exhibitionism. She additionally asserts that the popularity of the site - the large numbers of people wanting to "consume other people's privacy" - is an indication of the lack of concern for privacy (730).

In addition, many scholars have also argued that although many may claim to be concerned about privacy, their behaviour reflects something different. This apparent contradiction is known as the "privacy paradox" (Raynes-Goldie, "Digitally Mediated Surveillance" 4). The term was adopted to explain the apparent contradiction between surveys in which people indicated a strong concern for privacy, and studies that observed the behaviour of people carelessly disregarding privacy. In 2006, a study of 294 Facebook users and non-users at an American university indicated this dichotomy between reported attitudes and actual behaviour (Acquisti and Gross 11). The study found that on average users ranked the subject of "Privacy Policy" as very important in the "public debate" (more important than terrorism) (8). 81% of participants showed a significant degree of concern about the possibility of a stranger knowing where they lived, their location and their class schedule and 46% showed the highest degree of concern. The study then revealed that 89.74% of undergraduate users who conveyed the highest degrees of concern about the privacy risk cases presented were still joining Facebook (8). The study also showed, for example that more than 48% of users who showed the highest level of concern over strangers finding out their sexual orientation, had in fact made that piece of information open to the public on their Facebook profiles (11). It was also shown, however, that 30% of participants were unaware that Facebook in fact provided tools to limit the visibility and searchability of profiles (16). 77% of participants had not read Facebook's privacy policy and between 56% and 70% were

[4] Archive of Jennicam website: http://web.archive.org/web/*/http://www.jennicam.org

completely ignorant of various aspects of Facebook's data collection practices[5] (18). Lastly, 33% of the students believed that it was "either impossible or quite difficult" for people not associated with the university to access the university's Facebook network[6] (11). It was, however, in fact the case that the default settings on Facebook at the time where such that anyone on the Facebook network could search user profiles and anyone in the same geographical location or university could view a user's profile (2).

In dispute of the first claim (of Zuckerberg, Samuelson and Allen) raised here that privacy norms on social networks have changed drastically, this paper asserts that it is to many degrees a misjudgement. As Nissenbaum, Boyd, and Peterson all stress, the majority of a user's friends on a particular social network are his/her real-world friends as well. A study from 2008 revealed that only 0.4% of friendships on Facebook were merely online relationships (Mayer and Puller 332). Therefore most users' expectations for privacy on social networks are infused with their social interactions and privacy expectations of the offline world, and "the overwhelming majority of Facebook relationships are digital representations of their corporeal counterparts, and as such are animated by the social roles, expectations, and norms from the 'real world'" (Peterson 9). Additionally, as the 2006 Gross and Acquisti study showed, many Facebook users stated concerns for various privacy issues on Facebook, whether or not this was reflected in their behaviours is somewhat irrelevant with regard to the "exhibitionist" claim – exhibitionists generally do not have, or pretend to have, concerns for privacy. There may be no denying a rise in interest in **some** people disclosing their intimate details to millions on TV and online, and many consuming such revelations, but to claim that every Facebook user is motivated by the same desires and therefore does not want any form of privacy is far too simplistic a view.

[5] 67 % "believe that FB does not collect information about them from other sources regardless of their use of the site"; 70 % "that Facebook does not combine information about them collected from other sources"; 56% "that FB does not share personal information with third parties"

[6] At the time of this study Facebook was only open to university and high school students in America.

In addition, in dispute of the privacy paradox claim, concluding that the contradictory behaviour shown in the Gross and Acquisti study implies that users do not care about privacy at all, fails to recognise other significant factors that may have affected such behaviour. The high rates of ignorance regarding Facebook privacy controls as well as Facebook data practices, and the delusion of the isolated visibility of each network may have had a significant impact on the carelessness of the disclosures observed. A study at Carnegie Mellon University in 2007 aimed to determine if people (more general consumers on websites) would "incorporate privacy considerations into their online purchasing decisions" if privacy policies were made more accessible and clear. The experiment conducted consisted of providing subjects with a shopping search engine that annotated search results with a privacy rating and a concise summary of the particular retailer's privacy policy (Tsai et al. i). The results of the experiment indicated that with the annotated concise privacy information, subjects opted to purchase from retailers that had higher privacy protection and additionally, were willing to pay a premium for such purchases (21).

Furthermore, as Raynes-Goldie suggests, since the "privacy paradox" term was conceived in 2006, the social network "landscape" may have changed quite drastically ("Digitally Mediated Surveillance" 2). With regard to Facebook specifically, the extent of change will be revealed in the next chapter as the development of Facebook is traced. This chapter will specifically reveal the increased indignation of users and privacy advocates as each new change was implemented by Facebook. It is possible that this state of change may be reflected in privacy behaviours too. A study published in February 2012 comparing data between 2009 and 2011, shows that although social network users initially may have been careless with their privacy, since 2009 an increase from 56% to 63% of users have removed contacts; 36% to 44% have removed *comments*[7] from their profile; and 30% to 37% have

[7] See glossary

deleted their names from photographs in which they had been *tagged*[8] (Madden 2). The study also indicates that 58% of users have their profiles restricted to completely private and 19% to partially private (visible to *friends-of-friends*[9]), although it does not indicate the percentages in 2009. The primary implication of this study is that users are actively taking steps to manage and control their privacy on social networks, indicating that not only do users in fact care about privacy; they also behave in a manner that is consistent with such concerns.

Nissenbaum additionally asserts that Facebook users do in fact reflect their desires for privacy in their behaviour but not necessarily in relation to the narrow conception of privacy that implies users only require secrecy (151). The privacy paradox has frequently been levelled against the online behaviour of teenagers but as Boyd and Marwick stress in a very recent study of teenage attitudes and behaviour: "All teens have a sense of privacy, although their definitions of privacy vary widely. Their practices in networked publics are shaped by their interpretation of the social situation, their attitudes towards privacy and publicity, and their ability to navigate the technological and social environment" (1). Reinforcing the earlier argument that privacy goes beyond the need for privacy only in non-public realms, Boyd and Marwick's study shows that in fact "this is not a contradictory stance; it parallels how people have always engaged in public spaces" (25).

1.4.3. Privacy vs. Free Speech

Many advocates who argue against regulations to protect privacy have claimed that privacy regulation conflicts with other more important values and thus should be discarded completely. Of the values that conflict, one of the most significant and common that is asserted is freedom of speech. It is important at this point to keep in mind the social network privacy contexts established earlier, and the fact that various dimensions of privacy issues are often quite distinct. It is most often the case that social privacy, and specifically others

[8] See glossary
[9] See glossary

disclosing information about a particular user on a social network, conflicts with free speech. One such advocate that is wary of strict regulations of this kind of privacy issue is American First Amendment scholar, Eugene Volokh, who states that "the difficulty is that the right to information privacy - my right to control your communication of personally identifiable information about me - is a right to have the government stop you from speaking about me" (2). According to Volokh, the case of the government restricting such disclosures would be a violation of the First Amendment. However, as Solove asserts there have been many cases in America where the Supreme Court acknowledged that freedom of expression needs to be balanced by the law of defamation (*The Future* 126). This is the case in South Africa as well, where freedom of expression is guaranteed in the Constitution of the Republic of South Africa, but where it is not an absolute trumping of all other laws, including defamation law (Victoria 4). The problem arises in the case of social network users disclosing truthful information about a user, as defamation law is limited to revealing **false** facts about another person (Solove, *The Future* 126). However, Solove asserts that because the Supreme Court acknowledges that not all forms of speech need protection, "speech of private concern" should not be as strictly protected as speech that is legitimately of concern to the public (128 -129). For the majority of disclosures on social networks, the public would not be served in any way by knowing the information revealed, and as such, the law should protect these disclosures.

Furthermore, both Solove and Nissenbaum stress the importance of assessing the key purposes of free speech in the first place. This reveals how privacy serves the same ends as those of free speech (Solove, *The Future* 129). For example a fundamental reason for needing free speech is to ensure "individual autonomy" (130), but as the next section will reveal, privacy also promotes autonomy in that "the disclosure of personal information can severely inhibit a person's autonomy and self-development" and "risk of disclosure can inhibit people

from engaging in taboo activities" (130). Free speech also serves to promote democracy. However, political debates are only enriched by speech relevant to public interests, and not by speech of private concern – "reporting people's secrets rarely contributes much to politics", re-enforcing the need to distinguish between different types, and thus values, of speech. Furthermore, Nissenbaum stresses the need to "take into consideration not only the potential chilling of speech due to privacy, but the chilling of speech due to reductions in privacy" (111). This is especially relevant to the case of social privacy and self-revelation, where one's disclosure may be protected by freedom of expression laws **and** by the safety of its privacy.

1.5. Consequences of Diminished Privacy

1.5.1. Surveillance

In order to grasp a more comprehensive conception of privacy it is necessary to understand the purposes and values it serves, as well as the impact of diminished privacy. One of the most common concerns is that without privacy the potential for surveillance increases. Surveillance on social networks may occur in the social context, where a user's friends can observe his/her profile and his/her activities, and where a disclosure intended for the social context may be later observed by external parties who may in fact be institutions (for example law enforcement, potential employers, government) or other individuals. Surveillance may also occur in the institutional context, where the social network owner, in possession of all the data accumulated from its users' activities, can scrutinise such data.

Nissenbaum asserts that freedom from scrutiny, enables "artistic expression and intellectual development" to prosper and the formation of autonomous moral and political beliefs. Freedom from scrutiny implies that one is not burdened by the fear of "disapprobation, censure, and ridicule", or the pressure to subscribe to conventions (75).

In a similar vein, Jeffrey Reiman introduces the idea of an "informational fishbowl" where the people contained within are observable from one location (28). Reiman identifies four kinds of risks resulting from this situation:

1. Extrinsic loss of freedom - People may change or stop any unconventional activities out of concern for possible derision or limitation of future prospects like employment.
2. Intrinsic loss of freedom - People may start to perceive themselves and their behaviour through the eyes of those watching due to the above-described self-censorship.
3. Symbolic Risk -This involves the limitation of autonomous expression.
4. Psycho - political metamorphosis - In addition to the behaviour limiting effects, a restriction of how individuals **think** may be caused, resulting in stunted ambition and development (35–42).

The surveillance described here may be relevant to losses of both social and institutional privacy. However, the aspect of being observable from one location is specifically relevant to the centralised nature of Facebook, and thus to institutional privacy. In *The Facebook Effect*, David Kirkpatrick raises this issue in relation to social privacy more appropriately by stating that "Others ask how it might affect an individual's ability to grow and change if their actions and even their thoughts are constantly scrutinized by their friends" (16).

1.5.2. Reputation

In addition to the thwarting of autonomy that may arise from the awareness of being under surveillance, the results of surveillance itself may have severe consequences for one's reputation. The amount of information generated in social network activity per user is vast (the extent of which will be shown in the next chapter) and as such can provide quite an extensive view of a person. Even if a particular user chooses not to disclose a substantial

amount of information, as a result of the "aggregation effect" mentioned earlier, information can be inferred about a user, through the summation of small amounts of data and with the implicit information of a user's friend network. Grimmelmann reports on a study where researchers could deduce the age and nationality of a user of a social network based on the details of the user's friends (1173).

Solove warns that reputation damage becomes problematic when information that was intended for one context is placed in another context, as an individual may be misjudged due to having "only partial knowledge of someone else's situation" (*The Future* 66). Information about a person gleaned through aggregation or inference or taken out of context may portray an individual in an inaccurate or "distorted" manner (Solove, *The Digital Person* 45). Nissenbaum points out that if this incorrect or imprecise information is used further down the line in situations such as employment or credit ratings, the effects can be dire for the individual concerned. Specific examples of such consequences will be revealed shortly.

Furthermore, Solove points out the importance of being allowed a second chance. With the permanence of online information, all our past indiscretions and mistakes do not allow a recovery from possible youthful immaturity (*The Future* 72). "Still another effect of new information technologies is the erosion of privacy protection once provided through obscurity or the passage of time; e.g., youthful indiscretions can now become impossible to outlive as an adult" (Waldo, Lin, and Millett 31).

1.5.3. Identity Theft

Reputational and potentially severe financial harm may also occur through fraudulent indiscretions, in the form of identity theft - "the fraudulent construction of identities" (Nissenbaum 78). Identity theft may arise in both the social context where personal information can be gleaned and exploited by individuals obtaining publicly available information through the social network interface, but it is possible for it to occur as a result of

social network data safety negligence, where databases containing private[10] data may be hacked. In this case, as will be discussed further in the next section, when establishing requirements for institutional privacy, the social network owner should be held accountable for data safety. Thus identity theft is a relevant consequence of diminished institutional privacy. In the case of Facebook, the risk of information exposure may be especially high as millions[11] of users' data are stored on the centralised Facebook servers. In South Africa in 2011 it was reported that there were 20 cases of financially related identity theft per day (Zungo). With access to large amounts of personal data on Facebook, identity theft may in fact become particularly problematic in South Africa.

1.5.4. Case Studies

These consequences are not just speculative hypotheses; they are in fact evident in situations that have occurred frequently throughout Facebook's history and across the globe. In 2006, in Illinois, a police officer tried to catch two students who he had found urinating in public. One of the students (Marc Chiles) managed to escape, while the other (Adam Gartner) was apprehended. Gartner claimed that he did not know Chiles but the police officer proceeded to search the university Facebook profiles until he found Gartner. By looking at Gartner's list of Facebook friends, the police officer was able to infer whom Chiles was and that he was in fact Gartner's friend. Gartner was subsequently charged with obstruction of justice (Peterson 10). This case shows how easy it is to extrapolate information about an individual through a social network, without that person disclosing huge amounts of particularly harmful or illicit information, and how information used for a completely different purpose can have severe consequences on that person's fate further down the line.

However, there are indeed many cases of Facebook users posting potentially harmful information, which they had intended to remain within the context of their Facebook friends,

[10] Data restricted under settings that limit exposure to only the user or a limited set of people.
[11] As of October 2012 Facebook had 1.01 billion users ("Number of Active Users at Facebook over the Years")

and which had been subsequently used against them. In February 2012, in Johannesburg, a senior inspector at the *South African Civil Aviation Authority* was suspended for a negative Facebook post about his seniors, allegedly after one of the inspector's colleagues informed his seniors of the comment (Gibson). In 2011, in America, it was reported that "confusion about what American workers can or can't post has led to a surge of more than 100 complaints at the National Labour Relations Board - most within the past year - and created uncertainty for businesses about how far their social media policies can go" ("Employers Negotiate"). In Chicago, a car salesman was fired after posting complaints about the conditions of his work, however the National Labour Relations Board found that the salesman had a legal claim for his post to remain protected as he was "expressing concerns about the terms and conditions of his job, frustrations he had earlier shared in person with other employees" ("Employers Negotiate").

A more severe case of the unintended consequences of self-disclosure on Facebook is that of Shaheen Dhada, a 21 year old Indian woman, who posted a comment questioning Mumbai's shutdown during a politician, Bal Thackeray's funeral (Mccarthy). Dhada intended the post for her Facebook friends but it is presumed that someone saw the post and then informed *Shiv Sena*, Thackeray's hard-line political party (Narayan). A local Shiv Sena leader, Bhushan Sankhe, immediately lodged a complaint with the police, and just 25 minutes after the post, Sankhe phoned Dhada asking her if she believed it was right to have posted such a comment (Narayan), (Bhatt). Dhada immediately deleted her comment and apologised, but by then a mob had already started vandalising her uncle's clinic (Narayan). Within minutes the police arrived at Dhada's door to place her under arrest, and had in fact also arrested a friend of Dhada, who had *liked*[12] Dhada's post on Facebook. The police arrested the two for "insulting religious sentiments, and booked them under a little-known

[12] See glossary

provision of India's Information Technology Act, known as 66A" (Narayan). The act prohibits online content that is "grossly offensive or has menacing character" or incites "annoyance, inconvenience, hatred, danger, obstruction, insult" (Narayan). Dhada and her friend were released on bail and due to subsequent public outcry, the charges were eventually dropped, but Dhada had become so fearful of any further harm that she deleted her Facebook account.

This story has many significant dimensions that reinforce issues raised in this chapter. Most relevant to this section is the impact on Dhada's reputation (almost obtaining a criminal record) and her physical safety (the violence of the mob). This incident also shows the severe harm of surveillance to individual autonomy, as after the incident Dhada deleted her Facebook account, in fear of expressing her opinions again. She did subsequently open a Facebook account again but reported that she is now very careful about what she posts (Nair); an evident response of self-censorship. Furthermore, this story is a significant example of how free speech and privacy support the same values. If Dhada's post had remained contained among her Facebook friends or if her freedom to express her own opinion had been respected, Dhada would not have suffered such harsh consequences. It is also important to note that the context in which this incident took place, in what is clearly an extreme political landscape, is largely the reason for such a severe outcome. As the next chapter will reveal, a fundamental issue with Facebook is its rapid progression from a contained college network in an established democratic country, to a world-wide phenomenon encompassing a boundless number of contexts.

As indicated, damage to a user's reputation often occurs as a result of other people on social networks disclosing information about that user. The *Daily Mail* in 2007 pulled photographs off a Facebook *group*[13] called "30 Reasons Girls Should Call It a Night", and

[13] See glossary

published them in the newspaper. The photographs showed a number of drunken college women in very compromising positions and the article named every girl in the photographs. One of the photographs was of a student who had not posted it herself. The student was subsequently inundated with phone calls[14] from companies offering to pay her for interviews of a sexual nature, and to this day a search on Google of the student's name returns the *Daily Mail* article (Peterson 11). With the permanence, easy publication, and searchability that the Internet allows, this case shows the danger of not having control of disclosures made by others on social networks.

A case of identity theft via Facebook in the social context that resulted in reputational harm, occurred in Belgium in 2011. A woman was found guilty by a court in Ghent after she created a fake Facebook profile impersonating her ex-employer and conducting activities under the profile that implied he was committing adultery (Tigner). Although the extent of reputational harm in this case was not particularly severe, it is not difficult to imagine the further extremes that this kind of theft can achieve. Facebook tries to ensure that all profiles correspond to real identities (as will be covered further in the next chapter), however there are still instances that go unnoticed. Furthermore, cases of gleaning user details from Facebook and then employing such details in other contexts (for example loan applications) are also possible.

The risk of identity theft in the institutional context may be high too. In 2009, a website called FBHive discovered a security flaw that allowed it to access restricted user data on Facebook: "with a simple hack, everything listed in a person's "Basic Information" section can be viewed, no matter what their privacy settings are. This information includes networks, sex, birthday, hometown, siblings, parents, relationship status, interested in, looking for, political views and religious views" ("Private Facebook Info").

[14] It is assumed that the girl's phone number was obtained from her Facebook profile, after her name was revealed in the article (Peterson).

These cases indicate the harm that can result from diminished privacy on social networks, and the resulting limitations on critical aspects of one's life such as employment, autonomy and safety. With the application of the conceptions established in the following section, the exact reasons why these kinds of violations occur and how the Facebook environment itself facilitates such violations will be explained in the next chapter.

1.6. A Conception of Social and Institutional Privacy

Helen Nissenbaum's proposed framework of "contextual integrity" will form the basis of the conceptions of institutional and social privacy used in this study. The primary foundation of contextual integrity is that "a right to privacy is... a right to **appropriate** flow of information" (129). The appropriateness of information flow is dependent on the particular context concerned, as individuals exist in a variety of specific social contexts in which they act in distinct roles (129). Privacy is therefore governed by norms of appropriateness and norms of distribution. "Appropriateness" determines the kind of information for a particular situation and "distribution/transmission" determines the way in which, and with whom information may be disclosed. In other words this means that "a judgment that a given action or practice violates privacy is a function of the context in which the activity takes place, what type of information is in question, and the social roles of the people involved" (Waldo, Lin, and Millett 63).

In the health care context doctors are obligated to keep their patient's information confidential. If, for example, a patient's information is disclosed to a commercial corporation, the social norm of distribution has been breached. In a friendship context, information transmission (sharing) occurs voluntarily and reciprocally, but again norms of distribution may be violated if information shared between two friends, is revealed to a parent. Norms of appropriateness may be breached when activities appropriate to a social party or a bar take place in a work environment.

Nissenbaum asserts that these informational flows are also governed by the values of the particular context, i.e. the primary purpose of the context. When assessing the norms of appropriateness and distribution of novel situations introduced by new technologies, one needs to refer to the norms of existing contexts that are similar or are intended to achieve the same purposes. In addition, one needs to take into account whether the new technology practices in fact further the specific goals and values of the context.

1.6.1. Social Privacy

It has been shown earlier in this chapter that social networks are primarily an extension of real-world relationships, so Nissenbaum asserts that similar to the context of telephone communication, they should be considered as a context whose primary value is to facilitate information sharing, communication and connecting. Additionally, the telephone system does not exist as one distinct context, but in fact is a "medium for interactions occurring within diverse distinctive contexts, such as family, workplace, and medical" (223). Therefore, for social privacy to be maintained on social networks, the real-world social contexts from which social networks are derived need to be preserved by maintaining their norms of appropriateness and distribution. This implies that the social contexts that exist on social networks need to be separated appropriately, so that for example a photograph taken from the context of a party at a bar with friends does not enter the context of one's work environment (i.e. being visible to one's work colleagues or bosses), and that disclosures intended for one context need to remain within that context. The values of a system that facilitates communication and sharing need to be upheld, and that means that people should continue to want to disclose their information without fearing the kind of consequences described earlier.

It is useful at this point to revisit issues discussed earlier in this chapter in the light of contextual integrity. When addressing the challenge of legitimately requiring privacy in

public, Solove asserts that "although we do things in public, we do them in a particular context before a particular set of people" (*The Future* 165). Furthermore, Boyd and Marwick acknowledge that privacy involves more than the right to privacy in private ("the right to be invisible"), but additionally "who has the right to look, for what purposes, and to what ends" (6) – i.e. the contextual roles and values as defined by contextual integrity. Therefore it is clear that contextual integrity harmonises with the validity of requiring privacy in public, and additionally provides a way to determine the extent of such validity. Additionally, when addressing the privacy paradox (of people's concerns versus their behaviour), Nissenbaum emphasises that "there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information as long as the sharing and withholding conform with the principled conditions prescribed by governing contextual norms" (187) - again asserting that the complexities of privacy cannot be reduced to a strict definition of secrecy.

1.6.2. Institutional Privacy

As described earlier, the institutional context on social networks covers the relationship between the social network owner (a service provider) and its users (consumers), and thus as contextual integrity suggests, one can refer to the context of a consumer/merchant relationship as the basis for the requirements needed to uphold institutional privacy. The norms of this context generally ensure that within the relationship neither party has an unfair advantage over the other; the practices of the merchant in fact serve the primary values of the service that the merchant is intending to provide; and that which the consumer is intending to utilise; and finally trust is fostered (Nissenbaum 195). The nature of the consumer/merchant relationship on Facebook is such that the service provided to users is a medium in which to interact and share information, and the payment for such a service is now in the form of personal information (which Facebook uses for advertising). Facebook acquires vast

quantities of its users' information, and as such the quality of the consumer/merchant relationship is significantly dependant on Facebook's data practices.

Fortunately, even though social networks are new, the existence of merchants in possession of large stores of consumer data is not. Therefore there are common legally established standards for fair data practices that govern this relationship. Thus the conception of institutional privacy is based on the fair information practices as already established in most legal contexts globally.

Currently in America, the U.S Federal Trade Commission's (FTC) Fair Information Practice principles govern the practices of commercial entities and their use of electronic information. The five key principles involved are:

- "Notice/Awareness"- institutions must notify individuals of their collection practices before collecting their information.
- "Choice/Consent"- individuals must be able to choose whether and in what manner, their personal data may be used for purposes other than the initial reason for collection.
- "Access/Participation"- consumers should have access to their information and amend any incorrect or incomplete information.
- "Integrity/Security"- institutions should ensure that the information collected is secure and accurate.
- "Enforcement/Redress"- currently occurs primarily through self regulation as these principles are only recommendations and cannot be enforced according to the law. ("Fair Information").

The South African legal climate with regard to fair information practices is marked by the Electronics Communications and Transactions Act, as well as the soon to be promulgated

Protection of Personal Information Bill[15]. The Electronics Communications and Transactions Act aims primarily to enable electronic communications and transactions, specifically with the goal of ensuring wide and easy access for all economic classes ("Marketing: Understanding The ECT"). However, the act also focuses on developing a secure environment for electronic communications to take place and includes a chapter that outlines a non-compulsory set of principles for personal information and privacy protection. This section is voluntary but the Protection of Personal Information Bill will soon be enacted ("Marketing: Understanding The ECT"). This Bill was designed according to a model very similar to that of the European Union (E.U.) ("Protection of Personal Information"). The Bill involves eight principles that have been developed in various legislatures around the world and that "have become recognised as the leading practice baseline for effective data privacy regulation around the world" (Badat). The principles are:

- "Accountability"- which concerns the responsibility of institutions for compliance with the Bill.
- "Processing Limitation"- which ensures information is processed fairly and lawfully.
- "Purpose Specification"- which limits the scope of the uses of information allowed by an organisation.
- "Further Processing Limitation"- which limits the use of information to those other than initially identified (which need to be defined specifically and explicitly) and for which consumers have given consent.
- "Information Quality"- which ensures institutions preserve the quality of information.
- "Openness"- which asserts that information processing practises are to be transparent.

[15] In September 2012 the Bill was approved by the Portfolio Committee on Justice and Constitutional Development and will then be considered by the National Assembly and the National Council of Provinces ("Protection of Personal Information")

- “Security Safeguards”- which means institutions are to ensure information is safe from “risk of loss, unauthorised access, interference, modification, destruction or disclosure”.
- “Data Subject Participation”- which ensures individuals should be allowed to correct or remove any incorrect or obsolete information (Badat).

These principles cover the same principles as the FTC’s principles, however the explicit requirement for transparency takes the “Notice/Awareness” principle one step further in that not only would institutions need to inform consumers of their practices, but they would need to do so in a clear and direct manner. Additionally, the limiting of scope of the initial and further uses of information also extends the “Access/Consent” principle further. It is also significant to note that in terms of contextual integrity this extension directly links to the need to preserve the contexts of information. For these reasons and because this Bill is based on internationally recognised principles (as mentioned earlier), the conception of institutional privacy applied in this paper will consist of these eight principles.

The next chapter will reveal exactly how Facebook facilitates violations of social privacy by collapsing and colliding contexts in a number of ways. It will also reveal which dimensions of institutional privacy are violated by Facebook’s current data use policy and practices.

Chapter Two

Now that the requirements necessary to maintain both social and institutional privacy have been established, an analysis of Facebook's privacy practices can be undertaken. This chapter will begin this analysis by first tracing the development of Facebook over the last nine years since its inception in 2004, in order to understand the extent of its change from a contained Harvard network to a worldwide network open to anyone. By tracing its development, this paper also endeavours to understand the intentions and personal philosophy of Facebook founder Mark Zuckerberg for this social network, particularly in relation to the large commercial potential of user data Facebook has amassed over almost a decade. This will be followed by an analysis of Facebook's current privacy policies and controls. Once this context (historical and current) has been established, the conceptions of social and institutional privacy will be used to explain how and why violations have occurred and are currently occurring on Facebook. Furthermore, the extent of Facebook's accountability for such violations will be assessed.

2.1. Facebook History

Mark Zuckerberg created Facebook in his Harvard dorm room at the beginning of 2004 for Harvard students (Kirkpatrick 31). Although it may not have been an articulated, fully developed vision at the time, Zuckerberg became famous for saying "I think we can make the world a more open place" (qtd. in Kirkpatrick 42).

2.1.1. Previous Social Networks

At the time of Facebook's inception (originally known as TheFacebook (Kirkpatrick 27)) two popular social networks already existed - Friendster and MySpace - but these were not the first (28). In 1985 America Online started their Internet services that networked

people online through chat rooms[16], message boards[17] and later (1997) an instant messenger[18] service (America Online Instant Messenger - AIM) (64). People would acquire ("quasi-anonymous") usernames and interact with one another. The main difference between AIM and recent social networks is that users typically used this service to interact with their virtual friends only: "Though they maintained email address books inside these services, members did not otherwise identify their real-life friends or establish regular communication pathways with them" (64).

Then, in 1997, the sixdegrees.com service was started. This was "the first online business that attempted to identify and map a set of real relationships between real people using their real names, and it was visionary for its time" (Kirkpatrick 65). On sixdegrees.com one created a profile based on one's real identity (listing one's name, biographical information and interests), and could connect with friends, create groups and search other user profiles (Goble). Unfortunately it occurred at a time when server and database hosting was very expensive and the average users' computing power was very limited due to the slow dial-up modem speeds (Kirkpatrick 66), and in 2000 sixdegrees.com closed its service (Boyd and Ellison 214).

In 2002 Friendster emerged (Boyd and Ellison 215) and by 2003 it had "several million users" (Kirkpatrick 68). It intended to leverage off the fact that it was also a social network for real-world friendships, by allowing people to meet others through friends of their friends (68). With the emergence of digital cameras and faster Internet, Friendster developed the technology to include photographs for each user's profile page, which were also expected to correlate with their real identities. The creators of Friendster were very adamant about this

[16] Chat room is "Web site, part of a Web site, or part of an online service…that provides a venue for communities of users with a common interest to communicate in real time."(Rouse)
[17] Message board is an online bulletin board (Rouse, "What Is Discussion Board (discussion Group, Message Board, Online Forum)?")
[18] Instant messaging is "the exchange of text messages through a software application in real-time" (Rouse, "What Is Instant Messaging (IM or IM-ing or AIM)?")

requirement for users to retain their real identities on the site, and began kicking so-called "fakesters" (people using fake names and identities) off (Boyd and Ellison 216). Because of this harsh reaction, and additionally, because of many technical performance difficulties, Friendster began losing users.

By August 2003, MySpace was launched with the intention of drawing in estranged Friendster users (Boyd and Ellison 216). The creator of MySpace, Tom Anderson, deliberately allowed users to have pseudonymous identities, and to customize their profile pages. This kind of leniency was also evident in the fact that anyone could join MySpace without an invitation from an existing user as on Friendster, and later on minors were allowed to join too.

When Zuckerberg launched Facebook in 2004, MySpace had amassed over a million users (Kirkpatrick 73). As with both MySpace and Friendster, new Facebook users were required to sign up by creating profiles with photos and some biographical information (including relationship status, contact numbers, emails and favourite books/movies/music) (Kirkpatrick 31-32). However, unlike both previous social networks, Facebook was limited to the elite Harvard network only. Similar to the emphasis of real identities on Friendster, Facebook users could only sign up with their real names and their Harvard email addresses (Boyd and Ellison 218). In addition, users had control over who could view their information within the Harvard network (Kirkpatrick 32). In particular contrast to MySpace's flashy profile pages, was the fact that Facebook profile pages were simple and standardised to resemble that of the college face book, a pre-existing printed student directory that contained photographs and basic information of students at a particular university (Kirkpatrick 23,76).

2.1.2. University Networks

By March 2004, Zuckerberg opened up Facebook to Columbia, Stanford and Yale (Schneider). One month after its inception it already had 10 000 users (Kirkpatrick 35). The

privacy setting was such that students could not see profiles of students at other colleges, but after many complaints Zuckerberg realised that opening this up would allow for more growth, and so changed this setting. If two users at different colleges both agreed, then they could view each other's profiles (Kirkpatrick 37).

2.1.3. Advertising

In September 2004, the *wall* was added to profiles. This feature enabled users to write messages on other users' profiles. "Suddenly every TheFacebook user had their own public bulletin board" (Kirkpatrick 87). In this same month the number of users reached 400 000 (89). As the number of users and servers needed to house user data increased exponentially, so did the maintenance costs. Zuckerberg turned to advertising to finance this (Kirkpatrick 37). A company that sold advertising for college newspaper websites, Y2M, began to place some advertisements on Facebook, and was extremely surprised to see the effective results of a MasterCard advertisement for student credit cards: the number of students who had signed up for the card in a day exceeded double what they had expected to receive over four months (Sutherland 15). However, at the time Zuckerberg wanted to keep advertisements on the site as minimal as possible, but understood that some advertising was necessary to cover the site's running costs (Kirkpatrick 42).

In 2005, the further potential of targeted advertising via Facebook was realised when Interscope Records used Facebook to target college cheerleaders in the promotion of a Gwen Stefani song that contained a cheerleading chant. Other than using cookies[19] to track website users, this kind of specific targeting (i.e. targeting based on user provided information) had been used by very few Internet sites at the time (Kirkpatrick 133). It was also more effective than cookie tracking, as cookies collect information per computer, which may be shared by a number of users in very different demographic groups, whereas each Facebook profile is

[19] Cookies are small pieces of data created by a website and saved on a user's computer to store details about the particular user the next time the user visits the website ("Cookie Definition")

directly linked to a distinct user. Zuckerberg and his colleagues at Facebook began to realise the potential of their vast collection of user data. One of the developers soon assembled a list of the valuable user details that could be used for effective targeted advertising and that covered a wide range of potential targets: "geography, gender, course, keywords in profile, class year, major, relationship status, favourite books, movies or music, political affiliation, and university states" (Kirkpatrick 133). Developers also started to write algorithms to tap into this information. Unlike MySpace at the time, Facebook could guarantee that all such data was validated against real identities. A major breakthrough came in June 2006, when one of the largest advertising agencies in the world, Interpublic Group, agreed to invest $10 million in advertising on Facebook (O'Leary).

2.1.4. High School Networks

This critical aspect of ensuring real identities posed a problem for Zuckerberg when he decided to open up Facebook to high school students as, without official college email addresses, validating users would not be possible. Zuckerberg eventually settled for authentication via existing users. In other words, Facebook began to encourage existing college users to invite their high school friends to join the network. The new high school users could then do the same for the rest of their friends (Kirkpatrick 140). At first, the high school and college networks were separate (high school students could not see college student profiles and vice versa), but by February 2006 the two were merged.

The next major development in Facebook's rapid progress was their photo-hosting feature. This feature enabled users to upload photos onto their profiles, on which their friends could comment. In addition to this feature, the developers at Facebook added the ability to tag users in the photos, which would link to their profiles (Kirkpatrick 144). 85% of users had been tagged in a photo a month after this feature was introduced (146).

Then in September 2006, another significant feature was launched: the *News Feed*, a page that aggregated and displayed all the activities of a user's friends. It was introduced without any warning to users. Zuckerberg was shocked to see the extremely negative response following the launch (Kirkpatrick 172). Almost instantly groups against the News Feed emerged, about five hundred in total (Kirkpatrick 178). In one specific group that gathered 13 000 members within three hours ("Students against Facebook news feed"), someone wrote "You went a bit too far this time, Facebook... very few of us want everyone automatically knowing what we update...news feed is just too creepy, too stalker-esque and a feature that has to go"(qtd. in Leyden). In response, Zuckerberg got several of his developers to hastily write new privacy controls so that users could choose which of their activities would be displayed to their friends (Kirkpatrick 178). In addition, Zuckerberg spent all night detailing these new controls in a blog post (179), which started off with an apology and the admission: "We really messed this one up" (Zuckerberg).

This controversy provides great insight into the conflicts between Zuckerberg's vision for transparency and people's concerns about privacy. Zuckerberg has been known to say many times "you have one identity" (Kirkpatrick 186), which he believes should be connected to the endeavour for openness, stating that: "the days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly...the level of transparency the world has now won't support having two identities for a person" (qtd in Kirkpatrick 186). Zuckerberg believes that "having two identities...is an example of a lack of integrity" (qtd in Kirkpatrick 186). This idea of "ultimate transparency" or "radical transparency" seems to proliferate throughout the company, with these two terms being adopted by many Facebook employees (Kirkpatrick 197). In 2012, Zuckerberg affirmed that to "Be Open" is one of the company's five core values, adding that "a more open world is a better world because people with more

information can make better decisions and have a greater impact" ("Zuckerberg Reveals Facebook's 5 Values"). Zuckerberg's zealotry appears to be genuine, as Danah Boyd asserts "my encounters with Zuckerberg lead me to believe that he genuinely believes this, he genuinely believes that society will be better off if people make themselves transparent" (Boyd). Sheryl Sandberg, who became Facebook's chief operating officer in 2008, also affirmed that "Mark really does believe very much in transparency and the vision of an open society and open world, and so he wants to push people that way" (qtd. in Kirkpatrick 195). However, Sandberg also stated that "I think he also understands that the way to get there is to give people granular control and comfort. He hopes you'll get more open, and he's kind of happy to help you get there. So for him, it's more of a means to an end." Sandberg's opinion may explain a lot about why controversies have emerged almost consistently throughout Facebook's development. If Zuckerberg believes that privacy controls offered on Facebook are just a temporary option, then it may explain why, despite its many attempts at changing privacy policies and features, there still remains significant privacy issues and a significant amount of dissatisfaction among privacy advocate groups and some users (which will be discussed further shortly).

2.1.5. Worldwide Open Network

Zuckerberg's goal to create an open world came closer to fruition when in late September 2006 Facebook was opened up to everyone. Instead of joining a college or school network users could now join a regional network (a network associated with their town, city or country). Facebook introduced extra privacy controls at the same time including allowing users to block others in their network from searching or contacting them. Users could also control whether their profile photographs would appear in search results (Arrington).

In 2007, another significant controversy emerged when Facebook launched *Beacon*, an advertising platform that appeared to be the first active attempt to monetise the purchasing

behaviour of its users. With Beacon in place, when a user made a purchase on a particular partner website, that purchase activity was published via the News Feed (Grimmelmann 1147). Beacon was introduced with an opt out in the form of a temporary pop up window that would display in the bottom corner of a page after a transaction was made on a particular site (1148). If a user closed the pop up window or ignored it, the purchase story would be published to the user's profile (Vielmetti). Many users were shocked to discover that their purchases, some of which were embarrassing or intended as a surprise, were revealed to all of their friends, and an anti-Beacon group soon had more than 70 000 members (Grimmelmann 1184). As a result, a class action lawsuit was filed against Facebook. In September 2009 Beacon was discontinued and in December 2009 the lawsuit was settled (Boyd and Hargittai).

Perhaps as a result of the failure of Beacon, in March 2008 Sheryl Sandberg, former vice president of Global Online Sales and Operations at Google, was hired by Zuckerberg as chief operating officer in order to turn Facebook into an "advertising powerhouse" (Kirkpatrick 240; Smith). At the time Facebook was only just covering its rapidly growing operating costs. Sandberg began running bi-weekly sessions at Facebook on how to monetise the large store of user data that it owned (Kirkpatrick 241). "Engagement ads" were a product of these sessions. These advertisements would appear to a user in the form of a link to the particular business's Facebook profile with a message encouraging the user to, for example like the profile. These advertisements produced about $100 million in revenue in the first year, with Facebook charging $5 per thousand views. Since Sandberg joined, advertisers using Facebook's self-service advertisements (advertisements that smaller advertisers buy directly from the Facebook site with a credit card) tripled in one year. By 2009, Facebook's overall revenues were more than $550 million, an increase of over $250 million since 2008 (Kirkpatrick 246).

2.1.6. More Features

In contrast to the controversies of the News Feed and Beacon features, Facebook did in fact provide some privacy controls with the introduction of *Friends Lists* in 2008. This control gave users the ability to create various groups and select which friends could be added to these. These groups could then be used to limit who had access to certain kinds of information (Peterson 30). In December 2009 Facebook overhauled many of its privacy controls in order to provide what it claimed to be improved privacy for its users (Bankston). These changes intended to simplify privacy controls by removing regional networks, which had previously allowed many users to unknowingly expose their profiles to other users in their entire city or country. Another change allowed users to select the privacy setting of each post (e.g. a *status update*[20] or posted photo). Facebook also provided users with a tool to guide them through the various privacy controls and settings. However the privacy guide recommended settings which encouraged users to allow exposure to "everyone" (completely public – to search engines and non Facebook users as well), whereas before the default was such that information was exposed to the regional network. Furthermore, Facebook also changed certain user details (gender, current city, *friends list*[21] and *Page likes*[22]) to be permanently public[23]. Before the change only a user's name and network were publicly available ("EPIC's Facebook Complaint"). Because of this, the Electronic Privacy Information Center filed a complaint with the FTC regarding what they termed "unfair and deceptive business practices" (Schwartz). In 2012, this was finally settled. Facebook agreed to "give users 'clear and prominent' notice when their information is shared; obtain their express consent before doing so;… maintain a privacy program; and have privacy audits every two years" (Schwartz).

---

[20] See glossary
[21] See glossary
[22] See glossary
[23] Accessible and searchable to all Facebook users and non-users (see next section on Facebook privacy policy)

Facebook furthered its growth on the Internet in early 2010 by launching its *Social Plugin*[24] and *Graph API*[25] platforms that allowed other websites to integrate with Facebook, and which enabled other developers to create applications using Facebook data and actions. For example, a user could like a website and this action would then be linked to the user's Facebook profile. In just one week of launching, about 50 000 websites had adopted the Social Plugin (Parr). These new changes yet again concerned many, including advocacy groups like the Electronic Privacy Information Center who filed a second complaint with the FTC stating that the Social Plugins were "misleading and deceptive" because it was not clear the extent of access third party developers had to user data ("Social Networking Privacy"). Many users declared a "Quit Facebook Day", and Facebook eventually responded to their concerns with an announcement conceding that their privacy settings page was too confusing (Boyd and Hargittai). As a result, Facebook launched a new, less complex settings page in May 2010.

In September 2011 Facebook appeared to be taking further steps for improved privacy when it launched an enhanced version of its 2008 Friends Lists feature. This original feature had only been adopted by 5% of users, according to Zuckerberg (Scott). The improved version automatically creates friends lists based on data that Facebook compiles. Automatic lists include family, school friends, university friends, and friends living in a user's city or hometown. It also creates a "close friends" list, which a user needs to populate him/herself. However, this is facilitated with suggestions based on tracked frequent interactions with friends.

[24] A plug-in is an additional piece of "software that is installed into an existing application in order to enhance its capability" ("Plug-in Definition from PC Magazine Encyclopedia")

[25] API stands for application programming interface and is "a language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol"("API Definition from PC Magazine Encyclopedia")

By 2011 Facebook had amassed 500 million users (Hepburn) and was earning $5.11 per user in targeted advertising revenue (Weise). Since then, many more features were instituted on Facebook (and are covered in the next section in which Facebook's current privacy policy is analysed). In the first three months of 2012, Facebook had a net income of $205 billion and a revenue of $1.06 billion, and on 18 May held its Initial Public Offering (Ortutay).

2.2. Current Privacy Policy

Now that an historical context has been established, a description of Facebook's current [26] privacy policy will be provided. Facebook terms this policy its "Data Use Policy". The policy is broken up into subsections and in total is 8 700 words in length.

2.2.1. Information Facebook Receives

The first section is titled "Information we receive about you" and details what Facebook knows about its users (Couts). Facebook keeps all information a user shares. This includes the information required for registration, all information linked to activities on the site, and all information a user's friends share about the user ("Data Use Policy"). Additionally, Facebook receives information when a user or non-user interacts with websites that use the Social Plugin or Platform (described in detail shortly). Andrew Couts, in his article analysing the policy, summarises all the data Facebook receives as follows:

- Name
- Age
- Gender
- Email address
- Networks
- Photos and videos
- Tags and facial data
- Profiles you view
- People you chat with via Facebook Messenger
- Relationship status

[26] As of June 8 2012

- Likes
- Lists of Interests (movies, music, books, etc)
- Political association
- Websites visited
- Purchases using Facebook Credits
- Metadata of the above activities (time, date, place of activity)
- Browser type
- Operating system type
- IP address
- GPS location
- User ID number
- Username ("Data Use Policy") (Couts)

Additionally, Facebook performs aggregation (as explained in the previous chapter, combining separate pieces of data for further interpolation) on certain data: "We also put together data from the information we already have about you and your friends. For example, we may put together data about you to determine which friends we should show you in your News Feed or suggest you tag in the photos you post" ("Data Use Policy").

It is then indicated that some of the shared information can be made private but some will always be public. Public information can be associated with a user outside of Facebook. It can be searched via Facebook's search utility as well as on any search engine. It can also be accessed via "Facebook-integrated games, applications, and websites" used by a user and his/her friends ("Data Use Policy"). The following information is always public: "name, profile pictures, cover photos, gender, username, user ID, comments made on public websites that use Facebook's commenting plug-in, comments made on public websites through Facebook's commenting plug-in about you by other people" (Couts). Additionally, if a friend shares information about a user with a public setting, that information will be public.

One is able to make most of the information sharing on Facebook "private" and to vary the degree of privacy to some extent. This means that one can choose to share with all of one's friends, or a certain list of friends. A description of how to employ these controls is

provided in the next section (“Sharing and finding you on Facebook”) which will be explained shortly.

Facebook then, very briefly and quite vaguely, explains what it does with user information: “We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use” (“Data Use Policy”). It then only provides six examples of how it uses this information. In addition, these examples are worded in a manner that seems to advertise Facebook and provide justification for the uses rather than objectively listing them. Facebook can share user information if a user has given permission, or the user has read this Data Use Policy, or any identifiable information has been dissociated from the user.

The period of data storage is described as “as long as it is necessary to provide products and services to you and others”. Additionally, it is stated that “typically” this period will be up until an account is deleted. At this point the policy details information regarding the deleting and deactivating of an account. A user can either put his/her “account on hold” (deactivate it) or terminate his/her account completely (delete it). If an account is deactivated then information is not deleted but the user’s timeline is not visible. If an account is deleted, it is stated that it takes about a month to delete information, although “some” information may still exist for 90 days. Data that cannot be solely linked to a user’s account, like group postings or messages to other users, will not be deleted.

2.2.2. Information Disclosures and Facebook Search

The next section in the policy is titled “Sharing and finding you on Facebook”. This section first details the controls a user can employ to restrict access to their information sharing. As explained earlier, a user can select the audience of certain posts (including status

updates, photo uploads or *check-in*'s[27]). As shown in the image below, the audience can be defined as public, friends or a custom audience that a user must create by setting up a specific friends list, using the Friends Lists feature (as described in the History section earlier).

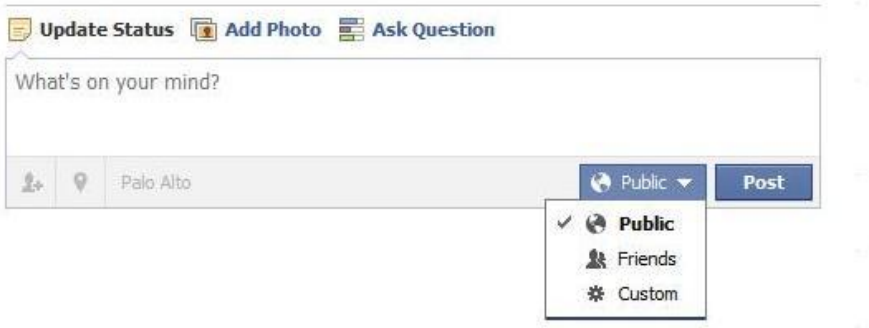

Figure 1: Feature to Restrict Audiences

It is also indicated that although one can restrict these posts, if a user comments on a friend's post, the user cannot control the audience. Additionally, "If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story" ("Data Use Policy"). Basically this means that "any content that is about you, but controlled by someone else, is out of your hands" (Couts). If one does not see a sharing icon (the drop down list in the image above) next to a piece of information, then it is an indicator that that information cannot be made private (as described earlier, related to what is public information).

Next, the policy describes how users can be found in the Facebook search functionality. If a user has linked his/her email address or phone number to his/her account then anyone can search for that user using the email or phone number. This can however be restricted with privacy setting controls. In addition, a user can be found via the contact importer functionality which uses information from other services like Gmail to find users.

[27] See glossary

Slightly out of place here is some information on the Activity Log, a page that allows a user to view, edit (content and visibility), or delete some of their Facebook activities.

The last part of this section details the accessibility of information about a user that his/her friends have shared, specifically with regard to tagging, groups, and *Pages*[28]. A user can select a setting that allows him/her to either automatically approve all tags any friends make, or for approval before all tags, or select friends who do not need approval. A user can elect to join a group, and his/her name will be visible as "invited" until the user opts out. All activities on a Page are public.

2.2.3. Third Parties

Following this, a section entitled "Other websites and applications" is provided. First Facebook's Platform is explained and discussed. The Platform allows other (outside of Facebook) websites, applications and games to access user information. Third-party applications have access to all of a user's public information, including his/her User ID as well his/her friends' User IDs. For any additional information the application must ask for explicit access to the information. It is indicated that a user can elect to close off access to their public information by Platform applications. This, however, means that the use of any of the Platform applications is completely restricted. Facebook also provides a set of controls to view a list of applications a user has added and the last time each of these applications has retrieved user information. Additionally, here a user can remove applications, review permissions a user has given to applications and the audience of stories related to application activity. An image of this control is shown below.

[28] See glossary

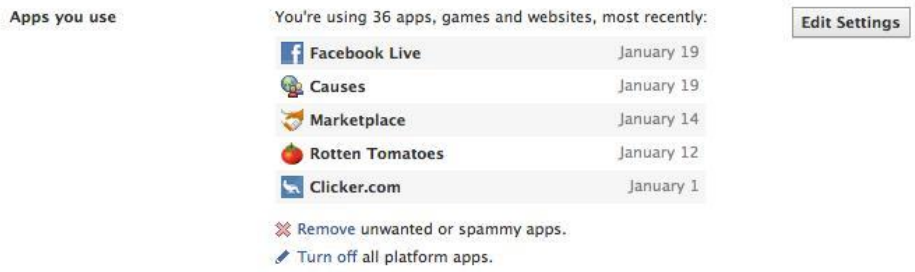

Figure 2: Application Control Feature

If a user removes an application, it is suggested in this policy that he/she should contact the application directly to request deletion of remnant data. This would mean a user would have to track down the third party application owners to make such a request. It is also important to note that an application is able to access all of a user's public information if his/her friend has installed the application. Additionally, information that a user may have only shared with a friend, can also be accessed by the application, if it has requested permission from the friend. There exists an additional control that allows a user to restrict the type of data available to applications via a friend's application. An image of this control is shown below.

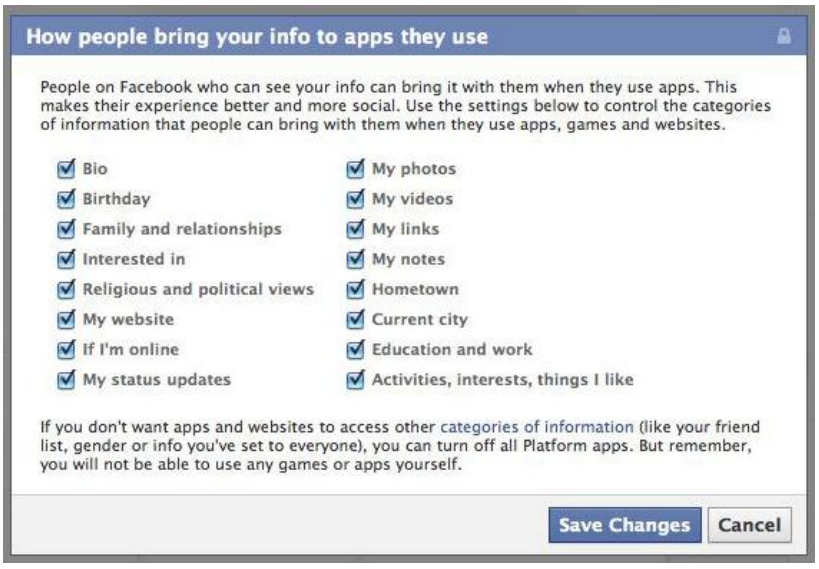

Figure 3: Control Access via Friends' Application

In addition to applications, another way Facebook links to external entities is by allowing users to log into other websites with their Facebook credentials. To do this Facebook gives the website the user's User ID.

As described in the history section earlier, the Social Plugin is yet another way that Facebook interfaces with external websites. When a user or non-user visits one of these websites, Facebook logs information regarding this visit (including user name, IP address, browser, visit time) (Couts). This logging is performed through the installation of cookies on a user's computer (to be described in more detail shortly). This data is kept for 90 days maximum, after which any elements that allow it to be associated with a specific user are removed.

One last Facebook/third-party collaboration is the *Instant Personalization.* If a user is logged into Facebook and browsing one of the chosen partner websites, that website can access all the public information of the user. This service, like the previous ones mentioned can also be turned off but again, the other website needs to be contacted directly to request data deletion. However, the first time one of the websites is visited, a notification informing of the Facebook partnership appears. Here a user can immediately elect to turn off Instant Personalization, in which case the website is required to delete all user data it may have already acquired straight away and may not access any more data at a later date. The policy also asserts that any partner websites must enter into an agreement with Facebook protecting users' personal data.

The last part of this section states that by default a user is searchable in all online search engines, but can elect to turn this off.

2.2.4. Advertising

The next section of the policy details information concerning Facebook advertising. Facebook performs three different kinds of advertising: *Personalized Ads*; *Sponsored Stories*;

and Facebook content. Facebook asserts that personal information is never shared with third-party advertisers. Information is only shared once "we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you" ("Data Use Policy"). Sponsored Stories occur as a result of the activities of a user's friends (e.g. liking a product or service, or "RSVPing" to a commercial event) and appear in a designated advertising space on the side of a Facebook page. Facebook may advertise its own features in the same way it uses sponsored stories. This policy also mentions Facebook advertisements that are "paired with social actions your friends have taken". It is not clear how this is different to Sponsored Stories, however unlike Sponsored Stories, a user can choose to opt out of appearing in these kinds of advertisements.

2.2.5 Tracking Technologies

A section titled "Cookies, pixels and other system technologies" is covered next. Here cookies are explained as "small pieces of data that are stored on your computer, mobile phone or other device" and pixels as "small blocks of code on web pages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies" ("Data Use Policy"). Local storage is described as an "industry-standard" technology that works in a similar manner to cookies but has the ability to keep more information. A few brief examples of the uses of these technologies are listed, such as to speed up page loading and navigation on the Facebook site, to track the use of Facebook features. It is then stated that third party websites that integrate with Facebook may use cookies as well. These technologies may be blocked by changing browser settings but this will affect the use of Facebook and the other websites.

The final section in this policy is titled "Some other things you need to know". Here it is first stated that Facebook "complies with the US-EU and U.S-Swiss Safe Harbor

Frameworks[29]" with regard to the "collection, use, and retention of data from the European Union". This section also indicates that Facebook may keep and share user information if they have "good faith belief that the law requires" it. Additionally, user information may be shared with "the people and companies that help us provide, understand and improve the services we offer". Only a few examples of these people or companies are given, but it is stated that these entities may only use the information in ways allowed by the Data Use Policy.

It is then indicated that a user may have access to and rectify most information that Facebook stores. A downloadable copy of personal information is also available. It is also stated that "We do our best to keep your information secure...We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products".

Changes to the policy will be publicised on the Data Use Policy page and on the Facebook Site Governance page. It also states here: "If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances". If changes are made for purposes other than legal or administrative, then users have seven days to make comments requiring any changes. Voting for a change will be allowed if more than 7 000 comments are made regarding this change. If more than 30% of registered users vote, it will be binding.

2.3. Why Privacy Violations Occur

With the historical and current context of Facebook's attitude and actions towards privacy established, this section will now endeavour to explain how and why privacy violations on Facebook have occurred and in which ways Facebook is responsible for these violations. This will be done by making use of both the social and institutional privacy

[29] US-EU and U.S-Swiss Safe Harbor Frameworks are programmes that ensure American organisations processing or storing data of users from the EU or Switzerland comply with the data protection regulations of the EU (European Commission's Directive on Data Protection) and Switzerland (Swiss Federal Act on Data Protection) respectively ("Main Safe Harbor Homepage").

definitions established in the previous chapter. In some instances certain Facebook features are responsible for eroding both institutional and social privacy. However, first an analysis of social privacy violations occurring on Facebook will be provided.

2.3.1. The Architecture of Online "Public"

With the understanding that people do in fact require privacy in public as established in the previous chapter, it is necessary to tackle exactly how the "public" that exists in the online Facebook environment is different to real-world public. This will reveal why privacy invasions occur with regard to the conception of social privacy, which requires that the diverse range of contexts existing on Facebook remain preserved by appropriate separation.

The first fundamental difference between online and offline public is related to the architecture of physical space. In the real and corporeal world, there exist structural boundaries that people are immediately aware of and that enable an amount of privacy despite being in public (Boyd, "Facebook's Privacy Trainwreck" 14). For example, a wall can hinder the audibility of a person's voice (Peterson 16). Yet in the realm of online social networks "one can be an [observer] being physically present; one can communicate 'directly' with others without meeting in the same place. As a result, the physical structures that once divided our society... have been greatly reduced in social significance"(Meyrowitz i).

Additionally, different physical spaces have different social norms. For example, one behaves differently in a library than in a bar because:

> The Physical separation of social situations is a by-product of the properties of the corporeal world. Walls, roofs, and fences not only keep intruders out, they define specific audiences or communities within which social norms operate, and make it easy to see where and to whom information flows (Peterson 15).

The lack of physical or tangible markers distinguishing different social situations leads directly to a collapsing of contexts, which, as contextual integrity (and the social privacy conception upon which it is based) asserts, allows privacy invasions to occur.

A further analysis of the News Feed controversy mentioned earlier provides an example of this context collapse and reveals why the introduction of this new feature in fact became so controversial. In her paper "Facebook's Privacy Trainwreck Exposure, Invasion, and Social Convergence", Danah Boyd provides an excellent analogy between the News Feed controversy and a real-world example. Here she asks the reader to "Imagine that you are screaming to be heard in a loud environment when suddenly the music stops and everyone hears the end of your sentence. Most likely, they will turn to stare at you and you will turn beet red" (14). Boyd explains that similarly many Facebook users were continuing with their activities on Facebook in the belief that unless someone was specifically choosing to monitor their profile regularly, their actions would remain relatively obscure to the rest of their Facebook friends. The sudden and unexpected introduction of the News Feed created a huge shift in the environment and the conception of public within which users were interacting, and as such resulted in significant objection from users. In the offline world, often privacy is assumed as the default because the publication and dissemination of information requires effort as a result of physical constraints. In the online context of social networks, the very opposite is the case. What was once "private-by-default" is now "private-through-effort" (Boyd and Marwick 9), and with the introduction of the News Feed this was even more the case. Users had to actively restrict each post and action subsequently to ensure privacy.

2.3.2. Invisible Audiences

In addition to the absence of an architectural separation of social contexts on Facebook, there are more features of the online environment that create a significantly different version of "public" and thus contribute to further collapsing of contexts. Boyd and

Marwick identify four specific features that radically reconstruct this environment. They are "persistence, replicability, scalability, searchability" (9). "Persistence" indicates that online (and specifically Facebook) activities remain stored on servers for indefinite lengths of time. As seen in Facebook's privacy policy, unless a user actively deletes his/her account, his/her personal data will be stored on Facebook's servers indefinitely. In addition, if a user does delete his/her account, all data about him/her controlled by his/her friends or for example on public Pages will remain. Recall the account from the previous chapter, in which the tabloid article containing the embarrassing photograph and name of a student still appears five years later in Google search results. "Replicability", implies how commonly and easily data is copied from its original context and "scalability", how quickly data may be spread to wide audiences. Lastly, "searchability" represents the immediate accessibility of data via search engines. As indicated in the privacy policy, all users' profiles are searchable both on online search engines, unless the control to switch this off is changed, and additionally via the Facebook search functionality.

The result of all these features is that any information disclosed on Facebook can draw audiences that may not have been anticipated at the time of revelation. This is what Boyd and Ellison term "Invisible Audiences" (3). Because one cannot anticipate all the possible eventual audiences of particular activities on Facebook, the number of potential contexts in which any piece of data may be viewed is unbounded and so once again, contexts converge and violations are felt, as illustrated by the case studies presented in the previous chapter. In addition to the invisibility of potential future audiences, although a user may have some awareness of who his/her Facebook friends are (and may also have privacy controls set to limit his/her audience of friends), at the time of disclosure there is no immediate and tangible indication of every friend with access to the disclosure, nor a friend's particular response to such a disclosure (Boyd, "Facebook's Privacy Trainwreck" 16). Without this

essential feedback, implications of every information revelation may not be present in a user's mind and additionally, because a user may not be aware of a particular audience reaction, any necessary adjustments to remedy resulting conflicts are lost. This may be exacerbated by the fact that very often self-disclosure on Facebook happens impulsively. Solove asserts "because you can't see or touch your audience, because you blog in the solitude of your room, in front of your computer late at night, it doesn't seem like exhibitionism. There's no bright spotlight. It's just you and your computer" (*The Future* 199). So in addition to the fact that the online world lacks the architectural indicators that guide our information revelations, this realm also lacks the necessary "social heuristics" (Peterson 18).

It is important to acknowledge at this point the existence of the Facebook Friends List that was mentioned in both the history and privacy policy sections. By setting up specific lists of friends one is in fact able to limit the audience at the time of posting and thus have better visibility of the audience. However, as a particular list may grow - in 2011 about 2 million *friend requests*[30] were accepted every 20 minutes on Facebook across the world (Hepburn) - an awareness of the exact people in the list may be difficult to maintain, thus blurring the visibility of audiences.

Chris Peterson points out further shortcomings of Friends Lists by first asserting that this feature remains "chronically underused" (31) and as mentioned in the history section earlier, the first iteration of the Friends Lists feature had been adopted by only 5% of users (Scott). Peterson states that Facebook does not emphasise strongly enough that Friends Lists can be employed for privacy protection, and that Facebook does not make it easy to use this feature efficiently. However, at the time Peterson wrote this, in order to create a particular list a user needed to manually add each friend out of a potentially large number of friends. Since Peterson's assertions of these important points, the Friends Lists feature has been improved to

[30] See glossary

add the smart lists as described earlier. The existence of the automatic lists as well as the suggestions of friends to add to the "close friends" list does in fact facilitate the process of audience limiting. However, Facebook could do more to emphasise the benefits of employing this feature and the question of whether it is still underused remains. In a survey conducted in June 2012, it was revealed that out of 104 people only 27% were adopting the Friends Lists feature (Couch).

2.3.3. Social Convergence

The early lack and subsequent underuse of the Friends Lists feature helps to explain the continuing existence of another argument raised against Facebook that maintains its role in contributing to the collapsing of contexts or "social convergence" (Boyd, "Facebook's Privacy Trainwreck" 15). Often, the reason why audience invisibility is a problem is because of the existence of multiple disparate audiences. Because on Facebook one may be friends with one's grandmother, one's work colleagues and one's close friends, the convergence of all social contexts is rife. In addition to the flattening of one's social world that occurs on Facebook, it is very common for people to have mere acquaintances as friends, what Boyd terms "weak ties" ("Facebook's Privacy Trainwreck" 18). Gross and Acquisti also observe that "social networks are both vaster and have more weaker ties, on average, than offline social networks" (3).

Despite Zuckerberg's claims that having more than one identity is disingenuous and deceitful, it is in fact very common for people to have different personas and behaviour relevant to different contexts and subject to distinct audiences. In the real world one has a complex and highly structured set of social connections – "each connection involves different levels of exposure and different ways of sharing information. And while we may share information freely among one social circle, we may not want information to bleed between the different social circles we occupy simultaneously" (Solove, *The Future* 202). Solove

refers to many sociologists, philosophers and psychologists when stressing that we are "complex, multifaceted" beings and thus " we express different aspects of our personalities in different relationships and contexts" (*The Future* 69)[31]. However, on Facebook one's social network is greatly simplified and the "nuanced barriers to information flow" are removed (*The Future* 202). From Zuckerberg's statements insisting on the integrity of one identity, it is clear that this is an intentional design of Facebook.

Although the progress of the Friends Lists feature does allow for more separation of contexts there may still be a limit to the extent to which distinct lists can capture the nuances and changing characteristics of real life relationships. "Adding 'FriendYouDontLike' to a controlled vocabulary will not make it socially complete; there's still 'FriendYouDidntUsedToLike'" (Grimmelmann 1186). With this example, Grimmelmann is emphasising the difficulties in trying to reduce a rich range of real life relationships to a set of discreet lists controlled by a limited range of technical interface features.

Furthermore, Facebook insists on users having only one account that correlates with their real life identity, so users are additionally limited to separating contexts by having separate accounts for particular contexts. Facebook goes to somewhat extreme measures to ensure real identities are used. In 2011 famous author Salman Rushdie's account was deactivated and Facebook demanded Rushdie submit proof that the account was real. Once Rushdie had provided a copy of his passport, Facebook reactivated his account, but insisted that the account name be changed to Ahmed Rushdie, as Salman is his middle name (Gaylord). It is clear that Zuckerberg's philosophy of an open society corresponds with Facebook users having one account each. However, the fact that Facebook can validate the

[31] Solove refers to William James, a philosopher and notable psychologist, who asserts that both young people and adults behave differently around different people. He refers to sociologist Erving Goffman, explaining his view that "we live our lives as performers; we play many different roles and wear many different masks". He also refers to Arnold Ludwig, professor of psychiatry, and philosopher Hannah Arendt when addressing the myth that the private self if more genuine

information provided by users against their real life identities, means that advertising can be directly targeted at users.

Even though Friends Lists may help control the audiences of our disclosures, as acknowledged in the Facebook privacy policy, there still remains a limit to the control a user has over the audience of comments on friends' posts or public Pages and groups. Additionally, a user cannot control the privacy settings nor the disclosures of his/her friends. For example, a friend can tag a user in a photograph, and although the user can choose to remove the tag, that photograph still remains. An exacerbation of this loss of control arises as many people are able to tag a particular photograph. Furthermore, it is also very possible for a user's friend to copy, and disseminate to wider audiences, a post intended only for that user's friends. This appears to have been the case with Shaheen Dhada as discussed in the previous chapter. Violations occur when a user may have different expectations of privacy to those of his/her friends. Additionally, as revealed in the previous chapter[32] a substantial amount of informational insight can be inferred from the cumulative data of one's friends. Because of the existence of weak ties (as mentioned earlier) on Facebook, it is even more likely that a mismatch of privacy expectations and behaviour may occur between a user and his/her Facebook friends (Grimmelmann 1175).

2.3.4. Changing Contexts and Instability

It is important to be cognisant of the fact that when Facebook first started it was limited to just the Harvard network. This made it somewhat implicit that the college context remained intact allowing contextual integrity to be naturally preserved (Peterson 32). However, because of the rapid pace of development of Facebook and the many (often unexpected) changes put into place by Zuckerberg (as indicated in the history section), this preservation of contexts has been drastically shattered, with users sometimes left in a state of

[32] Recall Grimmelmann's report on a study where researchers could deduce the age and nationality of a user of a social network based on the details of the user's friends (Grimmelmann 1173)

shock and indignation (for example, the case of Beacon). Facebook is now open to everyone and exists across the world, covering a large number of contexts in different countries, sometimes resulting in severe consequences, as evident in the case studies from the previous chapter.

The kind of instability described above is in itself a significant reason why many privacy violations are felt on Facebook. In addition to contexts colliding at a single point in time, from one period to the next, the change in various features can cause contexts to unexpectedly change. As Grimmelmann explains in reference to contextual integrity: "once a site has established a social "context" with specific informational "norms of flow," it transgresses those norms by changing the structure of informational flow" (1169). When Beacon was introduced, users were surprised to see information that they had expected to remain in one context suddenly moved to an advertising context. This also happened earlier with the introduction of the News Feed, when users' expectations of information visibility were abruptly broken.

As described in its Data Use Policy, Facebook has the right to make changes at any time to any of its features. What is quite disconcerting is the visibility and notification of these changes. As pointed out, changes to Facebook's policy will be publicised only on the Data Use Policy page and on the Facebook Site Governance page. It does say that "If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances". However, what constitutes a "material" change is not described or specified in the documentation.

As was discussed using the Beacon and News Feed controversies as examples, this kind of instability on Facebook may have dire consequences for social privacy. However, with regard to institutional privacy, volatility is problematic as well. Firstly, in terms of the safety of users' personal data stored on Facebook servers, it is quite possible that with so

many dynamic code changes, the protection of data may be jeopardised ("Security Safeguards"). According to Grimmelmann, such incidents have occurred in the past (1170). What makes this even more disconcerting is the fact that in its policy, with reference to data security, Facebook states that it cannot make "guarantees about any part of our services or products". With regard to the definition of institutional privacy established in the previous chapter, it is of fundamental importance that the safety of personal data is maintained and that a user be assured of this. Secondly, a user may decide to disclose information on Facebook with the knowledge of its initial use. However, if Facebook then suddenly changes its policy to entitle it to use that data for an entirely different purpose, according to the definition established, this constitutes a violation ("Further Processing Limitation"). Furthermore, the requirement of "Further Processing Limitation" also emphasises the need for clear and explicit notice and consent for any changes to data use. As already pointed out here, it is not clear what conditions allow for change notifications to be placed in a prominent place outside of the Data Use Policy.

2.3.5. Privacy Policy

The Data Use Policy in itself is problematic in terms of institutional privacy as well. As indicated, the length of the policy is a protracted 8 700 words, an intimidating document to tackle and longer than the U.S. Constitution which is 4 543 (Bosker). As pointed out earlier in the description of the policy, there are a number of vague statements about the exact use of user data and often only a few examples are given of the use (seen in the general use of data section, the use of cookies, and the sharing of data with third-party services). If Facebook can afford to use so many words in this policy, it should most certainly be able to explicitly and objectively list the exact use of data. According to the institutional definition of privacy, a user should know the exact use of his/her data.

Additionally, in "Saving Facebook", Grimmelmann summarises a number of surveys that have shown that users rarely read Facebook's privacy policy and if they do, often don't understand most of what is written in it (1182). Boyd additionally questions why a user's understanding of privacy settings has to be through the "abstract process" of trawling through the privacy policy, which is "removed from the context of the content itself" ("Putting Privacy Settings"). As required by the institutional privacy conception, data practices are to be open and transparent ("Openness"). This is certainly not the case with the lengthy, vague and at times confusing state of the Data Use Policy, despite the fact the policy is written in relatively simple, non-legalistic language.

The analysis of this privacy policy has revealed that there are several more issues which are problematic for institutional privacy. Perhaps most obviously is the sheer extent of personal data Facebook has access to as revealed in the Data Use Policy. As established by the institutional privacy requirements it is important that the scope of data a company may collect should be limited ("Purpose Specification"). The fact that Facebook's large data collection is all stored on one server is also problematic for security reasons, especially in light of the risks of identity theft described in the previous chapter. Although up to this point Facebook itself has not deliberately used user data in any particularly malevolent manner, it is stated in the policy that Facebook may reveal data for law enforcement purposes. It is not clear what circumstances this covers exactly, so the potential for Facebook or government and law enforcement, to abuse this store of user information exists[33].

[33] Although in America the Stored Communications Act restricts the government from forcing Internet Service Providers to reveal electronic information it stores (Ward 566). In South Africa, The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 "makes it illegal for any authority to intercept communication without the permission of a judge designated to rule specifically on all interception applications in South Africa." This covers information an Internet service provider may be storing (Swart).

2.3.6. Data Subject Participation

The fact that user data is centralised and owned by Facebook, means that the "Data Subject Participation" requirement should be vigorously maintained. Facebook has improved its policy when it comes to data deletion, as now when a user deletes his/her account, according to the policy, all data will be deleted. However, the shortfall here is that once again data controlled by a user's friends will remain. Additionally, for the deletion of any data held by third-party websites/applications, a direct and explicit request for this deletion needs to be given to the websites/application developers concerned. This process may not seem obvious to a user and with the large amount of third party applications available, it may be very difficult to keep track of such data leakage. Furthermore, as indicated, applications may access a user's data if that user's friend installs the application. In this case a user may not even be aware of such an application accessing his/her data in the first place. Unless a user deletes his/her entire account there also exists no easy way to delete large amounts of data at a time, instead each piece of information needs to be removed tediously one at a time. These issues conflict with the requirement of "Data Subject Participation", as users should be able to easily delete any of their data. "Data Subject Participation" is also violated by the fact that the policy again rather vaguely states access to "most" data without any explicit indication of what "most" covers. In 2010 an Austrian law student, Max Schrems, decided to request a copy of all his Facebook data from Facebook directly. He received a document that was 1,200 pages long, but it still did not contain all of his information (Solon). Schrems subsequently filed a number of complaints against Facebook. Soon after, Facebook instituted the data download tool as indicated in the Data Use Policy. However, according to Schrems, this only provides access to 23 out of 57 categories of data that Facebook owns (Solon).

2.3.7. Default Settings

For many of the issues raised above (both social and institutional), Facebook often asserts that their provision of controls (like the Friends Lists) implies that they actively care about privacy. Somewhat contradictorily, as mentioned previously, Zuckerberg has said that privacy as a social norm has disappeared and that people are now naturally changing to want to reveal more information. However, it is imperative to acknowledge in what way Facebook is in fact responsible for and encouraging such information disclosure and apparent changes in social norms. Solove asserts the ability of the architecture of websites to influence people's behaviour and the significant power of default settings (*The Future* 200). Throughout the analysis of Facebook's privacy policy it is very clear that although controls exist, the default state is always that information is open to the public. When a new user joins Facebook, his/her profile is by default open to the public, and he/she has to actively go through each privacy control to change this. Throughout most introductions of new features, the default was to share information publicly. For example when Facebook allowed user profiles to be accessible via online search engines, the default was that this would be the case and to control this, one would have to actively opt out (Boyd and Hargittai). Looking once again at the News Feed introduction, the default state of the Facebook environment was changed "from a 'pull' to a 'push' environment overnight" (Peterson 20), meaning that it then became the norm for information to be widely and freely disseminated, as opposed to its previous state where it was somewhat contained within a user's discrete profile.

The state of default settings is imperative in guiding the behaviour of users as extensive research has shown that people rarely change defaults (Boyd and Hargittai) – "most people find it easier to accept a default choice made on their behalf regarding a putative decision than to change that choice, even if the default choice is less advantageous to them than changing that choice" (Waldo, Lin, and Millett 76). Peterson describes a study on

residents of Iowa which consisted of two parts. In the first part subjects were requested to indicate if they wanted their organs donated (if they died in a car accident) by ticking off a box in a form. Here 42% of subjects ticked the box. In the second part, subjects were asked to indicate if they did **not** want their organs donated by ticking the box. In this case only 12% of subjects ticked the box, leaving more than double the number of people from the previous case apparently happy with donating their organs (Peterson 23).

The result of Facebook defaults is that users are led to share more and more information, thus making both social and institutional privacy infringements more likely. When one considers Zuckerberg's frequently expressed desire for openness and information sharing as described earlier, and the additional advertising pay-off Facebook receives from increased information disclosure, it appears that these defaults are very much intentional.

When assessing Zuckerberg's personal philosophy, it is not clear exactly how much of this push for increased information revelation is motivated by the advertising gains of Facebook's massive data store. As indicated by accounts of various people (Kirkpatrick, Boyd, Sandberg), it does appear that Zuckerberg is genuinely fanatical about his vision for an open society, with people having one transparent and homogeneous identity. Whether or not Zuckerberg is using this zealotry as a disguise to commercially exploit Facebook users' data, the fact is that Facebook does benefit hugely from its advertising revenues, and Sandberg was hired explicitly for this purpose. With Facebook now accountable to its shareholders, the need to take advantage of its user data is even more significant. What is important to note regarding the details of how violations occur, is that although many claim (including Zuckerberg himself) that people no longer care about privacy and that the social norms regarding privacy have drastically changed, as this paper has shown, expectations are mostly the same. What is different is the environment in which these social interactions now occur: "Privacy is in a state of flux not because the values surrounding it have radically changed, but

because the infrastructure through which people engage with each other has" (Boyd and Marwick 26). Facebook is in many ways responsible for this change in the online environment – an environment which causes conflicts from collapsed contexts on many different levels; one which centralises and controls users' personal data in uncertain and thus discomforting ways; and one which encourages maximum information revelation through its default settings.

Chapter Three

With the conceptions of privacy already established and the analysis of Facebook completed, this chapter will assess the success of Diaspora* as an example of an alternative social network to Facebook. First it will be explained what Diaspora* is and how it functions as a social network. A history of the somewhat turbulent two-year development of this social network will be given, indicating the context in which the project started, specifically in relation to what the climate of opinion around Facebook was at the time. Additionally, the focus will be on an explanation of the motivations and ideals of the founders of Diaspora*. An assessment will be given of how Diaspora* successfully tackles some of the Facebook issues elucidated in the previous chapter, and the ways in which it helps to preserve both institutional and social privacy. Finally, it will be shown where Diaspora* is unsuccessful in resolving these issues.

3.1. Diaspora*

The Diaspora* social network is fundamentally different from Facebook and most social networks that preceded it, because it is a distributed or federated social network. Distributed social networks are based on a decentralised network structure that allows users to the choose from a range of social network providers, in the same way one may choose an email service provider and still be able to communicate with those using different email service providers (Esguerra). On a centralised social network like Facebook, if a user wants to see another profile, the user sends a request to a central server. The server will then take the data from that profile (which is housed on the server) and then forward it to the user. In a distributed network, there is no central server, and communication occurs directly between users or between a number of different host servers (Zhao).

Before Diaspora* emerged there already existed other distributed social networks, and since Diaspora* started many more have emerged. Three predecessors to Diaspora* which

still exist currently are BuddyCloud, founded in 2007 (“ Company Information on BuddyCloud”); StatusNet founded in 2008 (Wauters), and OneSocialWeb founded in February 2010 (Krynsky). Although the coding languages, network architecture and protocols of each of these social networks are very different, all three offer federated social networks with privacy control features (“Comparison Distributed Social Networking”). Just after Diaspora* began acquiring funding, Friendica was established (Byfield). Friendica is currently still running, and has successfully established a number of features that Diaspora* aimed to achieve (including integration with Facebook, Twitter, Tumblr, StatusNet and even Diaspora* (Zhao),(“The Internet Is Our Social Network”)). The question as to why Diaspora* received the attention it did, when many working options already existed, will be answered by tracing its development. As will be discussed shortly, Diaspora* happened to arise at a propitious time with regard to Facebook’s privacy controversies. When the New York Times published a story about the project and its founders, Diaspora* “was introduced to the masses” (Wauters, “OneSocialWeb”). For these reasons, Diaspora* was chosen as the comparative social network for this paper.

A distributed network - and specifically Diaspora* - means that the network is not stored in one place (Grippi, Salzberg, Zhitomirskiy, Mei, et al., “Diaspora* Means a Brighter Future for All of Us”). The Diaspora* software was created to be installed and run on a user’s server/computer (referred to as a “pod”), thus allowing the user’s personal data to be stored on his/her own computer and under his/her control. The user is still able to interact with other users of the network in the same manner as on centralised networks like Facebook, the difference occurring in the backend communication protocols between pods.

Additionally, if a user does not have the capacity or skills to install the software on his/her computer and create his/her own pod, he/she has the option of joining one of many “community pods”. These are pods that are set up by individuals and have the capacity to

store many users' data. There are currently[34] 60 community pods, housed in many different countries, including the United States, Greece, Spain and France (Morley). Each pod can host a variable maximum number of users, with one pod hosting a maximum of 15 000 users (Bleicher). It is then the responsibility of the pod host to keep his/her server running and maintain software updates.

David Morley, one of the pod hosts, maintains a web page that lists all the available pods and provides statistics about the pods including pod location, user rating, and percentage of pod "uptime" (how often the servers have been reliably running). The Diaspora* founders hoped for pod hosts to start running their pods on different kinds of business models, creating a heterogeneous landscape of interlinked social networks (Bleicher 57). One pod host:

> could charge users US $5 per month to encrypt all their messages, while the host of My-seed.com could provide a free service using advertising as done on Facebook. diasp.org could extend invitations only to engineers, while Diaspora.lordgandalf.nl could offer a Lord of the Rings theme and games. But because all pods built using Diaspora's source code and standards speak the same language, users on different pods are still findable and approachable (Bleicher 57).

Another difference between Diaspora* and Facebook is the fact that Diaspora* is open source[35]. The project was open source from the start but primarily run by its founders. As of 27 August 2012, Diaspora* became an entirely community driven, open source project when its founders handed it over officially. The story of its development from May 2010 to August 2012 will follow.

---

[34] 29 November 2012

[35] Open source software is "software that is developed, tested, or improved through public collaboration and distributed with the idea that it must be shared with others, ensuring an open future collaboration" (Rouse, "What Is Open Source Software (OSS)? - Definition from WhatIs.com")

3.2. History

3.2.1. The Seed

Diaspora* was created after its four founders, Max Salzberg, Daniel Grippi, Ilya Zhitomirskiy, and Raphael Sofaer, were deeply inspired by a talk given by Eben Moglen in February 2010 (Liu). Eben Moglen is a Columbia Law School professor as well as the founder, director-counsel and chairman of the *Software Freedom Law Center* (Pinto). The talk Moglen gave at New York University was entitled “Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing” (Sevignani 600).

In this talk, Moglen spoke out directly against Mark Zuckerberg stating: “Mr Zuckerberg has attained an unenviable record. He has done more harm to the human race than anybody else his age" (Moglen). Moglen went on to criticise how the Web had changed from an open, distributed network into a restricted environment of surveillance, levelling some of the blame at Mark Zuckerberg, stating that “he turned it into a structure for degenerating the integrity of human personality, and he has to a remarkable extent succeeded with a very poor deal. Namely, ‘I will give you free Web hosting and some PHP doodads, and you get spying for free all the time’” (Moglen). Moglen warned that many of us are blindly sacrificing our privacy in exchange for the convenience of handing our information to centralised companies (Grippi, Zhitomirskiy, Salzberg, and Sofaer, “Kickstarter Pitch”).

He then raised the key question that mobilised the founders, as described in the Diaspora* blog: “why is centralization so much more convenient, even in an age where relatively powerful computers are ubiquitous? Why is there no good alternative to centralized services?” (Grippi, Zhitomirskiy, Salzberg, and Sofaer, “Kickstarter Pitch”). With the urgency emphasised by Moglen’s statement that “every day that goes by there’s more data inferences we can’t undo. Every day that goes by we pile up more stuff in the hands of the

people who got too much" - the four students realised that they had to "set out to fill the hole in our digital lives" (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "Kickstarter Pitch").

In addition to understanding the initial impulses behind Diaspora* it is essential to contextualise the environment at the time of Moglen's speech, specifically in relation to what was happening around Facebook. As mentioned in the previous chapter, after a series of privacy controversies and outcries, in December 2009 Facebook had made a privacy setting change which meant that a number of user details that were previously restricted by default were now public and available to search engines. As described previously, the outcry was large, resulting in the Electronic Privacy Information Center filing a complaint with the FTC (Schwartz).

Fuelled by the rising frustrations with Facebook and instigated by Moglen, the four students set out to create a better social network – "the privacy aware, personally controlled, do-it-all distributed open source social network" (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "Kickstarter Pitch").

3.2.2. Initial Ideals and Intentions

Salzberg, Grippi, Zhitomirskiy, and Sofaer decided to bring their plan to fruition and so posted a video pitch to the crowd sourcing funding website Kickstarter on 23 April 2010 (Bleicher 58). The intention here was to fund their "summer distraction" project (Liu). In this video and their subsequent blog posts, the students expressed their own frustrations with Facebook. In addition to their obvious discontent with the fact that Facebook owns all its users' data, they also expressed their aggravation with the fact that if users were dissatisfied with Facebook's privacy policy, they could delete their account but then would be cut off from interacting with the rest of their Facebook friends (Bleicher 57–58).

The nature of the distributed network not only meant that users could feel secure owning their personal data, but with community pods "as soon as it becomes public that a

company is exploiting the data of the users of its pod, they move away and the company is dead (in that sector). So the product shifts from you being the product to the software being the product" (" Client Side Encryption"). The founders additionally aimed for Diaspora* to perform like a social network aggregator so that "it would connect to every service you used to have for you. For example, your seed will keep pulling tweets and you will still be able to see your Facebook newsfeed " (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "A Little More About The Project"). This feature, the developers believed, would free users from being tied to one social network.

3.2.3. Public Reception

The Diaspora* team aimed to raise $10 000 in 39 days for the project they had planned to run over the course of the summer (Bleicher 59). In just the second week after the pitch had been posted, the project began to draw a large amount of attention and investment from top developers, famous open Internet advocates, and prominent technology investors (Weise). Al Gore phoned the team to commend their initiative and after just 12 days, the $10 000 target had been reached. The media attention followed with interviews with the *New York Times*, the *BBC*, and many technology magazines (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "A Little More Than 24 Hours Left!"). The *New York Times* piece ended up on the team's home page (Weise). The team blogged on May 31st:

> The sheer number of current supporters is unprecedented on Kickstarter, and we are thankful for every last backer. Together, we have struck a chord with the world and identified a problem, which needs to be solved (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "A Little More Than 24 Hours Left!").

The next day, the final day of the fund-raising, the project had garnered $200 641 from 6474 contributors. This was all before a "single line of code" had been written (Bleicher 59).

The public attention surrounding the project was inextricably linked to the battle it appeared to be waging against Facebook, and " 'Facebook Killer!' was the battle cry heard around the 'net, a real-life story of David versus Goliath" (Liu). Days before the Kickstarter pitch was launched, Facebook had just announced its introduction of the Social Plugin and Open Graph protocol that allowed websites across the Web to be integrated with Facebook, as mentioned in the previous chapter. Also, as described previously, this was not well received among many privacy advocates - the Electronic Privacy Information Center filed a second complaint with the FTC ("Social Networking Privacy"). Users were also "alarmed that it could track them beyond their personal pages" (Weise) resulting in a "Quit Facebook Day" initiative (Boyd and Hargittai).

With the pressure on the students to be privacy saviours, they realised they needed to get down to programming their solution. Sofaer's brother was a developer at a software consulting company, Pivotal Labs in San Francisco, and because of this connection, the CEO offered the team the company's office space. They began work there in June 2010 (Bleicher 59).

By 15 September the Diaspora* code was released to the public. The team posted their code to GitHub, the code-hosting website and used the Affero General Public License (APGL) to license their software. The APGL meant that the code was open for free use and modification, with any subsequent modifications to be released according to APGL too (Bleicher 59). The software interface resembled Facebook quite strongly: a user had a profile, and could make status updates, post photographs and interact with other users in the same way as on Facebook (Weise). The backend however, was very distinct. Because it was such a novel infrastructure and possibly because of the students' limited practical software development experience, the released code was riddled with bugs and security flaws (Liu). Developers who were previously big supporters of the project referred to it as "Swiss

cheese", an indication of the many apparent security holes (Pincus). Some of the flaws could have enabled accounts to be hijacked and users to be added as friends without their consent (Goodin). An owner and software developer of a top Japanese software company, stated that "the bottom line is currently there is nothing that you cannot do to someone's Diaspora* account, absolutely nothing" (qtd. in Goodin).

The students took these criticisms constructively and began fixing the mistakes and strengthening security (Pinto). At the same time they also started to incorporate new features such as Twitter Hashtags[36] and created their own pod "joindiaspora.com" (Weise).

In addition to improving the security and adding features from exisiting social networks, the students also focused on more ways to improve privacy features that were lacking in Facebook. In an August blog post, it became clear that the team were starting to focus on issues of social privacy, stating that they were aware of the need to allow "contextual sharing", which they described as an "intuitive way for users to decide, and not notice deciding, what content goes to their co-workers and what goes to their drinking buddies". They also acknowledged that it would be a challenging task to cater for in a user interface (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "An Overdue Update"). The solution to this problem came in the form of a feature called *Aspects*, similar to Facebook's then very underused and under-advertised Friends Lists feature. Aspects were described as "personal lists that let you group people according to the roles they play in your life" (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "Private Alpha Invites Going Out Today"). With any combination of Aspects (i.e. contact groups) a user can filter who he/she sees in his/her activity stream[37] and restrict the audience for posts. There is no limit to the number of Aspects a user may have and contacts can be assigned to multiple Aspects (Holloway). In late November these features along with the security fixes were released (Pinto). This release was

[36] Hashtags are tags that provide categories for posts on Twitter (Rouse, "What Is Hashtag?")
[37] The Diaspora* equivalent of the Facebook News Feed (described in Chapter Two, History Section)

far better received and soon Diaspora* had about 600 000 users, although consisting mainly of "distrustful techies and Europeans" (Weise).

The introduction of Aspects became a fundamental feature in the step towards a better, more privacy conscious social network. This became evident in June 2011 when Google released Google Plus, its attempt at gaining ground in the social networking realm (Halliday). As Liu astutely observes: "Google could still put ads in front of more people than Facebook, but Facebook knows so much more about those people. Advertisers and publishers cherish this kind of personal information". One of the key features Google Plus promoted were *Circles*, which were very much the same as Diaspora*'s Aspects. Facebook also appeared to respond to the introduction of these features by attempting to improve the original underused and little known Friends Lists feature in September, as described in the previous chapter. In the Diaspora* blog the team responded to these occurrences, expressing their pride that Google had copied their Aspects feature and acknowledging that Facebook was finally "moving in the right direction with user control over privacy"; attributing Facebook's move as a response to Google Plus and the growing support for Diaspora* (Grippi, Zhitomirskiy, Salzberg, Mei, et al.). Google claims that its ideas preceded Diaspora* (Weise) but whether this was true became somewhat irrelevant in light of the failure of Google Plus to attract a significant number of users. In February 2012, Google Plus only managed to draw users onto its network for an average of 3 minutes over the whole the month of January, compared to 7.5 hours for Facebook users (Winter). This indicated to the Diaspora* team how powerful the "inertia" of Facebook users would be (Weise).

Outwardly however, the team seemed to still be focused and idealistic about making a distinct change to the online privacy environment. In a blog post, the team announced that they had agreed to abide by the Computers, Freedom, and Privacy's Social Network Users' Bill of Rights that had been adopted at the 2010 conference. The conference was the

twentieth annual CFP conference and was held at San Jose State University ("Main Page - CFPWiki"). The CFP "is the leading policy conference exploring the impact of the Internet, computers and communications technologies on society" ("Main Page - CFPWiki"). The Diaspora* post listed the Bill as follows:

1. Honesty: We will honor our privacy policy and terms of service.
2. Clarity: We will make sure that our policies, terms of service, and settings are easy to find and understand.
3. Freedom of speech: We will not delete or modify user data without a clear policy and justification.
4. Empowerment: We will support assistive technologies and universal accessibility.
5. Self-protection: We will support privacy-enhancing technologies.
6. Data minimization: We will minimize the information users are required to provide and share with others.
7. Control: We will work toward enabling users to own and control their data and won't facilitate sharing their data unless they agree first.
8. Predictability: We will obtain the prior consent of users before significantly changing who can see their data.
9. Data portability: We will make it easy for users to obtain a copy of their data.
10. Protection: We will treat user data as securely as our own confidential data unless they choose to share these data, and notify them if these data are compromised.
11. Right to know: We will show users how we are using their data and allow them to see who and what has access to their data.
12. Right to self-define: We will allow users to create more than one identity and use pseudonyms. We will not link them without their permission.
13. Right to appeal: We will allow users to appeal punitive actions.
14. Right to withdraw: We will allow users to delete their accounts and remove their data.

This list, however, was immediately followed by somewhat of a disclaimer, stating that the Diaspora* adoption of the Bill was "aspirational", explaining that they "aspire to have the required functionality in place soon [in order to] enforce all these rights, and to this end, we'll use the aforementioned principles to guide our product development from this day forward"

(Grippi, Zhitomirskiy, and Salzberg). Most of this list is relevant to institutional privacy as defined in Chapter One, however the "Right to self-define" is relevant to social privacy as with the allowance of multiple unlinked identities (something that is not allowed on Facebook as mentioned in Chapter Two), one can separate social contexts thoroughly. This will be explained further shortly.

By September 2011, the Kickstarter fund money had run out and Sofaer decided to return to school in New York (Liu). Shortly thereafter, Yosem Companys, who had been brought on a few months earlier as president of the Diaspora* foundation to help guide the development of the project, left abruptly due to "internal strife" (Liu). A release that was due for November was unexpectedly called off a few weeks before it was due as the remaining team did not feel ready for the release (Weise). Many were starting to question the future of the project, and the doubt became evident with the waning of funds and with the *Wall Street Journal* article entitled "Whatever Happened to Diaspora* The Facebook Killer" published on 7 November (Liu). The Diaspora* team received one more devastating blow when, on 11 November , Ilya Zhitomirskiy committed suicide (Pinto). There was subsequently a fair amount of speculation in the media, questioning whether the stresses of the project difficulties, and the high expectations for the four founders led to Zhitomirskiy's suicide (Chen), with Zhitomirskiy's mother stating that "I strongly believe that if Ilya did not start this project and stayed in school, he would be well and alive today" (Weise).

Grippi and Salzberg took a break in December but returned in January 2012 with a new desire to keep on with the project. Dennis Collinson (previously a software engineer at the software company Pivotal Labs) and Rosanna Yau (a graphic and interaction designer) joined the project as head of engineering and user experience designer respectively (Weise). In June 2012 Diaspora* moved to Y-Combinator, the "start-up accelerator", to participate in

their three month program that had successfully guided many previous start-ups (Dropbox, Scribd) (Weise).

Unfortunately, Y-Combinator was not as successful with Diaspora* and on 27 August, Grippi and Salzberg announced that they would be stepping down from running the project and "giving control of Diaspora* to the community" (Grippi and Salzberg). They insisted that they would still play a significant role in the Diaspora* community. In their blog announcement, the two stated that:

> Today, the network has grown into thousands of people using our software in hundreds of installations across the web. There are hundreds of pods that have been created by community members, and it has become one of the biggest GitHub projects to date. It has been translated to almost fifty languages, with hundreds of developers worldwide contributing back to the project.

The move to community governance did not, in fact, mean an end to the social network. Sean Tilley worked closely with the founders before the handover and is now one of the primary people controlling the community project. The project has successfully released the next version of the code. This is the version that was previously intended for the November 2011 release and which was called off. In a blog post from the 29 October, it is clear that community members are still working on the code. The blog post makes specific mention of many other existing decentralised social networks, listing: Libertree, TentStatus, BuddyCloud, Friendica, StatusNet, and MediaGoblin[38], and additionally discusses plans to make Diaspora* capable of interacting with these social networks (Tilley).

3.3. Privacy Policy

The privacy policy of joindiaspora.com (the pod created by the Diaspora* team themselves) is still in development (Grippi and Salzberg, "Diaspora* Is Back in Action").

[38] Libertree, TentStatus and MediaGoblin emerged after *Diaspora**.

However, the diasp.org is one of the most popular and longest running pods and does have a privacy policy, so this will be analysed. Once signed up to this pod, a link to its privacy policy is provided. The policy is a refreshing 800 words long, about a tenth of Facebook's Data Use Policy, and like Facebook's policy is written in an informal tone and without complicated legal terms. The policy first describes what information the pod collects, which is detailed to be information required for registration purposes. The uses of the information are listed: "to personalize your experience"; "to improve our website"; "to improve customer service"; "A 3rd party vendor is used for support tickets, when submitting a support ticket you are sharing the information you supply and your Browser/IP data" (the vendor's name is listed along with a link to their privacy policy); "to process transactions"; "to administer a contest, promotion, survey or other site feature"; "to send periodic emails" ("Disap.org Privacy Policy"). It is then asserted that both public and private information "will not be sold, exchanged, transferred, or given to any other company for any reason whatsoever, without your consent, other than for the express purpose of delivering the purchased product or service requested".

The policy then explains what security measures are in place to keep data safe. It is stated that a number of measures are taken and additionally states that the pod server remains in a safe place and that SSH access restriction[39] with RSA keys[40] is implemented. This section also asserts that all data is transferred via Secure Socket Layer[41] (SSL) technology.

An explanation of cookies is given and it is confirmed that the pod uses cookies to keep track of user preferences and to gather website traffic data in order to "offer better site experiences and tools in the future".

---

[39] Secure Shell (SSH) is an "interface and protocol for securely getting access to a remote computer" (Rouse, "What Is Secure Shell (SSH)? - Definition from WhatIs.com").
[40] Rivest-Shamir-Adleman (RSA) is an "Internet encryption authentication system" (Rouse, "What Is RSA Algorithm (Rivest-Shamir-Adleman)? - Definition from WhatIs.com")
[41] Secure Socket Layer (SSL) is a protocol for securing the transmission of messages on the Internet (Rouse, "What Is Secure Sockets Layer (SSL)? - Definition from WhatIs.com")

The next section deals with information disclosure to third parties. It is asserted again that “personally identifiable information” is not sold, traded or transferred to third parties. Outside companies are, however, used to provide data statistics and to measure site performance. These parties use “non-personally-identifying information”, that are commonly available with web browsers and servers. Some of the data that is included is listed (“browser type, language preference, referring site, and the date and time of each visitor request”). The data is collected in order to provide insight into visitor use of the pod. It is stated that third party companies comply with the diasp.org privacy policy. The name of the third party company in use is listed and a link to its privacy policy is provided. Data may be transferred if needed to “comply with the law or valid court order, enforce our site policies, or protect ours or others rights, property, or safety”.

The policy then goes on to explain that links to outside party products or services may be provided on the diasp.org website but that diasp.org will not be held liable for the policies or activities of these sites but does “seek to protect the integrity” of its site.

Lastly, any changes to the privacy policy will be posted on the privacy policy page. The last modification date of the policy is provided (25 November 2011).

3.4. Analysis

3.4.1. Successful Solutions

Now that an overview of how Diaspora* works, its features and its founders’ intentions has been provided, an assessment of whether Diaspora* successfully offers a privacy improved alternative to Facebook can be given. The most obvious and primary feature that Diaspora* boasts is the ability for its users to own their own data. If a user hosts his/her own data then none of the requirements established for institutional privacy are even needed. However, most current users of Diaspora* do not house their own data and instead choose to store their data on one of the community pods. The assumption here is that with

regular updates on the pod listing website, a reliable and transparent insight into the trustworthiness of pod hosts will be provided. In this case, however, the user would need to rely on the privacy policy of his/her selected pod.

In the case of the diasp.org privacy policy, the collection and use of users' personal data is simply and clearly explained and the safety of data is assured. These are three key aspects of the institutional privacy requirements: "Openness", "Purpose Specification", and "Security Safeguards". A fundamental aspect of Diaspora* that is clear in this policy is the fact that user data is not exploited for advertising purposes and so defaults do not need to encourage information revelation as on Facebook.

Although not mentioned in the policy, one of the features of Diaspora* software and therefore universal to all pods, is the ability to download and/or export all personal data from one pod to another. This feature fulfils the "Data Subject Participation" feature by allowing users full access to and even ownership of their data. The feature appears prominently at the bottom of a user's Account Settings page as shown in the image below:

Figure 4: Diaspora* Data Portability

This portability feature in the context of the decentralised network structure empowers the user by making pods, and eventually other social networks, accountable for the way in which they treat their users and their users' data, as explained by the Diaspora* team themselves:

> And because your information is yours, not ours, you'll have the ultimate power — the ability to move your profile and all your social data from one

> pod to another, without sacrificing your connection to the social web. Over time, this will bring an end to the indifferent, self-serving behavior that people can't stand from the walled gardens that dominate social networking today. When you can vote with your feet for the environment where you feel safest, the big guys will have to shape up, or risk losing you (Grippi, Salzberg, Zhitomirskiy, Mei, et al., "Diaspora* Means a Brighter Future for All of Us").

The levelling of power that portability produces, is extended further by the fact that Diaspora* has been created to perform like a social network aggregator. At the moment Diaspora* integrates with Tumblr, Twitter and Facebook, allowing a Diaspora* user to post to them, and plans eventually to have functionality that allows feeds from these services to be pulled too (Grippi, Salzberg, Zhitomirskiy, Mei, et al., "Diaspora* Means a Brighter Future for All of Us").

So far the ways in which Diaspora* offers a reasonable way to uphold key aspects of institutional privacy have been shown. Diaspora* has however, also managed in some ways to help maintain better social privacy. The Aspects feature helps to provide this. As explained earlier, like Facebook's Friends Lists feature, this allows for the separation of social contexts, and as illustrated in Chapter One, this is an essential aspect of social privacy. Diaspora* appears to be more successful in the implementation of Aspects than Facebook is with its lists, as it has advertised prominently from the start that they are to be used as a way to contextually share information. As soon as a user starts adding friends, categorising can begin.

In addition to Aspects, Diaspora* offers another fundamental feature that assists contextual information disclosure by allowing multiple user accounts. A user may also create pseudonymous accounts, none of which have to be linked. As shown in the previous chapter, Facebook strictly forces users to have only one account and an account that is consistent with

all of their real life personal details. With Diaspora*, one can have an account that is relevant to one's work life only and another for one's social life. With accounts separated in this manner, there is far less risk of issues such as one's employer seeing a compromising photograph. As the team blogged, pseudonyms allow "you [to] express yourself candidly, and be your authentic self...and this both protects you (if you want to say something your boss or your parents disagree with)" (Grippi, Salzberg, Zhitomirskiy, Mei, et al., "Diaspora* Means a Brighter Future for All of Us"). The "authentic self" being in stark contrast to the authenticity that Zuckerberg appears to push for with his "one identity" statements.

3.4.2. Shortfalls

Although Diaspora* has achieved a lot in its attempt at creating an improved privacy social network, it is certainly not a perfect one. One of the biggest problems with Diaspora*, as the failure of Google Plus indicated, is the fact that Facebook has achieved such a monopoly that luring people away from it is a difficult task. This means that if a user does decide to opt for Diaspora*, his/her experience of it will be limited by the likelihood that few of his/her friends will be on the network. The intentions of the Diaspora* project were such that it would eventually allow users to still connect with their Facebook friends but currently this has not been implemented (although as mentioned, one can update one's status on Diaspora* and have it update Facebook at the same time). As acknowledged by the team, because users on Diaspora* usually did not have many of their Facebook or real life friends connected, Diaspora* became a way to socialise with strangers. The team state that:

> The interactions on other networks are built around the assumption that you are addressing people you actually know – your 'friends'... Something entirely different is happening on Diaspora*... A diverse, international community of people meeting and discussing all sorts of things needs to be thought about differently (Grippi, Mei, Tilley, Yau, et al., "DIASPORA* Grows Up.").

The danger of invisible audiences described in the previous chapter seems to be very likely in this situation. Although one could possibly assume that people who are on Diaspora* currently are privacy conscious, it may certainly not be the case that every user of Diaspora* has equal expectations when it comes to privacy. Thus the collapsing of contexts that occurs as a result of the potentially limitless number of audiences for disclosures (that are exacerbated by the digital age of "persistence, replicability, scalability, searchability", as described in Chapter Two) may be even more frequent on Diaspora*.

Even with the case of audiences consisting of trusted real life friends, technological infrastructure (in this case the decentralisation) and interface design (for example the Aspects feature) cannot solve all the kinds of social privacy invasion problems that online interaction and information disclosure on social networks can cause. As acknowledged in the previous chapter, there is a limit to the kind of nuanced granularity that can be achieved with Aspects, as real life human relationships are intricate and diverse and fluctuate over time. This is something the Diaspora* team were aware of from the start when they first released their code to the public. As they stated in their Developer Release, the team realised that:

> Technology wouldn't be enough. Even the most powerful, granular set of dropdowns and checkboxes will never give people control over where their content is going, let alone give them ownership of their digital self (Grippi, Zhitomirskiy, Salzberg, and Sofaer, "Developer Release").

In addition, on Diaspora*, as on Facebook, it is difficult for a user to control what his/her friends disclose or spread about him/her. It is important to realise that there are certain privacy diminishing characteristics of online social networking that cannot be solved with technical controls or infrastructure alone.

Institutional privacy may not either be fully conserved in the current state of Diaspora* because there are also risks in allowing anyone (e.g. people inexperienced with

storing large amounts of user data, or without the financial capacity to do so) to host a pod. Aside from the podupti.me website, where reviews and performance details are provided for each pod, there is currently no initial or further due diligence performed as to the intentions and abilities a particular user may have for hosting a pod. It is true that accountability may rise with users' easy ability to leave a pod if dissatisfied, but currently all pods run for free so there is not much incentive for a host to keep users data strictly safe. Additionally, there is no easy access to view each of the pod's privacy policies on the podupti.me website. In order to view diasp.org's privacy policy, one needs to create an account with the pod first. Furthermore, the fact that inexperienced pod hosts may be creating their own privacy policies may also mean that the quality of such policies cannot be guaranteed.

The alternative of signing up to a pod is of course the option of configuring one's own computer to be the host. Unfortunately, despite plans to make this simple for users, it is currently extremely complicated. Before one can even start installing the Diaspora* software there is a long list of other applications and services that need to be installed (a total of 11) and then the instructions for the installation that follow are about four pages and 1598 words long ("Notes on Installing"). The advantages for institutional privacy specifically would be significant if this process was made simpler.

Although the portability feature offers many advantages with regard to data ownership and empowerment, complications may arise as Grimmelmann points out, "if you and I are contacts, is that fact your personal information or mine? Giving me the "ownership" to take what I know about you with me to another site violates your privacy" (1193). When the data that is generated on social networks is as a result of interactions and relationships with other people, determining strict lines between data ownership boundaries may not be a simple process. As Grimmelmann asserts further "thus, while data portability may reduce vertical power imbalances between users and social network site, it creates horizontal privacy

trouble" (1193). Furthermore, if data is continuously moved from site to site, it may also become less secure.

Perhaps one of the primary shortfalls of Diaspora* was the failure of its founders to provide a robust solution to the issue of sustaining a social network service that is both free and does not mine its users' data. For this reason, it makes sense for Diaspora* to run as a community project, but it still does not completely solve the issue of sustainability for current pod hosts. As more pod hosts emerge and/or if the hosting process is made simpler, the load of users could be spread sufficiently to allow for services to remain free for users and cheap to run for hosts.

Unfortunately, many saw the stepping down of the founders from the Diaspora* project as an admission of the failure of the entire project. It is true that many grand claims were made and aspirations pronounced at the start of the Diaspora* project both by the founders themselves as well as the initial public support, and that many expectations were not met. However, this enthusiastic reception does highlight the strongly felt need for this kind of service. Furthermore, this chapter has shown that Diaspora* successfully introduced and extended worthy solutions to the problems of both institutional and social privacy. The developments of the community coding contributions have been promising only three months down the line, so there may be a lot more to come from Diaspora*. If the integration of Diaspora* with all existing social networks is solved and the complexities of individual software installation is simplified as planned in the community blogs, Diaspora* may step even closer to being a robust and popular solution. Additionally, if integration is achieved, it may be the case that distributed social networks will:

> Take over slowly, like ivy enveloping the brick halls of Harvard University. At first, open-source projects such as Diaspora* will grow steadily and

> haphazardly, all the while tweaking their technologies, working out standards, and syncing with each other (Bleicher 82).

The fact that many distributed networks are currently running is a promising indication that soon there may exist a diverse, heterogeneous and equal social networking landscape in which all network owners are more accountable to their users, and where most networks facilitate both social and institutional privacy with their settings and controls.

Chapter Four

This chapter presents a summary of the conclusions from the previous chapters. Recommendations for further solutions to privacy issues occurring on social networks, which were not successfully accounted for by either Facebook or Diaspora*, will be made. Finally, suggestions for future avenues of research in this realm will be provided.

4.1. Social Network Privacy

Two conceptions of privacy (social privacy and institutional privacy) relevant to the context of online social networks were developed, primarily employing Helen Nissenbaum's proposed framework of contextual integrity.

Social privacy is the term used to capture the kinds of violations that occur as a result of users disclosing information about themselves on social networks and others further disclosing their information. The development of a conception of social privacy, as supported by contextual integrity, was fundamentally based on the importance of upholding expectations of the context in which information revelation occurs. When violations of social privacy occur on Facebook, it is as a result of the collision of contexts that cause such indignation and criticism. Social networks are fundamentally an extension of real-world interactions and, specifically on Facebook, occur primarily between real-world friends and acquaintances. Despite Zuckerberg's claims of privacy norms changing in ways that indicate people want to reveal more personal information, this report has shown that people still in fact, have the same expectations for privacy on social networks as they do in the real world. These expectations explain the outcries that have occurred as a result of various changes in Facebook's privacy policy. This indignation perhaps was most overtly seen through the substantial publicity of Diaspora* and its subsequent branding as the "Facebook Killer" or the "Anti-Facebook", as described in Chapter Three. For social privacy to be maintained, a

social network needs to preserve an appropriate separation between the rich diversity of social contexts.

The institutional privacy definition was used to deal with the kinds of issues arising from the harvesting of users' personal data by Facebook and its exploitation of that data for commercial purposes. In accordance with contextual integrity, this definition was developed using a legal conception of fair information practices. The requirements therefore needed to uphold institutional privacy were based on South Africa's soon to be enacted Protection of Personal Information Bill. The principles in the Bill are based on well accepted practices developed around the world and are:

- "Accountability"- which concerns the responsibility of institutions for compliance with the Bill
- "Processing Limitation"- which ensures information is processed fairly and lawfully
- "Purpose Specification"- which limits the scope of the uses to which information may be put by an organisation
- "Further Processing Limitation"- which limits the use of information to those initially identified (which need to be defined specifically and explicitly) and for which consumers have given consent
- "Information Quality"- which ensures institutions preserve the quality of information
- "Openness"-which asserts that information processing practises are to be transparent
- "Security Safeguards"- which means institutions are to ensure information is safe from "risk of loss, unauthorised access, interference, modification, destruction or disclosure"
- "Data Subject Participation"- which ensures individuals should be allowed to correct or remove any incorrect or obsolete information (Badat).

4.2. Facebook

Chapter Two endeavoured to apply the conceptions of privacy to Facebook to assess how Facebook enables violations of both social and institutional privacy, and to what extent Facebook can be held accountable for these actions. This was performed firstly by tracing the development of Facebook over the last decade, while trying to pinpoint Mark Zuckerberg's intentions, and secondly, by analysing Facebook's Data Use Policy and its technical privacy control features. From this critical analysis, it was concluded that Facebook violates social privacy by collapsing and colliding contexts in the following ways:

- Social networks lack the physical and architectural constraints that exist in the offline world that allow for revelations made in public to remain discreet and for contexts to be separated. With the introduction of News Feed, Facebook created a further merging of contexts so that information revelation that used to be "private-by-default" became "private-through-effort".
- Four fundamental features of the online realm and inherent in Facebook (persistence, replicability, scalability, searchability), enable "invisible audiences". This implies that, because the number of potential future audiences for a piece of disclosed information may be boundless, contexts once again may collide.
- Social contexts converge as a result of the common lack of divisions within a user's Facebook friends collection, which additionally often consists of many "weak ties" (casual acquaintances). Although Facebook does currently offer the Friends Lists as a way to limit information disclosure to particular audiences, it does not advertise this feature sufficiently as a tool for maintaining privacy. Furthermore, the fact that Facebook insists that users each have one account in accordance with their real life identities, limits users' ability to interact contextually. In light of Zuckerberg's insistence that the world

should be more open and transparent and his repeated assertion that having more than one identity is deceitful, this social convergence appears to be intentional.

- Violations often occur on Facebook as result of the disparity between a user's privacy expectations and those of his/her friends. Because on social networks one has little control over how one's friends choose to disclose information, this disparity is especially problematic.
- Finally, contexts have converged on Facebook, as a result of the numerous fundamental structural changes it has made over the years, from the introduction of features such as News Feed to its significant transformation from an enclosed Harvard network to a worldwide open network.

This kind of instability due to continual changes is problematic for institutional privacy too because of the risk to data safety it may cause. For example, Facebook also adds in its policy that it cannot make "guarantees about any part of our services or products" (which violates "Security Safeguards"). Instability also means that the initial data use agreed to by users has changed numerous times over the years, with data now being used for commercial purposes, and spread to many third parties (which violates "Further Processing Limitation"). Furthermore, the Data Use Policy does not make it clear exactly which changes users will be explicitly notified of, and this also violates the "Further Processing Limitation" requirement, which asserts the need for explicit notice and consent for any changes.

Both institutional and social privacy suffer as a result of Facebook's complicated, excessively long and vague privacy policy, which leaves users unaware and confused as to the extent of their exposure to both Facebook and the rest of the Web. In terms of institutional privacy, it could be said that the "Openness" requirement is violated by this lack of transparency.

The Data Use Policy also reveals the large amount of user information to which Facebook has access. The range of types of data is wide and may in fact be problematic in term of the "Purpose Specification" requirement, which aims to restrict the scope a company may have to utilize personal data. Furthermore, the fact that the data is centralised on Facebook servers may be problematic for security reasons and also because it may increase the potential for abuse by both Facebook and government or law enforcement.

Due to the fact that Facebook owns and stores all its user data, the requirement of "Data Subject Participation" should be thoroughly maintained. However, it was shown that because of the data leakage to all the third party websites and applications with which Facebook integrates, the task of deleting data is challenging and tedious. Furthermore, users have no control over the data that their friends may have disclosed. The Data Use Policy also reveals that a user may access "most" of his/her data, but it is not at all clear what this covers.

The most fundamental privacy violation, for which Facebook can be held directly accountable, despite its claims to improve its privacy policy and controls, is the state of its default settings. As shown in Chapter Three, the power of the default is such that it can directly influence people's behaviour. Documented research has shown that people will often allow a choice (including critical life decisions such as organ donation) to be made on their behalf, by trusting the default option. In the case of Facebook, this technique specifically encourages more information disclosure, as the default settings are such that disclosures are always open to the public. Zuckerberg claims that such increased information revelation is due to shifting norms but at the same time, he is also seemingly fanatical about fulfilling his vision of an open and transparent society, and therefore in fact pushes for a change in norms. As explained in Chapter Two, it is not clear whether Zuckerberg is motivated by commercial gain as much as by his obsession with transparency, as it appears that this zealotry is genuine. In light of Sandberg's belief that Zuckerberg provides privacy controls as a "means to an

end" (qtd. in Kirkpatrick 195), and the additional advertising pay-off that Facebook receives as a result of increased disclosures (and for which Sandberg was specifically hired), this report concludes that these default settings are definitely intentional, as are many of the structural changes introduced over the years that have caused numerous forms of context convergence.

4.3. Diaspora*

In contrast to Facebook's commercial exploitation and ownership of user data, Diaspora* emerged. Chapter Three assessed Diaspora*'s solution to the violations occurring on Facebook. This was done by tracing the history of Diaspora*, focusing on the founders' motivations and inspirations and by assessing the features that Diaspora* offers specifically to improve both social and institutional privacy. In addition to what Diaspora* offers in terms of an alternative to Facebook, it is imperative to acknowledge the media popularity and support it garnered as the "Anti-Facebook", indicating a significant discontent with the state of Facebook at the time, and again reinforcing that people do in fact care about privacy.

It was shown that Diaspora*'s primary decentralised feature solves most of the requirements needed to uphold institutional privacy, as a result of the ownership and control of data it allows. This is most true in the case of users running their own pods. Because of the data portability that Diaspora* facilitates, this may also be true to some extent in the case of users signing up to other pods as users can easily access, delete and correct all of their data, thus fulfilling the "Data Subject Participation" requirement. Because Diaspora* aims to integrate seamlessly with other social networks, it also extends its distributed model outside of its own network, thus reducing the monopoly a particular social network may have.

Diaspora* solves some social privacy issues as well through its proactive advertising of its Aspects feature to allow for contextual information disclosure, and through its allowance of multiple pseudonymous accounts per user. Allowing multiple accounts

acknowledges that users should legitimately have many different facets to their identity, and should be allowed to compartmentalise these facets. Furthermore, the problem of excessive self-disclosure of information is less likely to occur on Diaspora*, as a result of its default settings that assume that information is to be restricted.

Chapter Three also revealed the ways in which Diaspora* does not solve issues of social and institutional privacy successfully. It was pointed out that the danger of invisible audiences on Facebook is still an issue with Diaspora*. This danger may be made even worse on Diaspora* as, according to the Diaspora* team themselves, many users have connected to strangers across the world. In addition, as on Facebook, there is the high risk that a user's expectations of privacy may not match those of his/her friends, and there is still nothing allowing a user control of what information his/her friend discloses about him/her or from stopping a friend from copying and disseminating his/her information. Furthermore, there is a limit to the extent to which technical controls like Aspects (and Friends Lists on Facebook) can represent the rich social relationships that exist in real life.

In terms of institutional privacy, Diaspora*'s current distributed model can be problematic in light of the risks of allowing anyone to host a pod. There is no concrete assurance that a pod host has enough experience or capacity to keep information secure. With the current inaccessibility to each host's privacy policy and the lack of monetary incentive for hosting a pod, there is not much assurance with regard to a host's intentions either. This however, could be avoided if the current complexities of hosting one's own pod are simplified.

Additionally, although the portability feature is useful, it may also cause complications in determining exactly what data belongs to a user and what data belongs to his/her friends, when most of social network data is generated by interactions and relationships (i.e. data that is shared between users). The "Security Safeguards" requirement

may also be at risk as a result of data constantly being moved from pod to pod, as portability allows.

The difficult challenge of competing against Facebook was emphasised by the failure of Google Plus, which drew users for an average of 3 minutes over the whole of the month of January, compared to 7.5 hours for Facebook users (Winter) – a clear indicator of the strong pull that Facebook has acquired with its users. This issue could be solved by Diaspora*'s plans to integrate completely with all social networks. The fact that Diaspora* is now a community run project means that it can now run for free without having to sustain the Diaspora* founders, as all further developmental work is volunteered by a fairly large community of developers. As long as enough pod hosts emerge and/or individual pod hosting is made simpler to spread the load of users sufficiently, Diaspora* could remain a free service that does not need to mine its users' data or push for more privacy violating disclosures to sustain itself. This paper has shown that Diaspora* successfully introduced and extended some solutions to both institutional and social privacy, and very importantly brought the concept of an alternative distributed social network to more people's attention than the other distributed social networks that preceded it. If Diaspora* fulfils its plans to fully integrate with all social networks, there may soon exist a more level playing field for users to chose from, and one that does not need to conflict with a single man's fanaticism or a single company's commercial interests.

4.4. Further Solutions for Maintaining Privacy

As indicated above, there are still outstanding privacy issues despite the improvements that Diaspora* brings. As stated in Chapter One, in America the FTC's Fair Information Practices principles, which guide institutional privacy, are currently only guidelines in America and not enforceable by law. In South Africa, the case is the same for fair data practice guidelines as the Protection of Personal Information Bill has not yet been

enacted. For American users of Facebook, this means that Facebook is often not held accountable for its data practises. The data of users outside of America and Canada (which obviously includes South African users) is controlled by Facebook Ireland Ltd. ("Data Use Policy"). Because Ireland is part of the European Union, these data practices are regulated by the EU Data Protection Directive ("Legal Procedure Against 'Facebook Ireland Limited'"), which, as stated in Chapter One, enforces principles very similar to those of the South African Protection of Personal Information Bill. These principles are enforced by EU law, so technically users in these countries (which include South Africans) have better means to hold Facebook accountable. However, as the organisation "Europe vs. Facebook" has made clear, there are still a number of violations to the Data Protection Directive that Facebook is committing ("Legal Procedure Against 'Facebook Ireland Limited'"). "Europe vs. Facebook" has filed several complaints with the Irish Data Protection Commissioner over the years, some of which have resulted in audits by the Commissioner who then requested a number of Facebook changes (Tate). Without the protestations of this organisation however, Facebook may have continued not to be held accountable for its practices despite the EU regulations. Therefore, I believe that for institutional privacy to be improved on social networks, data protection regulations need to be enforced more strictly, and by the law.

However, the law could be used successfully to tackle social privacy issues on social networks as well. For example, if someone disseminates information that another user disclosed to a specific Facebook audience, that person should be held liable. Furthermore, as Solove asserts, and as pointed out in Chapter One, if someone discloses personal information about another user that is of no use to public interest, that person should be held accountable by the law in the same manner that defamation law holds people accountable. Solove also points out that in America, employers are legally obligated to reveal to job applicants if any information resulting from a credit reporting check (via credit agencies) directly influences

the applicants employment chances. This law is in place so that a job candidate may be able to explain any inaccurate or incomplete facts. The same law could be extended to the increasingly common practice of employers conducting informal background checks by looking at candidates' Facebook profiles (Solove, *The Future* 203).

Although the law may control the use that others make of personal information, one could argue that it cannot directly limit the extent of information a user reveals about him/herself. However, the law could enforce the settings of social networks so that (as on Diaspora*) the default setting restricts publication to the most limited audience, and information disclosure to third parties (for example Facebook's third party apps, Social Plugin etc) are "opt-in" as opposed to "opt-out".

Another solution to this issue of self-disclosure, as proposed in most of the research, is education, and particularly education directed at teenagers who have been shown to reveal more information than most other age groups. Grimmelmann stresses that "targeted efforts to explain a few key facts about social-network-site privacy in culturally appropriate ways could help head off some of the more common privacy goofs users make" (1141–1142). Perhaps schools could run informal workshops, explaining how to successfully employ the various controls Facebook currently offers. These workshops could also provide some of the many examples of cases where self-disclosure resulted in dire consequences as discussed in Chapter One.

As elucidated earlier, both Facebook and Diaspora* suffer from the issue of invisible audiences. No matter how many technical controls such as Aspects and Friends Lists are available or how concise and clear a privacy policy may be, a social network needs to provide privacy both through its interface controls as well as through its environment. In addition to employing appropriate defaults as a way to improve this, a social network can do a lot more in terms of the feedback it provides to its users. For example, Danah Boyd suggests that when

a user posts a photo on Facebook, while selecting a specific audience, the user could be given the option of directly viewing a list of all the people contained in that audience. She states that:

> When I post a photo in my album, let me see a list of EVERYONE who can view that photo. When I look at a photo on someone's profile, let me see everyone else who can view that photo before I go to write a comment. You don't get people to understand the scale of visibility by tweeting a few privacy settings every few months and having no idea what "Friends of Friends" actually means (Boyd, "Putting Privacy Settings").

Peterson points out that feedback could also be provided by allowing users to see who has viewed their various disclosures (35). This feature is and was present on a number of social networks already including Friendster and LinkedIn. However, this feature could then paradoxically conflict with the privacy Facebook currently does afford to a user's browsing of other profiles. This clash of privacy rights highlights the complexities of maintaining privacy on social networks. As indicated, the primary feature of social networks is to facilitate interactions between people, and as indicated on both Facebook and Diaspora* these interactions occur between many users around the world. Satisfying all expectations for privacy is a difficult and intricate endeavour.

4.5. Further Research

4.5.1. Other Distributed Networks

This paper was limited to the analysis of only Diaspora* as an alternative to Facebook. It was chosen particularly because of the publicity it received and because it emerged at a time in Facebook's history that was especially controversial in terms of privacy issues. However, as indicated in Chapter Three, there are currently a number of other social networks that are also based on the distributed model. Further research analysing these social

networks, and a comparison between these networks and Diaspora* to determine if they offer an even more successful solution to Facebook would be of benefit.

4.5.2. Further Facebook Changes

Due to Facebook's rapidly changing state, the investigation of Facebook was limited to extend no further than June 2012. Further research could take into account the subsequent changes. Most notably since June 2012, Facebook acquired facial recognition technology, that allowed it to recognise users from uploaded photographs that had not yet been tagged, and then suggest tags for these photographs (Sengupta and O'Brien). Soon after this feature was instituted, as part of an investigation into Facebook's data practices, the European Data Protection Commissioner (DPC) based in Ireland, recommended that Facebook disable this feature (Lunden). Facebook subsequently disabled the feature but stated that it would bring it back for Europeans on terms the DPC agrees with and did not state on what conditions it will restore the feature for America and Canada (Sengupta and O'Brien). Another significant change for Facebook is the further alteration it has made to its Data Use Policy, the most significant of which is the retraction of users' ability to vote on new changes in the future (Kerr). This has once again raised concern among advocacy groups such as the Electronic Privacy Information Center. Facebook has also added some new controls that could improve social privacy, such as the ability for a user to request other users to remove photographs of him/herself but at the same time, Facebook once again removed existing controls that helped maintain privacy (such as the control that stops other users searching a user on Facebook) (Taylor). Now almost a decade since Facebook's inception, these changes appear to continue to follow the same general pattern observed in Chapter Two – a pattern of introducing some privacy controls, while at the same time also introducing often radical changes that lead users to reveal more information at the cost of privacy. As already discussed, this again appears to

confirm Sandberg's view that Zuckerberg provides some privacy controls as a temporary measure towards his long term goal of "radical transparency".

4.5.3. Google

In terms of the investigation of online violations of privacy, the practices of Google also demand a thorough critical analysis. The centralised nature of Google, and the huge data store it has on a wide range of user data collected from about 60 services (including for example: search activities, email messages, calendar information, and Google Plus social network related information) may be problematic for privacy too (Arthur). In a manner similar to Facebook's transition from a small college network to an international corporation, Google has evolved into a company that looks quite different from when it started. In 2009 it was reported that Google dropped its "Don't Be Evil" motto (Foremski) and now appears to be very much like Facebook in its churning of users personal data to money through advertising. Furthermore, Google also appears to be exploiting its user data at the cost of privacy, and in 2012 it was reported that 30 European data protection commissioners criticised changes Google had made to its privacy policy in March 2012 (Arthur). One of the major changes criticised was the fact that Google merged the data collected from its 60 separate services into one single data store. The criticism also pointed out that "the company was storing, without consent, cookies and data about sites people visited for between 18 months and two years" (Arthur).

Like Facebook (since its Initial Public Offering in May 2012), Google also appears to be under pressure to meet shareholders' expectations. While both Internet giants offer "free" services to users, it seems that instead of the traditional form of monetary payment for these services, users now pay with their personal data and, often unknowingly, with their privacy too.

4.6. Conclusion

When I first began the research for this report, I had a strong but at the same time not very succinct sense that privacy violations were occurring on Facebook. As the research progressed and as presented in this report, it became distinctly clear exactly what, why and how violations occur. This report endeavoured to apply the general framework of Helen Nissenbaum and the wide ranging work of Solove to the specific issue of social network privacy. Previous work on which this research was based (particularly the work of Danah Boyd, James Grimmelmann and Chris Peterson) that was more specific to social network privacy than Nissenbaum and Solove, tended to focus on social privacy violations only; while the legal context dealt mostly with issues suited to institutional privacy. However, with the guidance of Kate Raynes-Goldie, this paper acknowledged the distinction between social and institutional privacy and tackled both thoroughly in the assessments of Facebook and Diaspora*. The conceptions developed here helped to determine exactly how violations occur on Facebook, and then additionally helped to determine whether Diaspora* offered a successful alternative to Facebook. Additionally, these conceptions, have guided further requirements necessary for the preservation of privacy on social networks, and I believe can be used to assess effectively the practices and conditions of other online social networks in the future.

5. Glossary of Facebook Terms

Check-in: When a user checks-in, they post information regarding their current location onto Facebook. This is usually done through one's mobile device using GPS technology to determine the current location (Watkins).

Comments: Comments on Facebook are opinions or expressions posted by other users in response to a status update or photo by a particular user (Rouse, "What Is Facebook?").

Friend request: A user adds a Facebook friend to his/her list of friends by sending a friend request. A user does this by selecting the profile of another user and selecting the "add" option. The other user then receives this invitation and can choose whether to accept or decline ("Friend Definition").

Friends list: A Facebook user can view his/her collection of friends in the form of a list. The collection is therefore referred to as a friends list ("Friend Definition").

Friends-of-friends: This term is used to explain the relationship a user has to the friends of his/her Facebook friends. Facebook uses it as a category of friends one may have and is used with the Friends Lists feature explained in Chapter Two.

Group: A Facebook group is a page used by organisations, businesses or groups of people with common interests to coordinate activities (Rouse, "What Is Facebook Group?").

Like: A Facebook user expresses their approval of something on Facebook (a post, a status update, a comment or a photo etc) by clicking a like icon (Rouse, "What Is Facebook 'Like' Button?").

Page: A Facebook Page is a public profile for organisations and businesses. Pages acquire fans when a user likes the Page. Pages operate in the same way user personal profiles do. This means Pages can have features like status updates, photo uploads and events, and users

who are fans of the Page see these activities in their News Feeds (Rouse, "What Is Facebook Page?").

Page Likes: This is the list of Pages that a user has become a fan of (i.e. the user has liked the Page).

Tag: A tag is a hyperlink that links posts like photos, status updates and comments to a specific user's profile page ("Tagging").

Status update: A status update is a feature that allows users to post usually brief messages to their profile pages expressing their thoughts. The status update also appears in users' friends news feeds (Rouse, "What Is Facebook Status?").

6. Works Cited

Acquisti, Alessandro, and Ralph Gross. “Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.” *Proceedings of the 6th International Conference on Privacy Enhancing Technologies*. Berlin: Springer-Verlag, 2006. 36–58. Print.

Allen, Anita L. “Coercing Privacy.” *William and Mary Law Review* 40 (1998): 723. Print.

“API Definition from PC Magazine Encyclopedia.” *PCMAG*. Web. 1 Jan. 2013.

Arrington, Michael. “Facebook Just Launched Open Registrations.” *TechCrunch*. 26 Sept. 2006. Web. 1 Jan. 2013.

Arthur, Charles. “European Union Lays into Google over Privacy Policy.” *The M&G Online*. 19 Oct. 2012. Web. 26 Jan. 2013.

Badat, Farzana. “Protection of Personal Information Bill.” *KPMG*. 13 May 2010. Web. 27 Dec. 2012.

Bankston, Kevin. “Facebook’s New Privacy Changes: The Good, The Bad, and The Ugly.” *Electronic Frontier Foundation*. 9 Dec. 2009. Web. 1 Jan. 2013.

Bhatt, Abhinav. “Facebook Arrest Row: We Support Police Action Against Women, Says Shiv Sena.” *NDTV.com*. 20 Nov. 2012. Web. 18 Dec. 2012.

Bleicher, A. “The anti-Facebook.” *IEEE Spectrum* 48.6 (2011): 54–82.

Bosker, Bianca. “Facebook Privacy Policy Explained: It’s Longer Than The Constitution.” *Huffington Post*. 13 May 2010. Web. 10 Oct. 2012.

Boyd, Danah. “Facebook and ‘radical Transparency’ (a Rant).” *Apophenia* 14 May 2010. Web. 1 Jan. 2013.

---. “Facebook’s Privacy Trainwreck Exposure, Invasion, and Social Convergence.” *Convergence: The International Journal of Research into New Media Technologies* 14.1 (2008): 13–20. Web. 5 Sept. 2012.

---. “Putting Privacy Settings in the Context of Use (in Facebook and Elsewhere).” *Apophenia* 22 Oct. 2008. Web. 10 Oct. 2012.

Boyd, Danah, and Nicole B. Ellison. “Social Network Sites: Definition, History, and Scholarship.” *Journal of Computer-Mediated Communication* 13.1 (2007): 210–230. Web. 5 Sept. 2012.

Boyd, Danah, and Eszter Hargittai. “Facebook Privacy Settings: Who Cares?” *First Monday* 15.8 (2010): n. pag. Web. 26 Sept. 2012.

Boyd, Danah, and Alice Marwick. “Social Privacy in Networked Publics: Teens’ Attitudes, Practices, and Strategies.” *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. 2011. 29. Web. 3 Sept. 2012.

"BuddyCloud - Company Information on BuddyCloud." *VentureBeat Profiles*. 9 Sept. 2008. Web. 4 Jan. 2013.

Byfield, Bruce. "Social and Private with Friendica." *Linux Magazine Online*. Web. 4 Jan. 2013.

Chen, Adrian. "Why Did This 22-Year-Old Entrepreneur Commit Suicide?" *Gawker*. 14 Nov. 2011. Web. 4 Jan. 2013.

"Comparison of Software and Protocols for Distributed Social Networking." *Wikipedia, the free encyclopedia* 25 Dec. 2012. Web. 4 Jan. 2013.

"Cookie Definition." *TechTerms.com*. July 2011. Web. 5 Feb. 2013.

Couch, Aaron. "The 5 Best Hidden Facebook Tricks You Should Make Use Of." *makeuseof*. 28 June 2012. Web. 10 Oct. 2012.

Couts, Andrew. "Terms & Conditions: Facebook's 'Data Use Policy' Explained." *Digital Trends*. 26 Aug. 2012. Web. 25 Sept. 2012.

"Data Use Policy." *Facebook*. 8 June 2012. Web. 30 Sept. 2012.

"Disap.org Privacy Policy." 25 Nov. 2011. Web. 1 Dec. 2012.

"Employers Negotiate Facebook 'Landmines'." *News24*. 26 Sept. 2011. Web. 18 Dec. 2012.

Esguerra, Richard. "An Introduction to the Federated Social Network." *Electronic Frontier Foundation - Deeplinks Blog.* 21 Mar. 2011. Web. 29 Nov. 2012.

"Fair Information Practice Principles." *Federal Trade Commision*. 23 Nov. 2012. Web. 21 Dec. 2012.

Foremski, Tom. "Google Quietly Drops Its 'Don't Be Evil' Motto." *Silicon Valley Watcher*. 1 Apr. 2009. Web. 9 Jan. 2013.

"Frequently Asked Questions Regarding EPIC's Facebook Complaint." *Electronic Privacy Information Center*. Web. 1 Jan. 2013.

"Friend Definition." *TechTerms.com*. Nov. 2009. Web. 5 Feb. 2013.

Gaylord, Chris. "Facebook's Success: Real Names Only." *ABCNews*. 5 Feb. 2012. Web. 1 Jan. 2013.

Gibson, Erika. "Man Suspended over Facebook Post." *News24*. 19 Feb. 2012. Web. 18 Dec. 2012.

Goble, Gordon. "The History of Social Media." *Digital Trends*. 6 Sept. 2012. Web. 29 Dec. 2012.

Goodin, Dan. "Code for Open-source Facebook Littered with Landmines." *The Register*. 16 Sept. 2010. Web. 30 Nov. 2012.

Grimmelmann, James. "Saving Facebook." *Iowa Law Review* . 94 (2009): 1137–1206. Print.

Grippi, Daniel, Ilya Zhitomirskiy, Maxwell Salzberg, and Raphael Sofaer. “A Little More About The Project.” *Diaspora* Blog.* 21 Apr. 2010. Web. 29 Nov. 2012.

---. “A Little More Than 24 Hours Left!” *Diaspora* Blog.* 31 May 2010. Web. 30 Nov. 2012.

---. “An Overdue Update.” *Diaspora* Blog.* 26 Aug. 2010. Web. 30 Nov. 2012.

---. “Developer Release.” *Diaspora* Blog.* 15 Sept. 2010. Web. 2 Dec. 2012.

Grippi, Daniel, Sarah Mei, Sean Tilley, Rosanna Yau, et al. “DIASPORA* Grows Up.” *Diaspora* Blog.* 3 Feb. 2012. Web. 2 Dec. 2012.

Grippi, Daniel, Ilya Zhitomirskiy, Maxwell Salzberg, Sarah Mei, et al. “Diaspora* Is Making a Difference.” *Diaspora* Blog.* 8 Sept. 2011. Web. 30 Nov. 2012.

Grippi, Daniel, Maxwell Salzberg, Ilya Zhitomirskiy, Sarah Mei, et al. “Diaspora* Means a Brighter Future for All of Us.” *Diaspora* Blog.* 21 Sept. 2011. Web. 29 Nov. 2012.

Grippi, Daniel, Ilya Zhitomirskiy, Maxwell Salzberg, and Raphael Sofaer. “Kickstarter Pitch.” *Diaspora* Blog.* 14 Apr. 2010. Web. 29 Nov. 2012.

---. “Private Alpha Invites Going Out Today.” *Diaspora* Blog.* 23 Nov. 2010. Web. 30 Nov. 2012.

Grippi, Daniel, and Maxwell Salzberg. “Announcement: Diaspora* Will Now Be A Community Project.” *Diaspora* Blog.* 27 Aug. 2012. Web. 30 Nov. 2012.

---. “Diaspora* Is Back in Action.” *Diaspora* Blog.* 7 Dec. 2011. Web. 5 Jan. 2013.

Grippi, Daniel, Ilya Zhitomirskiy, and Maxwell Salzberg. “Diaspora* Adopts Computers, Freedom, and Privacy’s Social Network Users’ Bill of Rights.” *Diaspora* Blog.* 24 Oct. 2011. Web. 1 Dec. 2012.

Gross, Ralph, and Alessandro Acquisti. “Information Revelation and Privacy in Online Social Networks.” *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. New York: ACM, 2005. 71–80. Print.

Halliday, Josh. “Google+ Public Launch Takes Battle to Facebook and Twitter.” *The Guardian*. 20 Sept. 2011. Web. 4 Jan. 2013.

Hepburn, Aden. “Facebook Statistics, Stats & Facts For 2011.” *Digital Buzz Blog.* 18 Jan. 2011. Web. 2 Jan. 2013.

Holloway, James. “Spot the Difference: Diaspora Vs. Google+.” *gizmag*. 28 Nov. 2011. Web. 4 Jan. 2013.

Holtzman, David H. *Privacy Lost: How Technology Is Endangering Your Privacy*. San Francisco: Jossey-Bass, 2006. Print.

Johnson, Bobbie. “Privacy No Longer a Social Norm, Says Facebook Founder.” *The Guardian*. 11 Jan. 2010. Web. 10 Sept. 2012.

Kerr, Dara. “Privacy Watchdogs Aren’t Happy About Facebook’s Site Changes.” *CNET*. 26 Nov. 2012. Web. 9 Jan. 2013.

Kirkpatrick, David. *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York: Simon & Schuster, 2010. Print.

Krynsky, Mark. “Storytlr Founders Announce Ambitious One Social Web Project.” *Lifestream Blog.* 10 Feb. 2010. Web. 4 Jan. 2013.

“Legal Procedure Against ‘Facebook Ireland Limited’.” *europe-v-facebook.org*. Web. 9 Jan. 2013.

Leyden, John. “Users Protest over ‘Creepy’ Facebook Update.” *The Register*. 7 Sept. 2006. Web. 31 Dec. 2012.

Liu, Alec. “What Happened to Diaspora, the ‘Facebook Killer’? It’s Complicated.” *Motherboard*. 2 Oct. 2012. Web. 29 Nov. 2012.

Lunden, Ingrid. “Facebook Turns Off Facial Recognition In The EU, Gets The All-Clear On Several Points From Ireland’s Data Protection Commissioner On Its Review.” *TechCrunch*. 21 Sept. 2012. Web. 8 Jan. 2013.

Madden, Mary. *Privacy Management on Social Media Sites*. Pew Internet & American Life Project, 2012. Web. 12 Sept. 2012.

“Main Page - CFPWiki.” *Computers, Freedom, and Privacy 2010 Wiki*. 24 June 2010. Web. 4 Jan. 2013.

“Main Safe Harbor Homepage.” *export.gov*. 4 Nov. 2012. Web. 1 Jan. 2013.

“Marketing: Understanding The ECT Act of 2002.” *interComm South Africa*. Web. 27 Dec. 2012.

Mayer, Adalbert, and Steven L. Puller. “The Old Boy (and Girl) Network: Social Network Formation on University Campuses.” *Journal of Public Economics* 92.1-2 (2008): 329–347. Print.

Mccarthy, Julie. “Facebook Arrests Ignite Free-Speech Debate In India.” *NPR.org*. 29 Nov. 2012. Web. 18 Dec. 2012.

Meyrowitz, Joshua. *No Sense of Place:The Impact of Electronic Media on Social Behavior: The Impact of the Electronic Media on Social Behavior*. Oxford: Oxford University Press, 1986. Print.

Mick, Jason. “Concerned About Privacy? You’re Probably up to No Good, Says Google CEO.” *DailyTech*. 8 Dec. 2009. Web. 12 Dec. 2012.

Moglen, Eben. “Freedom In the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing.” Internet Society. New York. 2010. Speech.

Morley, David. “Diaspora Pod Uptime - Find Your New Social Home.” *Diaspora* Pod uptime*. Web. 29 Nov. 2012.

Nair, Sandhya. “Will Be More Careful on FB Now: Shaheen Dhada.” *The Times Of India*. 17 Dec. 2012. Web. 19 Dec. 2012.

Narayan, Adi. “In India, a Facebook and Free-Speech Debate.” *BusinessWeek: Global Economics* 13 Dec. 2012. Web. 18 Dec. 2012.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009. Print.

“Notes on Installing and Running Diaspora.” *GitHub Wiki: diaspora*. Dec. 2012. Web. 5 Jan. 2013.

“Number of Active Users at Facebook over the Years.” *Yahoo! Finance*. 23 Oct. 2012. Web. 27 Dec. 2012.

O’Leary, Noreen. “IPG: First on Facebook.” *Adweek*. 16 Jan. 2011. Web. 31 Dec. 2012.

Ortutay, Barbara. “Facebook IPO Date: ‘FB’ Set To Begin Trading May 18 After $16 Billion Offering.” *Huffington Post*. 18 May 2012. Web. 2 Jan. 2013.

Parr, Ben. “Facebook’s New Social Plugins Come to 50,000+ Websites in One Week.” *Mashable*. 28 Apr. 2010. Web. 27 Sept. 2012.

Peterson, Chris. “Losing Face: An Environmental Analysis of Privacy on Facebook.” *SSRN Electronic Journal* (2010): 38. Web. 6 Sept. 2012.

Pincus, Jon. “What Diaspora Can Learn About Security from Microsoft.” *Liminal states* 15 2010. Web. 2 Jan. 2013.

Pinto, Nick. “Rise of the Facebook-Killers.” *The Village Voice*. 15 Feb. 2012. Web. 29 Nov. 2012.

“Plug-in Definition from PC Magazine Encyclopedia.” *PCMAG*. Web. 1 Jan. 2013.

Post, Robert. “Three Concepts of Privacy.” *Faculty Scholarship Series* (2001): n. pag.

“Private Facebook Info Accessible with a Simple Hack.” *FBHive*. 22 June 2009. Web. 27 Dec. 2012.

“Protection of Personal Information Bill.” *The South African Institute of Chartered Accountants*. 18 Sept. 2012. Web. 27 Dec. 2012.

“Protection of Personal Information Bill Goes For EU Model.” *Sabinet Law*. 27 Aug. 2009. Web. 27 Dec. 2012.

Raynes-Goldie, Kate. “Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook.” *First Monday* 15.1 (2010): n. pag.

---. “Annotated Bibliography: Digitally Mediated Surveillance, Privacy and Social Network Sites.” *Cybersurveillance and Everyday Life: An International Workshop*. Toronto, 2011. 13. Web. 10 Sept. 2012.

Reiman, Jeffrey. “Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future.” *Santa Clara Computer & High Technology Law Journal* 11.1 (1995): 27. Print.

Rouse, Margaret. “What Is Chat Room? - Definition from WhatIs.com.” *SearchSOA/TechTarget*. Sept. 2005. Web. 28 Dec. 2012.

---. “What Is Discussion Board (discussion Group, Message Board, Online Forum)?” *Whatis.com*. May 2011. Web. 28 Dec. 2012.

---. “What Is Facebook Group?” *Whatis.com*. Nov. 2011. Web. 5 Feb. 2013.

---. “What Is Facebook ‘Like’ Button?” *Whatis.com*. Aug. 2010. Web. 5 Feb. 2013.

---. “What Is Facebook Page?” *Whatis.com*. Aug. 2010. Web. 5 Feb. 2013.

---. “What Is Facebook Status?” *Whatis.com*. Aug. 2010. Web. 5 Feb. 2013.

---. “What Is Facebook?” *Whatis.com*. Feb. 2009. Web. 5 Feb. 2013.

---. “What Is Hashtag?” *Whatis.com*. Aug. 2009. Web. 23 Jan. 2013.

---. “What Is Instant Messaging (IM or IM-ing or AIM)?” *Whatis.com*. Jan. 2008. Web. 28 Dec. 2012.

---. “What Is Open Source Software (OSS)? - Definition from WhatIs.com.” *SearchEnterpriseLinux/TechTarget*. Nov. 2006. Web. 2 Jan. 2013.

---. “What Is RSA Algorithm (Rivest-Shamir-Adleman)? - Definition from WhatIs.com.” *SearchSecurity/TechTarget*. Sept. 2005. Web. 4 Jan. 2013.

---. “What Is Secure Shell (SSH)? - Definition from WhatIs.com.” *SearchSecurity/TechTarget*. July 2005. Web. 4 Jan. 2013.

---. “What Is Secure Sockets Layer (SSL)? - Definition from WhatIs.com.” *SearchSecurity/TechTarget*. Mar. 2007. Web. 4 Jan. 2013.

Samuelson, Robert J. “A Web of Exhibitionists.” *The Washington Post* 20 Sept. 2006. Web. 13 Dec. 2012.

Schneider, Adam. “Facebook Expands Beyond Harvard.” *The Harvard Crimson*. 1 Mar. 2004. Web. 30 Dec. 2012.

Schwartz, Daniel. “8 Facebook Privacy Flaps - Technology & Science.” *CBC News*. 25 Sept. 2012. Web. 25 Sept. 2012.

Scott, Mark. “Facebook to Launch Upgrade to ‘Friends’ List.” *Social Media Today*. 20 Sept. 2011. Web. 29 Sept. 2012.

Sengupta, Somini, and Kevin J. O’Brien. “In Europe, Facebook Agrees to Stop Facial Recognition.” *The New York Times*. 21 Sept. 2012. Web. 8 Jan. 2013.

Sevignani, Sebastian. “The Problem of Privacy in Capitalism and the Alternative Social Networking Site Diaspora*.” *tripleC - Cognition, Communication, Co-operation* 10.2 (2012): 600–617. Print.

Smith, Justin. “Facebook Hires Google’s Sheryl Sandberg as New COO.” *Inside Facebook*. 4 Mar. 2008. Web. 2 Jan. 2013.

“Social Networking Privacy.” *Electronic Privacy Information Center*. Web. 1 Jan. 2013.

Solon, Olivia. “How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories.” *Wired UK*. 28 Dec. 2012. Web. 8 Jan. 2013.

Solove, Daniel J. “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *San Diego Law Review* 44 (2007): 745–772. Print.

---. *The Digital Person: Technology and Privacy in the Information Age*. New York: NYU Press, 2004. Print.

---. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press, 2007. Print.

Sutherland, Adam. *The Story of Facebook*. New York: The Rosen Publishing Group, 2012. Print.

Swart, Heidi. “Secret State: How the Government Spies on You.” *The M&G Online*. 14 Oct. 2011. Web. 3 Jan. 2013.

“Tagging.” *Facebook Help Center*. Web. 5 Feb. 2013.

Tate, Ryan. “Facebook’s European Nemesis Is Crowdfunding a War Chest to Sue.” *Wired Business*. 4 Dec. 2012. Web. 9 Jan. 2013.

Taylor, Chris. “Facebook Rolls Out Privacy Shortcuts in Plain English.” *Mashable*. 21 Dec. 2012. Web. 9 Jan. 2013.

“The Internet Is Our Social Network.” *Friendica*. Web. 5 Jan. 2013.

Tigner, Ronan. “Belgium - Court Condemns Identity Theft on Facebook.” *Linklaters*. 3 July 2012. Web. 27 Dec. 2012.

Tilley, Sean. “Community-Driven: Two Months In!” *Diaspora* Blog.* 29 Oct. 2012. Web. 30 Nov. 2012.

Tsai, Janice Y. et al. “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.” *Information Systems Research* 22.2 (2010): 254–268. Web. 12 Sept. 2012.

Victoria, Bronstein. “What You Can and Can’t Say in South Africa.” *Democratic Alliance*. 19 Aug. 2009. Web. 17 Dec. 2012.

Vielmetti, Edward. “Hotwire and Facebook Beacon.” *Vacuum* 26 Nov. 2007. Web. 1 Jan. 2013.

Volokh, Eugene. “Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You.” *Stanford Law Review* 52 (2000): 63. Web. 17 Dec. 2012.

Waldo, James, Herbert S. Lin, and Lynette I Millett. *Engaging Privacy and Information Technology in a Digital Age*. Washington, D.C.: The National Academies Press, 2007. Print.

Ward, Ryan A. “Discovering Facebook: Social Network Subpoenas and the Stored Communications Act.” *Harvard Journal of Law & Technology* 24.2 (2011): 563–588. Print.

Watkins, Mark. “2011: The Year the Check-in Died.” *ReadWrite*. Apr. 2001. Web. 5 Feb. 2013.

Wauters, Robin. “OneSocialWeb: We’re Ahead Of Diaspora In The Creation Of An ‘Open Facebook’.” *TechCrunch*. 13 May 2010. Web. 4 Jan. 2013.

---. “Open Source Microblogging Startup StatusNet Lands More Funding.” *TechCrunch*. 3 Aug. 2010. Web. 4 Jan. 2013.

Weise, Karen. “On Diaspora’s Social Network, You Own Your Data.” *BusinessWeek: Technology.* 10 May 2012. Web. 29 Nov. 2012.

“Why Client Side Encryption Is a Bad Idea.” *GitHub Wiki: diaspora*. Dec. 2011. Web. 29 Nov. 2012.

Winter, Caroline. “Is Google+ a Ghost Town, and Does It Matter?” *BusinessWeek: Companies and Industries.* 16 May 2012. Web. 30 Nov. 2012.

Zhao, Wenjia. “Rethinking The Social Network: 3 Open-Source Alternatives To Facebook.” *Forbes*. 25 June 2012. Web. 4 Jan. 2013.

Zuckerberg, Mark. “An Open Letter from Mark Zuckerberg:” *The Facebook Blog.* 8 Sept. 2006. Web. 31 Dec. 2012.

“Zuckerberg Reveals Facebook’s 5 Values.” *News24*. 2 Feb. 2012. Web. 1 Jan. 2013.

Zungo, Thuli. “Identity Theft Costing South Africans Millions.” *Sowetan LIVE*. 5 Oct. 2011. Web. 27 Dec. 2012.