PRIVACY IN THE FACEBOOK ERA: A SOUTH AFRICAN LEGAL PERSPECTIVE

INTRODUCTION

In every generation there are new technological inventions that challenge the law to develop in order to fulfil its function of facilitating human interaction. In the late nineteenth century, the invention of hand-held cameras in conjunction with the growth in newspaper circulation figures and the development of sensationalist journalism[1] resulted in the development of the right to privacy as a legal concept in the United States of America. Before 1890, no American court recognised a right to privacy,[2] but towards the end of that year two young partners in a Boston law firm, Samuel Warren and Louis D Brandeis,[3] wrote an article in the *Harvard Law Review* arguing for the recognition of a right to privacy, or as they called it, "the right to be let alone".[4]

Warren and Brandeis were concerned that the new miniature camera technology would be used by the sensationalist press to publish pictures of individuals without their consent.[5] They argued that the courts had in the past granted relief for the invasion of privacy on a combination of different common law doctrines[6] but that in essence the courts were protecting the individual's "right to be let alone"[7] as part of the more general right to one's personality.[8] They further argued that new inventions and business methods made the recognition of the right to privacy necessary.[9][10]

The ideas expressed by Warren and Brandeis reverberated in many other countries.[11] The right to privacy was recognised by implication for the first time in South African case law in the 1950s and was protected under the *actio iniuriarum.*[12]

The next important technological invention that influenced the development of the right to privacy was the introduction of computers in the 1950s.[13] Concerns were expressed that the privacy of individuals would be infringed through the misuse of personal information, since computers are able to store vast amounts of information, including personal information, relatively easily, cheaply and for almost indefinite periods. Furthermore, computers are able to process and disseminate such information at incredible speeds.[14]

The threat posed to personal privacy by the computer came to public notice in various countries during the 1960s as a result of proposals by governments for the establishment of centralised data banks where personal data from various sources would be stored in one place.[15] In reaction privacy advocates voiced alarmist warnings to the public on the threats posed to privacy by computers.[16] Plans by several countries in the 1970s to conduct census surveys featuring the extensive use of personal identifiers, raised further privacy concerns.[17] In consequence, there was a need for the definition of the right to privacy to be enlarged from the "right to be let alone" to a much wider concept. Alan F Westin reformulated the definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[18]

The emergence of data protection laws in the 1970s and 1980s was a subsequent development.[19] Data protection law is related to privacy, but is a narrower concept in that it relates only to the processing of personal information.[20] Data protection law is considered by some writers to be a European creation, deriving from a groundbreaking judgment by the German Federal Constitutional Court in 1983 that recognised a fundamental human right to 'informational self-determination'.[21] All twenty-seven Member States of the European Union (the EU) have subsequently adopted data protection legislation, as have some non-EU European countries.[22] European data

protection law has furthermore strongly influenced data protection laws in jurisdictions outside Europe.[23] South Africa's recently introduced Protection of Personal Information Bill[24] is also a data protection act. The Bill also follows the European example.

The object of all data protection laws is to regulate the processing of personal information or data.[25] These laws aim to give legal protection to a person with regard to the processing of data concerning himself or herself by another person or institution.[26] [27] These laws all contain a set of data protection principles or fair information principles[28] that *inter alia* give the data subject active control over the use of his or her personal information.

The next step in the evolution of computer technology that influenced privacy and data protection law, was the development of personal computers and communication networks. Initially computers were stand alone devices and were merely used to expand and automate existing informational practices. Computers were mainly used by governments and large institutions, such as banks. All the information relating to a particular organisation was stored on a handful of stand-alone computers (also called "mainframes"). However, with the development of personal computers (the PC) linked by means of communication networks, including the Internet,[29] it was no longer necessary for an institution to keep all its information on a particular machine, at a particular place or even in a particular country. Networks enabled more users to gain access to a wider range of personal information. In theory, all the information kept by different organisations (such as financial, medical, educational or employment records) can be shared by different computer users across networks.[30] The notion of information that is stored in a file therefore became outdated.[31] The emphasis moved from the threat posed by computers to the threat posed by the much wider concept of Information Communications Technology (or ICT).[32] ICT technology makes it possible for vast amounts of personal information to be collected, stored indefinitely, processed in various ways and disseminated to an unlimited number of third parties.

Privately run Internet service providers made their appearance during the 1980s. That, coupled with the development of the World Wide Web, led to an expansion in the

popular use of the Internet in the 1990s.[33] The Internet has had a drastic impact on the way people interact. Instead of writing a letter, one can communicate instantaneously by electronic mail (e-mail). Instead of writing in a private journal, one can keep a "blog" (web log – log on a website).[34] One can join a text based discussion forum to consult with people who hold similar interests or keep in touch with friends or make new acquaintances on social networking websites such as Facebook, Twitter or MySpace.

OVERVIEW

The aim of this rather lengthy introduction is to show how technological developments have influenced the development of the right to privacy. The rest of this lecture explores the impact of Social Networking Services (SNSs) on the right to privacy. The aim of the lecture is to determine whether South African privacy law meets the challenges posed by this new technology, or whether it needs to be developed in some way. One could even venture to ask whether privacy still matters in this new technological era.

I shall begin this lecture describing and analysing of a particular SNS, namely Facebook, and identifying the potential privacy risks in the use of Facebook. Next, the right to privacy will be explored in more detail in order to establish whether privacy is relevant when using Facebook and other SNSs. Lastly, proposals will be made on how privacy law will need to adapt to meet the challenges posed by SNSs.

Owing to time constraints, the following issues will not be dealt with:

- Jurisdictional problems when suing for an infringement of privacy (I will confine my discussion to situations where a South African SNS user wants to sue another South African user).
- Conflict of laws issues will therefore not be dealt with either.

- Constitutional law issues will not be dealt with in detail – privacy is also protected under constitutional law, but in this lecture I shall be looking primarily at privacy in the law of delict.

SOCIAL NETWORK SERVICES

INTRODUCTION (EXAMPLES)

The title of this lecture refers to Facebook as an example of a social network service. Facebook is the most popular social network service in South Africa, but it is by no means the only one in existence today. The first SNS website was called Six Degrees,[35] and was launched in 1997. The popularity of these services took off with the launch of Friendster in 2002.[36] Facebook was launched in 2003 by a Harvard student, Mark Zukerberg.[37] With 500 million (500 000 000) registered users it is the most popular SNS worldwide. MySpace, with 130 million (130 000 000) registered users, is the most popular SNS in the United States. Other well-known SNSs include Twitter and LinkedIn, each of which has 75 million (75 000 000) users. The different SNSs cater for a variety of interests. For example, one finds professional sites such as LinkedIn, Visible Path and Xing which focus on business people. "Passion-centric" SNSs like Dogster help strangers connect on the basis of shared interests. Care2 helps activists meetand Couchsurfing connects travellers to people with couches.

For users, the service is free. Facebook sells advertisements to fund the service. Since advertisements on Facebook can be targeted at a specific demographic, they may be very successful. Since Facebook is selling targeted advertising, it is important to the service that users give as much personal information as possible.

DEFINITION

A widely accepted definition of SNS is that provided by dana boyd, a social media researcher. She defines SNSs as

> web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site." [38]

CHARACTERISTICS

From this definition, one can deduce some of the characteristics of an SNS:

(1) It allows a user to create a *profile* or representation of himself or herself that is made up of personal information. Six broad categories of information are provided for on Facebook. It is not compulsory to complete all the fields, but since the purpose of an SNS is to renew contact with old friends or make new ones, one needs to give enough information to enable your friends to find you. The six categories of information are:

   (a) First of all, so-called basic information where one may complete the following fields: the city one currently lives in; what one's hometown is; one's gender, birthday, whether one is interested in meeting men/women; whether one is looking for friendship, or whether one would like to date, to form a relationship or merely to network. One can also fill in one's political and religious views, write a biography and give one's favourite quotations.

   (b) A second category allows one to post a profile picture.

   (c) In a third category one can reveal one's relationship status and who one's family members are.

(d) A fourth category prompts one to state one's tastes in music, books, movies and television.

(e) In a fifth category information about one's educational background and one's employment situation is requested.

(f) A sixth category asks for contact information, such as one's email address, telephone numbers, physical address and any websites where one may be contacted. [39]

(2) A second characteristic of an SNS is that it allows the user to add *contacts* in order to build relationships or a social network. By adding someone as a contact, one gives him or her access to your profile information (that is the personal information I have referred to previously). The purpose of adding someone as a contact depends on the purpose of the SNS. On Facebook one adds a contact to meet new friends or, more often than not, to maintain an existing friendship, perhaps with someone you do not see very often any more, such as a friend from University. On LinkedIn one adds contacts to find a new job. On a dating website one would add potential dates as contacts. Various tools for finding new contacts are provided on the websites.

(3) The third characteristic of an SNS is that it allows a user to *traverse* to other users' sites and to leave a private or public message on the site. On Facebook a public message would be left on what is known as a user's "Wall". Everybody who was added as a contact by a user can see the messages left on the user's Wall and can respond to these messages. One can also interact with other users through certain applications. On Facebook there is an application or game called "Zombies" in which each user controls a zombie that can bite other zombies. Another type of application found on Facebook is "Causes", which allows a user to display his or her social commitments and helps him or her to find other users with the same causes. An application called "Photos" allows one to share photopraphs and "tag" another person in those photographs. "Tagging" a person

means that the application allows one to click on the photograph and then enter the person's name. Should someone else move their cursor over the picture, the person in the picture's name is displayed. If the person is also a Facebook user, the name becomes a link to his or her profile. A user is allowed to "un-tag" himself or herself on a photograph.

To sum up, the three characteristics of an SNS are that it allows a user to create a profile consisting of personal information, to add contacts in order to build a social network, and lastly to traverse to other users' websites to interact with those users.

REASONS WHY PEOPLE USE SNSS

From the definition and characteristics of SNSs, Grimmelman[40] identifies three aspects of social interaction that an SNS enables. These aspects are also the reasons why people join SNSs:

(1) First of all, the profile function allows the user to create an *identity*. It lets you say who you are and it allows you to present yourself the way you want to in the specific context. It is important to recognise that the identity that one portrays is aimed at the specific audience. In other words, it is a controlled impression for a specific audience. Other communications, like joining a specific group (eg Save Darfur), also sends a specific message regarding who you are to the other members in your network.

(2) Secondly, the contacts function allows the user to form or maintain one-to-one connections or *relationships* with other users.[41] By allowing someone to be your contact, you give him or her access to your profile. This means that you share personal information with the contact. Sharing personal information with someone shows that you trust them; it creates a sense of intimacy between you and strengthens personal ties.[42] Other tools or applications can also play a role in strengthening a relationship. On Facebook one can send a "gift" to another

Facebook user, thereby expressing your regard for that person, or you can "poke" someone (whereby the application leaves a message "you have been poked by ___") which means that you are thinking of that person.

(3) The function of traversing lists of contacts allows the user to *become part of a community* or a "social network". It also allows the user to occupy a specific place or have a specific status within the community. Users sometimes compete with each other to add more contacts. Certain applications also allow direct competition. For example, on Facebook one can play competitive games that display the competitor's scores.

Grimmelman concludes that by giving users a forum in which they can create social identities, build relationships and accrue social capital, Facebook and other SNSs fulfill a basic human need which explains why SNSs have become so popular. [43]

THREATS TO PRIVACY POSED BYSNSS

Privacy comes under threat on Facebook or other SNSs in the following ways:

(1) When the user reveals personal information on his webpage.

(2) When the SNS operator receives information from the user or third parties and processes it.

(3) When third parties gain access to the user's personal information.

(4) The launch of Facebook Places in August this year added a fourth threat to privacy.

I will now discuss these threats in more detail.

VISIBILITY

First of all, privacy becomes an issue when the user reveals personal information on his webpage. On SNSs, this act of disclosure is referred to as a user's "visibility" to other users.

All SNSs allow users to control their "visibility" in their "Privacy Settings". Facebook's privacy settings have evolved over the years. Initially privacy was linked to the network a student belonged to. A user had to have a valid university or college email address in order to subscribe to Facebook. The user's profile was visible to all other students with the same email domain, but to no-one else. Over the years the settings have changed. Now anyone with a valid email address can join Facebook. When the point was reached where information came to be shared with third parties, the privacy settings were introduced to allow users to determine which third parties could access their content.[44]

With Facebook's present privacy settings the user's name, profile picture, gender and the networks the user belongs to are always visible to everyone if this information has been supplied. A user does not have to provide a real name or a profile picture. However, Facebook encourages users to use their real names and studies have found that most users do supply a real name and an identifiable profile picture.[45] The setting that enables the name, profile picture, gender and networks of the user to be visible to everyone cannot be changed because, according to Facebook, "it's essential to helping people find and connect with you on Facebook". If the user has supplied the name of his or her hometown or interests, this information is also visible by default, but can be changed in the privacy settings to be visible to friends only.[46]

In Facebook there are three privacy settings to choose from for information other than the user's name, profile picture, gender and networks. Users can choose to make other information visible to "everyone", or to "friends of friends", or to "friends only". It is important to recognise that a "friend" on Facebook is someone you have listed as a "contact" – such persons are not necessarily friends in real life.

Facebook only allows persons who profess to be older than 13 years to sign up.[47] Information of users who say they are under 18 (but older than 13) is treated differently – although their profile picture, gender and networks are also visible to everyone, the visibility of other personal information is limited to "friends of friends" and to their networks, even if they have chosen to make it available to everyone.

Privacy settings are not foolproof and Facebook spells this out clearly on its website.[48]

Facebook was initially not indexed by Google, but at present, like most other SNSs, its publicly available information is indexed. This means that if you search for a person's name on Google, you will find a link to his or her Facebook site if he or she happens to subscribe to Facebook. Even if the person has set the privacy settings on "friends only", the person will still be traceable on his or her username and anyone would be able to view his or her profile picture (if one was provided).

Users can control their visibility to some extent by using the privacy settings to make personal information available only to friends, and of course by limiting the number of friends or contacts they add to their networks. In general, however, most users give out an extraordinary amount of information. The reasons for this will be explored later on.

PROCESSING OF PERSONAL INFORMATION BY THE SNS

Apart from the fact that a user's privacy is threatened by his or her visibility on Facebook, privacy issues are also raised by the collection and storing of personal information. As indicated previously, data protection principles should come into play when personal information is processed.

Facebook receives personal information from the user and from third parties. This information is stored on Facebook until the user deletes it. The collection and storing of personal information qualifies as data processing and the SNS should comply with any applicable data protection principles while processing the data. Facebook subscribes to the Safe Harbor agreement reached between the US Department of Commerce and

the European Union.[49] This agreement was reached after the EU adopted a Directive on data protection in 1995 which threatened to interrupt the flow of personal information between the EU and the United States, since the Directive prohibited the moving of personal information on EU citizen's to a non-EU member state if that state did not provide adequate data protection. [50] After the adoption of the Safe Harbor agreement, US companies have the option of voluntarily certifying that they will adhere to the Safe Harbor privacy principles. These companies are then deemed to provide adequate data protection or privacy protection as required by the EU Directive.[51] This means that Facebook must comply with seven privacy principles, which are briefly referred to as notice,[52] choice,[53] onward transfer,[54] access, [55] security[56] data integrity[57] and enforcement.[58] Facebook's detailed privacy policy aims to fulfill these requirements, although certain shortcomings are apparent.[59] Time constraints do not allow us to deal with these aspects in detail.

Facebook receives and stores the following personal information:

- All the personal information that the user gives out when he or she signs up for Facebook,
- Any content posted by a user, such as when a user updates his or her status, shares a link to a specific site with another user, or sends someone a message,
- Details of transactions or payments that a user make on Facebook;
- Friend information provided by a user in order for Facebook to help the user search for friends on Facebook,
- Activities by the user on the site, such as adding a connection or sending a gift,
- Information about the device, namely the computer or the mobile phone by means of which a user accesses Facebook. For example, the browser type, location and Internet Protocol (IP) address, as well as the pages that the user visits will be collected,
- Information contained in cookies is also collected. Cookies are small pieces of data that are stored for an extended period of time on the user's computer or

mobile phone. For example, a user's login ID is stored to make it easier for the user to login when he or she returns to Facebook.

Facebook also receives information about users from third parties:

- Facebook Platform provides an opportunity for users to connect with applications, such as games, that are not operated by Facebook. Developers can use the Platform to create applications that plug seamlessly into Facebook. When a user connects with such an application, the developer's website informs Facebook of this fact.
- Facebook also receives information from advertising partners, in order to evaluate the effectiveness of the advertisements shown to users.
- In addition, Facebook receives personal information on users from other users, as when a user is tagged in a photograph by another user.

THIRD PARTY ACCESS TO PERSONAL INFORMATION

The third type of threat that is posed to privacy on Facebook is when third parties gain access to personal information. This can happen in the following ways:

- By means of a security breach - this is not a risk that can be eliminated since no site is perfectly secure.[60]
- By means of commercial data mining. Facebook's terms of services prohibit third parties from using the site for this purpose, but the statement does not provide any real protection.[61]
- By means of database reverse-engineering. Facebook's "advanced search" option allows one to search the database of users using any of the fields in a profile, even those fields that were set so that "friends only" could see the information.[62]
- By means of the interception of a password, since the passwords are not sent in encrypted format.[63]

- By searching for a photograph of a user by using the name of the user. Facebook's access control for photographs is weaker than that for a user's profile. Soltren and Jones point out that "the ability of users to upload and tag photographs easily, and the difficulty for a user to de-tag large numbers of photographs, makes it easy for others to find photographs with few restrictions".[64]
- By disclosing personal information to advertisers. According to Facebook's privacy policy this will only happen with the user's consent.
- When other users upload and associate information to one's Facebook account by "tagging" a person in a photograph.

TRACKING THE LOCATION OF A USER

The fourth threat to privacy is posed by Facebook Places. Facebook Places is a geo-location service. Users can access "Places" through a mobile device, namely an iPhone. A user who wants to let friends know where he or she is at that moment can "check in" via the application and that fact will be noted on your friends "news feeds". Users can also be checked in by their friends. Although a user may answer "not now" indicating that he or she does not want to be checked in at the moment, at present users cannot opt out completely from all future attempts to check them in.[65]

There is also a "Here Now" feature which displays a list of all users who have recently checked in at a certain "Place".

REASONS WHY USERS REVEAL PERSONAL INFORMATION ON SNSS

This brings us to the question why SNS users provide so much personal information. As Acquisti and Gross points out:[66]

> Nobody is literally forced to join an online social network, and most networks we know about encourage, but do not force users to reveal - for instance - their dates

> of birth, their cell phone numbers, or where they currently live. And yet, one cannot help but marvel at the amount, detail, and nature of the personal information some users provide, and ponder how informed this information sharing can be….

The authors go on to name the following reasons why users share so much information:

> Changing cultural trends, familiarity and confidence in technology, lack of exposure or memory of the misuses of personal data by others can all play a role in this unprecedented information revelation.

Teenagers are avid users of SNSs and also reveal the most personal information. SNSs "play a key role in youth culture because they give youth a space to hang out amongst friends and peers, share cultural artifacts (like funny Websites, comments about TV shows), and work out an image of how they see themselves". [67]

Grimmelman[68] blames Facebook for the fact that people reveals to much about themselves. He argues that the social dynamics of social networking sites do more than simply give people a reason to use them notwithstanding the privacy risks. They also cause people to misunderstand the privacy risks. He points out that people rely on informal signals to help them envision their audience and their relationship to it. In his words "Facebook systematically delivers signals suggesting an intimate, confidential, and safe setting".[69]

He continues:

> People don't think about privacy risks in the way that perfectly rational automata would. Instead, real people use all sorts of simplifying heuristics when they think about risk, some psychological (people fear the unfamiliar), some social (people fear what their friends fear), and some cultural (people fear things that threaten their shared worldviews). …
>
> When these risks are privacy risks, and when that evaluation takes place in the context of a social network site, these observations have particular force. What people "know" about how the world works drives their perception of risks. For one thing, there is absolutely no plausible way to assign probabilities to many of the possible outcomes. With sufficient data, we could in theory make reasoned decisions about the statistical trustworthiness of large commercial entities. We can't reason in that way about the complex, situated,

> emotional–social dynamics of our contact networks. What is the probability that one of my contacts will republish some of my Wall posts on the Internet? The best we can do is rely—and mostly subconsciously—on the proxies for privacy risks that seem to work well in the social settings that we're familiar with. These proxies don't always work so well on Facebook.

Grimmelman give examples of the proxies that we use in real life and which does not transpose well to an SNS situation. For example, when in doubt people will do what everyone else is doing. One can therefore reason that 50 million users cannot be wrong. One falsely assumes that the 50 million users know something about how safe Facebook is.

Another typical human reaction is to reason that there is safety in numbers. One can argue that on a social network site with 50 million users, what are the odds that I will be singled out by, say, a newspaper that wants to write about my indiscretions as revealed on Facebook? This reasoning does not work for SNSs because privacy problems hit everyone at once.

Another mistake people make is to assume that when you are talking to a friend on Facebook, you are in a private space and since no one but your friend is listening, you can speak freely. Unlike in a restaurant, eavesdroppers on Facebook are invisible.

When we speak to people in person, nonverbal communication is used to indicate that we expect them to keep quiet about what we are discussing – we lean towards them or lower our voice. In the electronic environment these nonverbal cues are absent.

Overall, people's reasons for using social networking sites and their evaluation of the privacy risks involved are driven by social factors.

For young adults, the primary motivation seems to be a desire to be seen. This is hardly new, of course, but what is new is the fact that they are being seen in a digital environment "which confounds the traditional ways in which we control our audiences

and negotiate the boundary between the private and the public, the past and the future, disclosure and privacy". [70]

DO USERS CARE ABOUT PRIVACY?

Acquisti and Gross contend that there is often a dichotomy between young people's desire to protect their privacy and their behaviours.[71] Although they express a concern about their privacy, they still reveal a significant amount of personal information.

Barnes refers to the "privacy paradox" in present-day America where adults are concerned about invasion of privacy, but teenagers are not aware of the public nature of the Internet.[72] She points out that students will share drinking and fraternity pledging photographs with their friends, not expecting that university administrators, and I might add prospective future employers, will also have access to these photographs.

The behaviour of users of SNSs, especially young adults, in terms of revealing personal information, may lead one to infer that they are not really concerned about privacy. In fact, Facebook's founder, Mark Zukerberg, recently said the following:

> 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.[73]

Social network researchers disagree with this statement and question Facebook's attitude towards privacy. Boyd and Hargittai point out that "[a]t each point when Facebook introduced new options for sharing content, the default was to share broadly".[74]

Boyd and Hargittai point out privacy controversies have accompanied the various changes Facebook has made to the site over the years, indicating that users do care about the issue of privacy on Facebook. For example, in 2007 Facebook introduced Beacon, an advertising platform. When a user made a purchase on a partner website,

that information was placed on the user's Wall for sharing with the user's friends. Owing to the privacy controversy surrounding Beacon, Facebook discontinued it in 2009.[75]

At the end of 2009, Facebook again introduced a change in the privacy settings. When users logged on, they were prompted to consider changing their privacy settings. Users were asked to choose between "old settings" and "everyone" meaning that various types of content would be made visible to all other users. In April this year, Facebook introduced yet more changes and the result was a backlash against Facebook in the media. In May 2010 Facebook reacted by unveiling new, simpler privacy settings. This put a stop to much of the news coverage.[76]

In a study by Boyd and Hargittai among first-year students, it were found that "far from being nonchalant and unconcerned about privacy matters, the majority of young adult users of Facebook are engaged with managing their privacy settings on the site at least to some extent". [77]

This brings us to the next main topic, namely whether the right to privacy as a legal right, needs to be developed to meet the demands of users of SNSs.

PRIVACY

RECOGNITION

I indicated earlier that SA case law has recognised and protected privacy under the law of delict since the 1950s.[78] The South African Constitution also recognises the right to privacy as a fundamental human right in the Bill of Rights.[79] Section 14 provides:

> Everyone has the right to privacy, which includes the right not to have –
>
> (a) their person or home searched;

(b) their property searched;

(c) their possessions seized;

(d) the privacy of their communications infringed.

This section guarantees a general right to privacy,[80] with specific protection against searches and seizures, and infringement of the privacy of communications. However, this list is not exhaustive, and it extends to any other method of obtaining information or making unauthorised disclosures.[81]

Some commentators divide the constitutional right to privacy in section 14 into "substantive privacy rights" and "informational privacy rights".[82] The substantive privacy rights enable individuals to make personal decisions about such interests as their family relationships, home life and sexual orientation.[83] Informational privacy rights limit the ability of people to gain, publish, disclose or use information about others without their consent. [84] Seen in this light, the constitutional right to privacy is broader than the private law right, since the former also includes autonomy. [85]

DEFINITION

South African courts accept Neethling's definition of privacy.[86] Neethling defines privacy as "an individual condition of life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself [or herself] determined to be excluded from the knowledge of outsiders and in respect of which he [or she] has the will that they be kept private."[87]

From this definition it is evident that a person determines the destiny of his or her private facts himself or herself. The scope of his or her interest in privacy is therefore also determined by the person himself or herself.[88]

INFRINGEMENT OF PRIVACY - WRONGFULNESS

Since privacy relates to personal facts which a person has determined should be excluded from the knowledge of outsiders, it follows that privacy can only be infringed if someone learns of true private facts about the person against his or her determination and will.[89] Such knowledge can be acquired in one of two ways:[90] through an intrusion, that is where an outsider himself or herself becomes acquainted with the facts,[91] or through a disclosure, that is where an outsider reveals personal information which, although known to the outsider, nonetheless remains private, to third parties.[92]

A *de facto* infringement of privacy will only be wrongful if the infringement is considered unreasonable by the *boni mores* or the legal convictions of the community.[93] [94] In considering when an intrusion should be considered unlawful, one should distinguish between a situation where a person has made private facts known to a limited number of persons, and where he or she has made information known to an indeterminate but still limited number of persons.[95]

In the first scenario, where information is made known only to a limited number of persons, the disclosure is characterised by an element of confidentiality. An acquaintance with this information by an outside party would be unreasonable *prima facie* and thus wrongful.[96] However, the surrounding circumstances may make it apparent that the infringement should not be considered wrongful.

In the second scenario, that is where personal information is revealed to an indeterminable but limited number of persons, the acquaintance with the information by an outsider will be reasonable *prima facie*, but surrounding circumstances may reveal that it should be considered unreasonable and thus wrongful.

Let me illustrate this by referring to practical examples. If I tell someone a personal fact in confidence and a third party eavesdrops on our conversation, the third party is infringing my right to privacy. However, if the eavesdropping happened by chance because we were unknowingly carrying on our conversation in the vicinity of the third party, the legal convictions of the community will not consider the third party's conduct to be unreasonable and therefore it will not be wrongful. [97]

An example of the second scenario is where I appear on a public street. Should I be observed by someone on the public street, I cannot claim that my right to privacy has been infringed and anyone observing me would not be acting wrongfully, since if I appear in a public place I can expect that people will be able to observe my appearance. However, as Neethling correctly points out, this does not mean that the observation of people in public places can never be unreasonable.[98] For example, the constant shadowing of a person is contrary to the legal views of the community and therefore wrongful.[99]

A third type of situation that may arise is where a person acquires knowledge of private facts in accordance with the will and determination of the person to whom the information relates, but then discloses the personal information to outsiders against the will of the person to whom the information relates. The wrongfulness of this disclosure is more difficult to determine. According to Neethling such disclosure is not wrongful, since it is human nature to gossip about other people and the conduct is therefore not *contra bonos mores*.[100] However, in certain circumstances this conduct may be considered wrongful. For example, if the publication amounts to a mass publication, it would be considered unlawful.[101]

APPLICATION TO SNSS

In the context of SNSs, one could argue that subscribing to an SNS and completing your profile information is similar to appearing in a public place. The Internet is a very public place, and Facebook clearly warns subscribers that their privacy cannot be guaranteed. However, in my opinion the privacy settings that one choose, should also be taken into account when considering whether a person has really chosen to disclose his or her information to an indeterminate number of persons. If you chose to reveal your personal information to “Friends Only” and if you limited the number of friends that you added, it could be argued in my opinion that you did NOT choose to reveal your information to an indeterminate number of persons. You have, in fact,

revealed your personal information to a limited number of people. If one of your Facebook Friends then further discloses personal information that was provided by you in these circumstances, I would argue that you should have a delictual claim for infringement of privacy.

It should also be remembered that the wrongfulness of an infringement of privacy is negated by the presence of a ground of justification. Neethling identifies the following traditional grounds of justification as relevant to the right to privacy: necessity, private defence, consent to injury, and performance in a statutory or official capacity. Another ground of justification which is relevant to privacy is the protection of legitimate interests, including the public interest.[102]

In the context of SNSs, consent is a particularly relevant ground of justification. Whenever the user discloses personal information on his webpage, he or she consents to the publication of that private information. However, in order to be valid the consent must meet certain criteria.

The person consenting (the SNS user) must have a full knowledge and appreciation of the nature and extent of the possible harm. An SNS user can therefore not validly consent to the disclosure of his or personal information if he or she is not told what the personal information will be used for and who will have access to it. The consent must also be permitted by the legal order, in other words it should not be *contra bonos mores,* and the impairment must fall within the limits of the consent.[103]

Where I have revealed my personal information to a limited number of persons, I have only consented to the publication of my information to these persons, not to everyone on the Internet. It should therefore not be lawful for third parties to gain access to my profile. Where a person makes an extensive search on the Internet and especially on SNSs in order to compile a profile on another person, such conduct can in my view be considered analogous to the “shadowing” of a person in real life and should therefore be wrongful.

Reportedly some employers, especially in the USA, search the Internet these days for information on prospective employees. It is possible that an employer might gain access to, say, a compromising picture posted by a Facebook user as a student, never thinking that the picture might be seen by prospective employer a few years down the line. In my opinion, this would amount to an infringement of the privacy of the Facebook user. The information the user posted, was meant for a specific audience, at a specific time in his or her life. It was never the user's intention that this information should be seen by another audience at a later stage of the Facebook user's life.

Significantly, in August this year, the German Federal Cabinet approved a draft law that prohibits employers from looking at a prospective employee's Facebook profile.[104] In terms of this proposed Act, employers in Germany will be allowed to enter job applicants' names into search engines and professional networking sites, but must not examine their profiles on Facebook.[105] According to the draft law, employers may collect data in the public domain as a means of researching a job candidate, except where the legitimate interests of the employee in that data outweigh the legitimate interests of the employer. It specifies that social networks that are used for electronic communication may not be used for research, except for social networks that exist to represent the professional qualifications of their members.[106]

A subscriber to an SNS provides personal information for the purpose of forming social connections with other users. The use of that personal information in another context, such as by a prospective employer to screen job applicants, amounts to an infringement of the data protection principle that personal information should only be used for the purpose for which the information was originally supplied, or for a similar purpose. When the Protection of Personal Information Act is adopted in South Africa, this principle will form part of our law and could in my view be used to protect subscriber to SNSs against the use of their information for unrelated purposes.

In my view a person who uploads pictures on his or her website should not identify or "tag" other parties in the picture without their consent. At present Facebook requires that the e-mail address of a person who is being tagged should be provided. That

person then receives an e-mail notification that tagging has taken place so that the person has the opportunity to untag himself or herself. In other words, the user is given the opportunity to "opt-out" of the tagging function. To my mind a situation where one is asked to "opt-in" would be more reasonable. Not everybody in our society is necessarily technically confident enough to be able to remove a tag. Why should the burden of de-indentifying his or her image be on the person who did not upload the picture?

CONCLUSION: PROPOSALS

HOW SHOULD THE LAW DEVELOP?

I have begun this lecture by describing how the law has continuously adapted to accommodate new technological inventions in order to recognise and protect the individual's right to privacy. My proposal is that the law should also develop to recognise that people who use SNSs such as Facebook do not give up all expectations of privacy.[107] The mere fact that they reveal personal information on what may be considered a public forum does not mean that they intend to make that information available to all and sundry. Information revealed to "friends only" should be treated as information that has been published to a limited number of persons and any distribution of that information by third parties to a wider audience should be considered an invasion of the right to privacy.

Similarly, searches on the SNSs by third parties for purposes unrelated to the purpose for which the personal information was initially supplied should be considered as wrongful.

WHAT SHOULD FACEBOOK DO (OR NOT DO)?

Facebook itself also has to respect users' right to privacy. It should not change privacy settings overnight as it has done in the past. Since the terms of agreement between Faceboook and a user set the limits of a person's consent to the display of his or her

personal information, a unilateral change to these terms and conditions on the part of Facebook results in my view in a negation of the consent by the user.

WHAT CAN WE DO?

Teenagers are the most devoted users of SNSs and are also the most likely to underestimate the privacy risks inherent in such usage. Educating teenagers on this topic should therefore be a priority. When and where such education takes place, is also important. Teenagers are more likely to listen to their peers and to pay attention to information provided in their milieu – Facebook itself could probably do more to inform young adults about the privacy risks. Merely referring users to their privacy policy is not sufficient, as studies have shown that most users do not read privacy policies. However, since we cannot influence Facebook, we must try to do our part.

When talking to young adults, we should emphasise that they should be conscious of the fact that their conversations on Facebook may not be as private as they would like to think. Adding too many contacts as friends, or making your profile available to everyone, carries privacy risks that young people should be made aware of. They should be informed of the long-term negative effects that may result from the information they are supplying now.

---

[1] Between 1850 and 1890, US newspaper circulation grew 1,000 percent—from 100 papers with 800,000 readers to 900 papers with more than 8 million readers. See Solove Daniel J, Rotenberg Marc, Schwartz Paul M *Privacy, Information, and Technology*, Aspen Publ (2006) 9-11.

[2] Keeton Page *Prosser & Keeton on the Law of Torts* (1984) 849; Trubow George B "The development and status of 'information privacy' law and policy in the United States" 1–9 in *Invited papers on privacy: law, ethics, and technology* (Presented at the National Symposium on Personal Privacy and Information Technology held in Washington DC on 4–7 October 1981) (1982). A right to privacy was not recognised in English common law, which was the law inherited in the United States of America.

[3] Brandeis and Warren graduated first and second in their class at Harvard Law School in 1877. They founded their law firm in 1879. Louis Brandeis later became an associate justice of the United States Supreme Court (1916 to 1939).

[4] They borrowed the term from Justice Cooley who used it first in his book *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract* Callaghan and Company (1907) at 29.

[5] Warren and Brandeis wrote the article after a spate of gossip appeared in the Boston newspapers about the social affairs of Mrs Warren, the daughter of a senator from Delaware and one of Boston's élite. Boston was one of the cities "where a lady and a gentleman kept their names and their personal affairs out of the papers" (Prosser 1960 *Cal L R* 383–423) and when the press had a field day with the wedding of their daughter, Warren became annoyed.

[6] Eg on the basis of defamation, a property right (eg *Prince Albert v Strange* (1849) ER 1171 where private letters were published), breach of confidence or an implied contract (eg *Yovatt v Winyard* (1820) 37 Eng Rep 425 where recipes that had been obtained surreptitiously by an employee were published).

[7] Warren & Brandeis 1890 *"*The right to privacy*" Harvard Law Review* 193, 195.

[8] Warren & Brandeis 1890 *Harv LR* 193, 205, 207.

[9] Warren & Brandeis 1890 *Harv LR* 193–195:

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society... Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual... the right 'to be let alone.' Instantaneous photographs and newspaper enterprises 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." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the incision of privacy by the newspapers, long keenly felt, has been but recently discussed...

[10] The American courts and State legislatures began to apply the Warren-Brandeis' "right to privacy" terminology to situations other than the publication of information about individuals. In 1960 Prosser concluded that the overwhelming majority of American courts had declared that privacy in one form or another existed. Prosser was of the opinion, however, that what emerged from those decisions was not one tort, but a complex of four, which are tied together by the common name "right to privacy" but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff "to be let alone" (see Prosser William "Privacy" 1960 *California Law Review* 383, 389). He described these four torts as follows: intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs; public disclosure of embarrassing private facts about the plaintiff; publicity that places the

plaintiff in a false light in the public eye; and appropriation, for the defendant's advantage, of the plaintiff's name or likeness. Prosser's framework of four torts became widely accepted and in 1977 the *Restatement (Second) of Torts* accepted this division - see *Restatement (Second) of Torts* s 652B (s 625E (1977). In SA case law, *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (W) represented a false light situation whilst in *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) there was an appropriation of the plaintiff's name or likeness for advertising purposes.

The US Supreme Court also developed a constitutionally based privacy right from explicit constitutional protections against search and seizure, and the probable cause, self incrimination, and due process clauses as contained in the Third, Fourth, Fifth and Fourteenth Amendments. Informational privacy rights, as opposed to substantive privacy rights, were developed around the Fourth Amendment's prohibition against unreasonable searches and seizures and the Fourteenth Amendment's due process requirement. On the development of the constitutional right to privacy, see Tribe *Constitutional law* 1302 *et seq*.

11 For example, in Dutch legal literature, the article by Warren and Brandeis 1890 *Harvard LR* 193 is referred to as the foundation of the development of the right to privacy (see Verhey LFM *Horizontale werking van grondrechten, in besonder van het recht op privacy* (1992) 192; Sentrop JW *Privacy-bescherming in Nederland: schets van een ontwikkeling* (1985) 11–12. And in New Zealand, privacy as a legal issue arrived "by osmosis" from the USA (see Palmer G "Privacy and the Law" 1975 *New Zealand Law Journal* 747.

12 *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) ; *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (W); *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T); *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 267.

13 Computers have been used since the mid-1950s to process information. The first computer that was commercially used, the UNIVAC 1, was installed in 1951 at the United States Bureau of Census (Davis *Computer data processing* 8).

14 Flaherty David H *Protecting privacy in surveillance societies – the Federal Republic of Germany, Sweden, France, Canada, and the United States* (1989) 2; Schwartz Paul M "Data processing and government administration: the failure of the American legal response to the computer" 1992 *Hastings Law Journal* 1321, 1334–1343.

15 In the USA, eg, the Social Sciences Research Council proposed in 1966 the establishment of a Federal Data Centre with the authority to obtain computer tapes and other machine-readable data produced by all federal agencies. Its function would have been to provide data and service facilities to federal agencies and users outside the government. In the end the proposed Central Data Bank floundered amid a spate of hostile publicity. See Bennett Colin J *Regulating privacy: data protection and public policy in Europe and the United States* (1992) 74-75; Regan Priscilla M *Legislating privacy: technology, social values, and public policy* (1995) 7.

[16] See, eg, *The naked society* by Vance Packard (1964), *The privacy invaders* by Myron Brenton (1964), Alan Westin's *Privacy and freedom* (1967) and Arthur Miller's *Assault on privacy* (1971). This literature tried to raise public awareness of the intrusiveness of new technologies. There are numerous references to "Big Brother" and "1984"in this literature. Bennett *Regulating privacy* 70.

[17] For example, in the Netherlands, the history of privacy legislation began with the general census of 1971. See De Graaf F *Privacy en persoonsgegevens: het ontwerp van Wet Persoonsregistraties* (1987) 1; Nugter ACM *Transborder flow of personal data within the EC* (1990) 145. The census was planned in response to a request by the United Nations, the European Commission and Benelux that countries should conduct a census in or around 1970. Kuitenbrouwer F, Verkade DWF & van der Horst RJM *Drieluik privacybescerming: een overzicht en enkele exercities* (1984) 5. For the first time census forms were used that could be processed by computer (punch cards). Although the idea was that the forms would be divided in two and that the part with the personal information would be kept separate from the statistical information, it was nevertheless feared that the two parts could be brought together through the use of the unique number that was on every card. Memories of the Second World War when the meticulously kept record system of information on Dutch citizens was put to use by the Nazi invaders undoubtedly played a part in the protest that followed. Kuitenbrouwer et al *Drieluik privacybescherming* 6. Also see Overkleeft-Verburg G *De Wet Persoonsregistraties: norm, toepassing en evaluatie* (1995) 41–42. So large was the number of people who refused to cooperate that the census was deemed a failure, and no census was ever attempted again. Overkleeft-Verburg *De Wet Persoonsregistraties* 699.

[18] Westin Alan F *Privacy and freedom* (1970) 7.

[19] The first data-protection law was adopted in 1970 in the German state of Hesse. Sweden enacted the first national data-protection law in 1973, followed by the United States in 1974. Since then numerous other countries have adopted data-protection laws and many have already revised their first data-protection laws or have adoptd completely new, second-generation laws (the Netherlands adopted its second-generation data-protection law in 2000 (Wet Bescherming Persoonsgegevens 2000) and the United Kingdom adopted its in 1998 (Data Protection Act of 1998) On "generations" in data-protection laws, see Bygrave L A *Data Protection Law: Approaching its Rationale, Logic and Limit* (2002) 87–88.

[20] See Kuner Christopher "An International Legal Framework for Data Protection: Issues and Prospects" (January 24, 2009). (Available at SSRN: http://ssrn.com/abstract=1443802). [Accessed on 15 August 2010] Kuner points out that

> in European law, 'privacy' includes issues relating to the protection of an individual's 'personal space' that go beyond data protection, such as 'private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of

information given or received by the individual confidentially'. [Parliamentary Assembly of the Council of Europe, Resolution 428, para. C2 (1970). See Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8, which describes privacy in terms of such rights as respect for private and family life, and the freedom from interference by public authorities.] In the United States, the U.S. Supreme Court has interpreted the Constitution to protect, under the rubric of 'privacy', values that go beyond the protection of personal data, such as an individual's constitutional right to be free from unreasonable searches and seizures by the government; [*Katz v United States*, 389 US 347 (1967)] the right to make decisions about contraception, [*Griswold v Connecticut*, 381 US 479 (1965)] abortion, [*Roe v Wade*, 410 US 113 (1973)] and other intensely personal areas such as marriage, procreation, child rearing, and education; [*Roe v Wade*, 410 US 113 (1973) 152-53] and the right to associate free from government intrusion [*NAACP v Alabama*, 357 U.S. 449 (1958)].

21 Kuner, Christopher, "The 'Internal Morality' of European Data Protection Law" (November 24, 2008). Available at SSRN: http://ssrn.com/abstract=1443797. [Accessed on 15 August 2010]

22 Such as Iceland, Liechtenstein, and Norway.

23 Eg, Argentina, Canada, the Dubai International Financial Centre (DIFC), Hong Kong and Russia.The SA Law Reform Commission also followed the European Model in its proposals for a Protection of Personal Information Bill. See SA Law Reform Commission (SALRC) *Privacy and Data Protection* Project 124 Discussion Paper 109 (2005).

24 Bill 9 of 2009.

25 Korff Douwe *Data Protection Laws in the European Union* (2005) 1.

26 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 267.

27 According to Kuner, "data protection law gives rights to individuals in how data identifying them or pertaining to them are processed, and subjects such processing to a defined set of safeguards" (see Kuner, Christopher "Data protection law and international jurisdiction on the internet (Part 1)" 2010 *Vol. 18 No. 2 International Journal of Law and Information Technology* 176).

28 An example of these core rules can be found in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris 23 Sept 1981) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No 108/1981, Strasbourg 28 Jan 1981) which both have a set of principles of data protection. For example, the OECD Guidelines contain principles of collection limitation, data quality, purpose specification, use limitation, security safeguards and openness. See further Roos Anneliese "Core principles of data protection law" 2006 *CILSA* 102 107 et seq.

[29] The Internet is a worldwide network of computers that use common communication standards and interfaces to provide the physical backbone for a number of applications.See Wikipedia's article "Computer Network" at http://en.wikipedia.org/wiki/Computer_network. [Accessed on 15 August 2010]

[30] Lloyd Ian J *Information technology law* (1997) xxxviii – xxxix.

[31] "Today data is scattered in (in various locations) and thus it is no longer found in a single organised set (a file)" (Benyekhlef Karim "Dematerialized transactions on electronic pathways: a panorama of legal issues" 93–116 in *The electronic superhighway: the shape of technology and law to come* Mackaay Ejan, Poulin Daniel & Trudel Pierr (eds) (1995) 110).

[32] ICT refers to the merging (convergence) of telephone networks with computer networks through a single cabling or link system.

[33] The basic applications and guidelines that make the Internet possible had existed since the 1970s. However, it was only after the development of the World Wide Web by British scientist Tim Berners-Lee in 1989 that the Internet became widely used by the general public. (The World Wide Web, abbreviated as WWW and commonly known as the Web, is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them by using hyperlinks – see Wikipedia's article on the World Wide Web at http://en.wikipedia.org/wiki/World_Wide_Web. [Accessed on 15 August 2010] During the 1990s the global information and communications network that includes the Internet and other networks and switching systems such as telephone networks, cable television networks, and satellite communication networks, became known as the Information Superhigway. See Wikipedia's article on the Information Superhighway at http://en.wikipedia.org/wiki/Information_superhighway. [Accessed on 15 August 2010]

[34] Blog = web log. An online commentary about one's day or something specific.

[35] SixDegrees attracted millions of users, but was forced to close in 2000 because it failed to become a sustainable business. Boyd D M, & Ellison N "Social network sites: Definition, history, and scholarship" 2007 (vol 13 no 1) *Journal of Computer-Mediated Communication* article 11 available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. [Accessed on 15 August 2010]

[36] Boyd D M "Friendster and publicly articulated social networks" 2004 (2) Conference on Human Factors & Computer Systems available at http//www.danah.org/papers/CHI2004Friendster.pdf. [Accessed on 15 August 2010]

[37] See Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1144.

[38] Boyd D M, & Ellison N "Social network sites: Definition, history, and scholarship" 2007 (vol 13 no 1) *Journal of Computer-Mediated Communication* article 11. Available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. [Accessed on 15 August 2010]

[39] Grimmelman calculated that a fully filled-out Facebook profile contains about forty pieces of recognisable personal information – see Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1149.

[40] Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1152-1160.

[41] According to Boyd and Ellison the available research suggests that most SNSs primarily support pre-existing social relations, such as a shared class at school. Boyd, D. M., & Ellison, N. B. Social network sites: Definition, history, and scholarship. 2007 (vol 13 no 1) *Journal of Computer-Mediated Communication* article 11 available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. [Accessed on 15 August 2010]

[42] Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1154.

[43] Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1151.

[44] Boyd Dana & Hargittai Eszter "Facebook privacy settings: Who cares? 2010 Aug 2 (vol 15 no 8) *First Monday* available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589 [Accessed on 15 August 2010]

[45] Gross, Ralph & Acquistiti, Alessandro "Information revelation and privacy in online social networks (the Facebook case)" Proceedings of the 2005 Workshop on Privacy in the Electronic Society (WPES) ACM, 71-80 2005. Available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf. Also see Tufecki Zeynep "Can you see me now? Audience and disclosure regulation in online social network sites" 2008 Feb (Vol 28 No 1) *Bulletin of Science, Technology & Society* 20-36 available at http://userpages.umbc.edu/~zeynep/papers/ZeynepCanYouSeeMeNowBSTS.pdf. [Accessed on 15 August 2010]

[46] See http://www.facebook.com/#!/privacy/explanation.php#basicinfo. .

[47] In 2009, Facebook and other Internet services such as Myspace, Bebo, Google, Yahoo and Microsoft, signed an agreement with European Commission to protect under-eighteens using their services. They adopted a document "Safer Social Networking Principles for the EU" on 10 February 2009. The companies *inter alia* agreed to adopt a "report abuse" button on their sites for the reporting of inappropriate contact from another person, set all the details of under eighteens to "private" by default; stop profiles from under 18s appearing in the search functions within the service or through search engines; ensure that privacy controls are prominent and accessible; and prevent anyone under thirteen from using the service at all. The document is available at http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf. [Accessed on 15 August 2010]

[48] Facebook says on its website:

> Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information.

> We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.

See Facebook's Privacy Policy at http://www.facebook.com/policy.php. [Accessed on 15 August 2010]

[49] See the Safe Harbor's website at http://www.export.gov/safeharbor/.

[50] European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data Dir 95/46/EC 1995 *Official Journal* L 281/ 31

[51] See http://www.export.gov/safeharbor/.

[52] Notice entails that Facebook must provide the data subject with certain information, such as the purposes of the data collection, who in the organisation may be contacted with complaints or enquiries, third parties to whom information will be made known and the options that the organisation offer for limiting disclosure.

[53] Choice entails that Facebook must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorised by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorised subsequently by the individual.

[54] Onward transfer entails that where Facebook wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, Facebook can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

[55] Access entails that individuals must have access to personal information about them that Facebook holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

[56] This entails that Facebook must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

[57] This entails that personal information must be relevant for the purposes for which it is to be used. Facebook should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

[58] The enforcement principle states that in order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments organizations make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

[59] See the discussion by Jones, Harvey & Soltren, José Hiram "Facebook: Threats to Privacy" par 6. Dec 2005. Paper available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. [Accessed on 15 August 2010]

[60] Jones, Harvey & Soltren, José Hiram "Facebook: Threats to Privacy" December 2005. par 7.1. Paper available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. [Accessed on 15 August 2010]

[61] That a third party may be able to harvest personal information from the website, was proved by two students, Jones and Soltren, as later described in research paper written by them. See Jones, Harvey & Soltren, José Hiram "Facebook: Threats to Privacy" December 2005. par 7.2. Paper available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. [Accessed on 15 August 2010]

[62] Jones, Harvey & Soltren, José Hiram "Facebook: Threats to Privacy" December 2005. par 7.3. Paper available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. [Accessed on 15 August 2010]

[63] Jones, Harvey & Soltren, José Hiram "Facebook: Threats to Privacy" December 2005. par 7.4. Paper available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. [Accessed on 15 August 2010]

[64] Jones, Harvey & Soltren, José Hiram "Facebook: Threats to Privacy" December 2005. par 7.5. Paper available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. [Accessed on 15 August 2010]

[65] The American Civil Liberties Union Northern California was the first major organization to release a statement after the debut of Facebook Places. It predictably voiced concern about the feature that allows Facebook users to check their friends in without allowing them to say "no" for all future attempts. See http://news.cnet.com/8301-13577_3-20014168-36.html#ixzz0yq0ghn4e. [Accessed on 30 August 2010]

[66] Acquisti, Alessandro and Gross, Ralph "Imagined communities: Awareness, information sharing, and privacy on the Facebook." Privacy Enhancing Technologies Workshop (PET), 2006. Available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf. [Accessed on 15 August 2010]

[67] Jenkin, Henry and Boyd Dana 2006 "Discussion: MySpace and Deleting Online Predators Act (DOPA)" available at http://www.danah.org/papers/MySpaceDOPA.pdf. [Accessed on 15 August 2010]

[68] Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1160.

[69] Grimmelman James "Saving Facebook" 2009 (94) *Iowa Law Review* 1137 1160.

[70] Tufecki Zeynep "Can you see me now? Audience and disclosure regulation in online social network sites" 2008 Feb (Vol 28 No 1) *Bulletin of Science, Technology & Society* 20-36 available at http://userpages.umbc.edu/~zeynep/papers/ZeynepCanYouSeeMeNowBSTS.pdf. [Accessed on 15 August 2010]

[71] Acquisti, Alessandro and Gross, Ralph "Imagined communities: Awareness, information sharing, and privacy on the Facebook." Privacy Enhancing Technologies Workshop (PET), 2006. Available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf. [Accessed on 15 August 2010]

[72] Barnes, Susan B "A privacy paradox: Social networking in the United States" 2006 (vol 11 nr 9) *First Monday* 4. Available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312. [Accessed on 30 August 2010]

[73] On 8 January 2010. David Kirkpatrick *The Facebook effect: The inside story of the company that is connecting the world* New York: Simon & Schuster (2010) as quoted by Boyd Dana and Hargittai Eszter "Facebook privacy settings: Who cares? 2010 Aug 2 (vol 15 nr 8) *First Monday* available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. [Accessed on 15 August 2010]

[74] Boyd Dana and Hargittai Eszter "Facebook privacy settings: Who cares? 2010 Aug 2 (vol 15 nr 8) *First Monday* available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. [Accessed on 15 August 2010]

[75] Boyd Dana and Hargittai Eszter "Facebook privacy settings: Who cares? 2010 Aug 2 (vol 15 nr 8) *First Monday* available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. [Accessed on 15 August 2010]

[76] Boyd Dana and Hargittai Eszter "Facebook privacy settings: Who cares? 2010 Aug 2 (vol 15 nr 8) *First Monday* available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. [Accessed on 15 August 2010]

[77] Boyd Dana and Hargittai Eszter "Facebook privacy settings: Who cares? 2010 Aug 2 (vol 15 nr 8) *First Monday* available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. [Accessed on 15 August 2010]

[78] In *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) it was held that the *actio iniuriarum* was capable of protecting a person against unauthorized publication of his or her name and likeness in an advertisement. In *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (W), the court protected the right of a plaintiff not to be depicted in a false light (as being unmarried and looking for a boyfriend) as part of her right to privacy. Privacy was mentioned expressly for the first time in our case law in the late 1970s in *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T).

[79] The Constitution of South Africa 1996, s 14.

[80] See also Rautenbach IM "The conduct and the interests protected by the right to privacy in section 14 of the Constitution" 2001 *TSAR* 115; Kemp Gerhard "Die ondersoek van ernstige ekonomiese misdade in die lig van die grondwetlike reg op privaatheid"2000 *Stell LR* 437, 445.

[81] McQuoid-Mason David J "Privacy" in Chaskalson Matthew, Kentridge Janet, Klaaren Jonathan, Marcus Gilbert, Spitz Derick, Woolman Stuart (eds) *Constitutional law of South Africa* (1996) 18–11.

[82] McQuoid-Mason David J "Invasion of privacy: common law v constitutional delict – does it make a difference?" 2000 *Acta Juridica* 248; Devenish GE *A commentary on the South African Bill of Rights* (1999) 147.

[83] McQuoid-Mason 2000 *Acta Juridica* 248. Examples are: *Case v Minister of Security; Curtis v Minister of Safety and Security* 1996 (3) SA 617 (CC) where it was held (per Didcott J) that a ban imposed on the possession of erotic material "invades the personal privacy which s 13 of the interim Constitution ... guarantees that I shall enjoy"; *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 1 SA 6 (CC), where the Constitutional Court held that in so far as the offence of sodomy criminalises private conduct between consenting adults which causes no harm to anyone else, it violates the constitutional right to privacy because it intrudes on the innermost sphere of human life. The court held that "[p]rivacy recognises that we all have a right to a sphere of private intimacy and autonomy which allows us to establish and nurture human relationships without interference from the outside community".

[84] McQuoid-Mason 2000 *Acta Juridica* 248. Examples of invasions of constitutional informational privacy rights include taking a prisoners's blood for DNA testing without consent (*C v Minister of Correctional Services* 1996 (4) SA 292 (T)) and restoring erased computer information (*Klein v Attorney General, WLD* 1995 3 SA 848 (W)).

85 For a discussion of case law on the constitutional right to privacy, see Burchel Jonathan "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" 2009 March (vol 13.1) *Electronic Journal of Comparative Law* 11-13 available at http://www.ejcl.org. [Accessed on 15 September 2010]

86 *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271; *Jooste v National Media Ltd* 1994 (2) SA 634 (C) 645; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) 384; *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 789; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 (4) SA 549 (T) 553.

87 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 32.

88 In *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271 the court expressed it thus:

> The individual concerned is entitled to dictate the ambit of disclosure eg to a circle of friends, a professional adviser or the public. . . He may prescribe the purpose and method of the disclosure. . . Similarly, I am of the view that a person is entitled to decide when and under what conditions private facts may be made public."

See also Neethling "The concept of privacy in South African law" 2005 *SALJ* 19-20; Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 31.

89 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 33.

90 *Neethling*, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 33; *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 (3) SA 56 (W) 60; *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 789. Compare *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462–463; also see McQuoid-Mason David J *The law of privacy in South Africa* (1978) 134; Gross Hyman "The concept of privacy" 1967 *New York University Law Review* 34, 37.

91 Eg by unlawfully intruding on property, searching and seizing documents, secretly watching someone or using surveillance equipment to gather information on someone (see *S v A* 1971 (2) SA 293 (T)).

92 An example of an acquaintance through disclosure is eg when a doctor tells his friends about a patient's HIV status (see *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (A)).

93 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 221; McQuoid-Mason "Constitutional privacy" 18–2; Van der Walt JC "'Duy of care': tendense in die Suid-Afrikaanse en Engelse regspraak" 1993*THRHR* 558, 563.

94 The criterion of reasonableness (or what society recognises as reasonable) is also the yardstick the Constitutional Court utilises to determine the wrongfulness of an infringement of privacy. The constitutional (informational) right to privacy has been

interpreted by the Constitutional Court as coming into play wherever a person has the ability to decide what he or she wishes to disclose to the public (See *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) 557). The expectation that such a decision will be respected must be reasonable. In other words, it extends to those aspects of a person's life in regard to which he or she has a legitimate expectation of privacy *(Bernstein v Bester NO* 1996 2 SA 751 (CC) 792; *Protea Technology Ltd v Wainer* [1997] 3 All SA 594 (W) 608; 1997 9 BCLR 1225 (W) 1241). See also Currie & Klaaren *AIA commentary* 116–117 (par 8.2).

95 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 222.

96 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 222.

97 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 225.

98 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 225.

99 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 225 n 74 and authority cited there.

100 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 227.

101 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 231.

102 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 240.

103 Neethling, Potgieter & Visser *Neethling's Law of personality* 2nd ed (2005) 251; Van der Walt & Midgley *Delict* 115 (par 89); Van der Merwe & Olivier *Onregmatige daad* 92–93.

104 See Out-LAW News, 26/08/2010 at http://out-law.com/page-11336. [Accessed on 15 September 2010]

105 See Out-LAW News, 26/08/2010 at http://out-law.com/page-11336. [Accessed on 15 September 2010] See also http://www.bmi.bund.de/cln_156/SharedDocs/Kurzmeldungen/DE/2010/08/beschaeftigtendatenschutz.html. [Accessed on 15 September 2010]

106 See Out-LAW News, 26/08/2010 at http://out-law.com/page-11336. See also http://www.bmi.bund.de/cln_156/SharedDocs/Kurzmeldungen/DE/2010/08/beschaeftigtendatenschutz.html. [Accessed on 15 September 2010]

[107] Also see Papadopoulos S "Revisiting the public disclosure of private facts in cyberworld" 2009 (vol 30 no 1) *Obiter* 30-43 available at http://www.journals.co.za/ej/ejour_obiter.html and at http://www.up.ac.za/dspace/bitstream/2263/11810/1/Papadopoulos_Revisiting (2009).pdf [Accessed on 15 September 2010]