ETHICS AND SOCIAL NETWORKING SITES: A DISCLOSIVE ANALYSIS OF FACEBOOK

Abstract

Purpose: This paper provides insights into the moral values embodied by a popular social networking site (SNS), Facebook. We adopt the position that technology as well as humans has a moral character in order to disclose ethical concerns that are not transparent to users of the site.

Design/methodology/approach: This study is based upon qualitative field work, involving participant observation, conducted over a two year period.

Findings: Much research on the ethics of information systems has focused on the way that people deploy particular technologies, and the consequences arising, with a view to making policy recommendations and ethical interventions. By focusing on technology as a moral actor with reach across and beyond the Internet, we reveal the complex and diffuse nature of ethical responsibility in our case and the consequent implications for governance of SNS.

Research limitations/implications: We situate our research in a body of work known as disclosive ethics and argue for an ongoing process of evaluating SNS to reveal their moral importance. Along with other authors in the genre, our work is largely descriptive, but we engage with prior research by Brey and Introna to highlight the scope for theory development.

Practical implications: Governance measures that require the developers of social networking sites to revise their designs fail to address the diffuse nature of ethical responsibility in this case. Such technologies need to be opened up to scrutiny on a regular basis to increase public awareness of the issues and thereby disclose concerns to a wider audience. We suggest that there is value in studying the development and use of these technologies in their infancy, or if established, in the experiences of novice users. Furthermore, flash points in technological trajectories can prove useful sites of investigation.

Originality/value: Existing research on social networking sites either fails to address ethical concerns head on or adopts a tool view of the technologies so that the focus is on the ethical behaviour of users. We focus upon the agency, and hence the moral character, of technology to show both the possibilities for, and limitations of, ethical interventions in such cases.

Keywords: Social networking, Social Media, Disclosive Ethics, Morality of Technology, Design, Consequences

1   Introduction

The uptake of Internet sites such as Facebook, MySpace and YouTube has led to the widespread study of mainstream social networking sites (SNS). In broad terms, social networking involves social relations amongst people who have [and indeed desire] some type of relationship or affiliation (Wellman 1996). Thus, SNS may be conceptualized as socio-technical arrangements incorporating technologies that support such activities. Prior arrangements such as chat rooms, mobile phones and landline based telephones have held, and continue to hold, the potential to facilitate social networking. Thus we acknowledge that contemporary social networking sites, and the study of them, are historically situated. There may be new challenges raised, but there is also continuity. One facet of continuity, and the one we engage with here, is the issue of ethics and how moral challenges are brought about in ICT mediated spaces.

With respect to social networking, a scan of the popular press reveals some key ethical issues – many will be familiar with the trope of employer surveillance through SNS (Rothberg 2006; Rothberg 2008) and the usage for marketing purposes of data that has been marked as private (CNET 2008). Further well trodden themes in social networking research – such as identity, use/non-use, motives for use, privacy, surveillance, friending, commodification, and user exploitation – all surface issues with ethical dimensions[1]. In terms of identity work, for example, Light (2007) considers the way that social networking arrangements can facilitate marginalization, while Larsen (2007) discusses the seeming lack of sincerity and authenticity in Arto. Both of these studies are ethically charged. Similarly, issues of privacy, surveillance and information revelation have moral importance, but SNS studies by Joinson (2008) and Gross and Acquisti (2005) do not pursue an ethical slant. Even boyd's (2006) study of the tensions around using applications that rank friends and Petersen's (2008) work on the exploitation of users provide limited direct comment on the ethics of such practices. So, at present, the ethical issues associated with social networking spaces are not being tackled head on. Most crucially for our study, the moral values embodied by the technologies themselves are not called into question.

Several influential positions on ethics are informed by normative theories that aim to develop a set of best practices governing human conduct. Normative ethics sees morality as a human concern. It is based on a tool view of (information) technology (Orlikowski and Iacono 2001), in which people have control over the ends to which technology is deployed and thus are able to design systems and employ preventative measures to guard against the likelihood of undesirable behaviours and outcomes. Attention may focus on the consequences of action (consequentialism); the nature of the act, in terms of one's duties and others' rights (deontology); or the moral character of the agent (virtue ethics) (Johnson 2001). From this perspective, individuals engage in moral conduct by following principles and rules, or adopting habits and behaviours seen as virtuous. The Kantian individual, as an autonomous agent who makes decisions and moral judgements on the basis of rational considerations, has been a popular form of the deontological tradition in several academic fields (Bell and Adam 2004). The implications of research in this perspective are that it allows a consideration of the impacts of technology (Introna 2007) and how ethical issues may be addressed through, for example, policy interventions targeting governance of the Internet.

Our research in this paper is descriptive. Rather than offering a favoured set of norms and values against which an actor's moral conduct may be judged, we are concerned with the actors' attitudes and beliefs about morality. Descriptive ethics seeks to uncover the actors' values and ideals, their beliefs about which actions are right and wrong, and how they judge the character of moral agents.

---

[1] See, for example: identity (boyd 2006; Donath 2007; Light 2007; Liu 2007); motives for use/things gained from use, privacy/surveillance issues and profile completion (Donath 2007; Ellison et al. 2006; Gross and Acquisti 2005; Joinson 2008; Krasnova et al. 2010; Lampe et al. 2006; Lampe et al. 2007); friending (boyd 2004; boyd 2006; Donath 2007; Joinson 2008; Lampe et al. 2007); commodification and/or user exploitation (Fernback and Papacharissi 2007; Griffiths and Light 2008; Light et al. 2008; Magnet 2007; Petersen 2008; Röhle 2007) and use/non-use (Byrne 2007; Golder et al. 2007; Hargittai 2007; Lange 2007).

Such research requires empirical investigation rather than *a priori* judgements about the nature of right and wrong. We adopt a particular form of descriptive ethics which is disclosive in nature. Disclosive computer ethics focuses on the moral norms and values embedded in information technologies, applications and practices (Brey 2000b), although authors differ in the extent to which they attribute agency to non-humans and hence in where they attempt to locate the ethics of technology. Prior studies have addressed facial recognition systems, search engines and plagiarism detection systems (Introna 2005; 2007). Our research contributes to this growing body of work with some implications for the theory and practice of social networking. Specifically, we engage with prior research by Brey and Introna to distinguish our own perspective on locating the ethics of technology. Informed by this view, we then raise important and controversial questions about the extent to which intervention is possible in social networking activities, however morally desirable it may be in some cases.

The remainder of this paper is organized as follows. In the next section, we situate our research within the major bodies of work on ethics and outline how our concern to explore the ethics of information technology may be addressed by a disclosive ethics approach. Then we provide details of our own ethical stance and the intellectual position that has guided our work. Next, we present an empirical example drawn from the authors' ongoing research into social media. Drawing from this work, we make visible some of the strategies used to enrol members of Facebook and the potential implications of their enrolment. In our conclusions, we suggest some ways forward for theory development and practice and outline the conditions of possibility for such action.

2   Ethics, Disclosure and the Morality of Technology

The emergence of new technologies inevitably gives rise to ethical concerns. The uptake of social networking sites has raised questions about their potential to facilitate deception, social grooming and the creation of defamatory content, amongst others (Bahney 2006; Fox News 2007; Sweney and Gosden 2006). One popular form of this argument takes a consequentialist position which holds that what make an action (design) right or wrong are its ultimate consequences. From this perspective, the emphasis in technology design should be on achieving the greatest good for the greatest number, and developers of social networking sites are seen to have ethical responsibilities for ensuring that their designs are oriented towards achieving the desired goal. The developers, on the other hand, appear to hold a user oriented view – they make social networking sites for people to play with. Although they choose, or are compelled, to regulate particular aspects of interaction through privacy and acceptable use policies, such approaches are targeted at the members of sites in terms of what they can and cannot do, what might be done with their data and by whom. In this case, the ethical focus switches to what people should do and expect in terms of their moral obligations and rights. Such normative views of morality attribute agency to humans (in this case, the designers and users), while information technology is seen as an object in their hands which may be fashioned in ways that are morally acceptable or not. Overall, technology is seen as a neutral actor and hence questions about the morality of technology do not arise.

Whilst a human-centric approach to social networking is a valuable line of inquiry, it does mean that minimal attention is given to the role of technology in shaping such spaces and interactions, although a few studies do run counter to this trend. For example, Kim and Yun (2007) show how the functions and features of Cyworld shape user's relations with themselves; Kendall (2007) describes how the technological features of Livejournal reveal the tensions in social interactions; and boyd deals with how the Facebook News Feed application caused concern about exposure and invasion of privacy among users (boyd 2008a). Nevertheless, even studies that address the role of technology in shaping such spaces often present the technological functions and features as properties designed in by developers so that, again, the focus is on human agency. Technology as an actor is downplayed or ignored and morality is seen as a human concern.

In this paper, we adopt a disclosive ethics approach, a form of descriptive ethics concerned with embedded norms and values in information systems and related practices. A key point of difference

among authors in the genre is the extent to which they acknowledge technology as an actor, by which we mean the degree to which they separate the 'social' and the 'technical', and hence where they locate agency and, in turn, a capacity for ethical behaviour. We return to this point later on when we outline our own ethical stance, but first we highlight some key forms of a disclosive ethics approach as a prelude to describing the form adopted in this paper.

2.1 Approaches to Disclosive Ethics

Brey (2000a; 2000b) proposed a three-stage approach to disclosive computer ethics: i) a disclosure stage, where a computer system or software is analysed in terms of commonly-held moral values such as privacy or justice; ii) a theoretical stage, where moral theory is developed by abstracting from particular technologies, applications or practices; and iii) an application stage, where moral theory is applied to analyses resulting from the disclosure stage. His work may be seen as an effort to formalize 'a family of approaches' in computer ethics 'concerned with disclosing and evaluating embedded normativity in computer systems, applications and practices' (Brey 2000a, p. 11/12). In advocating a pre-theoretical disclosure stage, he runs into a critique from Messerly (2007) on the grounds that a research study will always be informed by preconceptions about the technology or practice such that a theory-neutral position is not possible. Thus Brey separates the disclosure and theoretical stages – analytically at least – but then resorts to a relative argument about the extent to which action is theory-laden at different stages of his proposed approach. Further analytical distinctions between technology and society are suggested by his references to embedded normativity, as well as to the development and use of computer technology separately from the products of such actions, such as systems, software and manuals (Brey 2000b).

Introna (2005) also focuses on disclosure as a first principle of information technology ethics, but he makes clear from the outset the intellectual resources – from phenomenology and ANT (actor network theory) – that inform his ethical stance (Introna 2007). His proposed framework for an ethics of information technology sees politics and ethics as opposite sides of the same coin. In effect, information technologies are designed and used in political acts that enclose some interests and exclude others. Any failure to disclose whose interests are included and whose are not, or to seek closure without regard to ethics, is a moral concern that needs to be made visible. In Introna's analyses, disclosure is not theory neutral and technology is not morally neutral; rather, he highlights the uncertainty in attempts to separate theory from disclosure, technology from society, designers from users, or winners from losers. Indeed, he claims that we cannot, in any obvious manner, locate where morality begins and where it ends.

It is to the implications of this last point that we address our argument in this paper. If we cannot locate morality with any degree of certainty, then what potential exists for security, privacy or other moral concerns, which in our case are related to the use of SNS? Like Introna, we find the intellectual resources of ANT useful for addressing our research issue, but our work differs from his in two ways. First, in contrast to the relatively opaque technologies disclosed by Introna – facial recognition systems, search engines and plagiarism detection systems, amongst others – we examine a seemingly more transparent arrangement, the SNS Facebook. SNS require active user involvement which can create the illusion of control when, in fact, the operation of the sites and the outcomes of their use are not at all transparent. Second, our ethical stance is more broad ranging than Introna's, in part at least because we adopt a reading of ANT that focuses on its methodological potential. Thus, we share Introna's concern to disclose the decisions and practices related to information technology design and use because we believe that the interests they enclose and exclude should be made visible. However, given the active nature of user involvement in our case, we also aim to learn about the actors' motivations for behaving as they do – reasons about which we are neither completely agnostic nor sufficiently informed to theorize them *a priori*. Such insight is important for understanding the possibilities for, and limitations of, ethical interventions in this case.

Our approach is influenced by Latour's (1999a) assertion that 'ANT is *more a method* to deploy the actor's own world building activities *than an alternative social theory*' (p. 15, our emphasis). In this

way, our aim in this section is not to present some theoretical ideas or concepts that are later used to frame an explanation of the actors' behaviours and reasons. Rather, we see ANT as a way of accessing a research site – of following the actors to find out what they do and how and why they do it – without an *a priori* theory that constitutes an actor as the bearer of particular competencies and interests. In short, our account of Facebook is descriptive not explanatory and is followed by a discussion that highlights the implications of our findings in terms of some widely understood moral concerns, such as security and privacy. First though, we outline some ideas from ANT that may be seen as principles that guided our methodological effort of recording the world-building activities of the site of interest and informed our ethical stance.

2.2 The Morality of Technology

ANT is premised on the view that technology and society are mutually constitutive. Thus we cannot attribute intentionality and purposeful action to humans alone. Rather, they are a property of institutions – hybrid entities of humans and non-humans (Latour 1999b). Thus when someone enters a site, such as MySpace or Habbo Hotel, a whole series of opportunities open up which prior to this encounter existed only as potentialities. Both they and the space are transformed – the member is now able to chat, play games or communicate with friends, while the possibilities of the space (some intended and some unintended) are also revealed. Furthermore, a range of possibilities are closed off. Latour (2005) addresses these potentialities and the way they are transformed into possibilities through *four sources of uncertainty about the 'social'* – the nature of groups, actions, objects and the way they associate to achieve a transformation.

Latour's central argument is that *objects can act to make a difference* to a state of affairs. In this way, they are *mediators rather than intermediaries* because they transform rather than simply transport the meaning of what they carry. Thus when we sign on to Facebook, the possibilities we have – for communicating with others, for disclosing who we are or are not, for making new friends – are revealed in a different way. A number of facilities are offered by the technology; we choose some and decline others, but the manner of their presentation, our adeptness in using the system, our original intention in signing on to our accounts, and so on, all participate in the transformation (or translation of interests) that takes place. We may be distracted by an invitation from another member, or we may single-mindedly pursue our original goal. In the latter case, the unexpected opportunity offered by another actor (a combination of human and object) was not sufficiently attractive to deflect us from our course. However, this may occur for many reasons – we may not be interested in the specific invitation, we may have grown weary of accepting invitations because the opportunities they offer are over-familiar, or we may have pressing business and be unwilling to tolerate distractions. The way technology acts may transform our intentions, but equally what we do has implications for the potentialities of the technology – its capacity to make a difference. And, of course, these transformative effects extend across the network, not least to the actor that sent us the invitation.

Thus, objects participate in the action, but how do they do so? Here, Latour's (2005) arguments about the *nature of groups* and the *nature of actions* are relevant. Groups are made, or performed, that is, actors are given an identity, and there exist many contradictory ways for this to be done. In other words, collectives of humans and non-humans come to stand for something through a negotiated process which renders the group capable of being represented. Representatives for the group need not have human form. For example, most of us at some time have been represented by a graph, a spreadsheet or a set of statistics that makes claims about our needs, wants, performance and so on. Furthermore, policy decisions affecting a wide population may be made on the basis of such representations. The process through which hundreds, even millions, of people come to be represented by some cells in a spreadsheet – the way that interests are aligned, that exclusions are made, that enrolments are strengthened – these are the concerns that may be addressed by ANT. It is in this sense that Latour (1999a) argues that ANT is a method – a way to trace social connections using the trails left by the controversies about group formation. The issue of morality, and where it lies, is obviously raised by these examples.

Clearly, every course of action involves a great variety of agents which seem to barge in and displace the original goals so that we never know for sure who and what is making us act (Latour 2005). However, the major distinction is to decide whether the agency is treated as an intermediary or a mediator, which is not dependent on its figuration – in human or non-human form. Although objects have agency, their activity is only visible for a short while, before it recedes into the background – with technology, for example, as we get used to how it works. Introna (2007) suggests some ways of maintaining this visibility. We build on his suggestions in our conclusions. For now, we have highlighted the hybrid nature of entities and thus the view that artefacts, as well as humans, participate in the action in ways that may be morally desirable or not. This perspective addresses the question of the morality of objects, and in our particular case, the morality of information technology.

2.3   Our Methodological and Ethical Stance

Our outline of the nature of groups, actions, objects and the way they associate suggests that, in an empirical investigation to trace an actor network, the researcher needs to address three main tasks: i) to identify the entities involved without pre-judging their nature as mediators or intermediaries based on their figurations; ii) to examine the associations they make, bearing in mind that such assemblages may fail; and iii) to account for a difference in the resulting order in terms of new agencies, withdrawn agencies, etc.

To that end, we engaged with Facebook on a regular basis over a two year period. We carefully enacted and recorded the registration process and then continued to engage 'in site' through our networks, aiming to understand the potentialities of the site, for example, how privacy is enacted (or not). The ethical challenges presented by the site's arrangements became evident in our own activity with Facebook and in conversations we have had with other people who use the site. For one of the authors, engaging with Facebook was an ethnographic event. He immersed himself in the site as a lived experience, usually daily. In addition to data collected 'in site', we also considered narratives about Facebook in the wider world. Thus, we drew on news stories of flashpoints and challenges as reported in the press, on television and across the Web.

Methodologically, our approach requires openness to the view that objects have a mediating rather than an intermediary role (that is, an ability to transform rather than merely transport the meaning of what they carry). A key implication of this perspective is that if objects have agency, they also have a capacity for ethical behaviour – that is, they also have morality. Furthermore, a diverse group of humans and non-humans associate in any course of action, and agency and hence morality is diffused among them. So tracing intention and attributing purposeful action is a significant undertaking, particularly in an increasingly technology-mediated world in which computer programs that are inconspicuous to us may execute without our knowing and have effects that even designers could not predict in advance. In short, since agency is hard to trace, then so too is morality.

We use ANT as a method for tracing the actors, but they cover a lot of ground (so our actor network is large) and actors can only be traced when they are on the move (so *a priori* judgements of their intentions are not possible). Thus, which actors can be held to account for the consequences of social networking and what type of purposeful action can be taken, and by whom, are complex questions. In short, it is problematic to trace the interests, intentions and potentialities that come together in the process of social networking, and hence that it is simplistic to attribute responsibilities for its consequences to *a priori* determined categories of humans identified as designers, suppliers or users of particular Internet sites. In a paper such as this, we cannot hope to give a full account of all of the agencies involved in the use of social networking sites, and the ethical issues arising. Nevertheless, in the section that follows we explore the Facebook site, tracing some of the key moments that a user of the technology can experience, aiming to disclose the ethics of the technology so that they may come up for scrutiny (Introna 2007).

3 Disclosing the Ethics of Facebook

Facebook is a social networking site that was founded in the USA in 2004, by a Harvard University student, Mark Zuckerberg. The site initially targeted fellow students at Harvard but later expanded to include other universities, colleges and high schools. Initially users had to provide a university email address to register, however Facebook later expanded to workplace networks, and in September 2006 it granted access rights to anyone, regardless of affiliation. Facebook has over 400 million active users as at April 2010 (Facebook 2010). Below we outline some of the key interactions a user can have with Facebook – creating profiles, making friends, publicizing activity. We focus on the extent to which the operation of these applications is transparent to the user and the potential implications for those that are enrolled into the network. We acknowledge that the processes and features associated with a given social networking site will change over time and that some of the ethical issues we raise here might well have been dealt with by the time this paper reaches print. For us what matters is our main argument which concerns the role of technology and the resulting diffusion of ethical responsibility in such spaces.

3.1 Creating Profiles during Registration

Users[2] of Facebook must create a profile and they begin doing this during the registration process. A message on the Welcome page emphasizes Facebook's networking potential – "*Facebook helps you connect and share with the people in your life*" – highlighting scope to keep up with family and friends, share photos and videos, and reconnect with old classmates. The sign up boxes ask for the minimum information needed to set up your profile – name, date of birth, password and e-mail address – although it is not evident that you are doing more than registering at this point. You can ask why date of birth (labelled 'Birthday') is required, by clicking on the text "*Why do I need to provide this?*" underneath the 'Birthday' data entry point. A pop up message gives the reassuring reply:

> "*Facebook requires all users to provide their real date of birth to encourage authenticity and provide only age-appropriate access to content. You will be able to hide this information from your profile if you wish and its use is governed by the Facebook Privacy Policy.*"

Facebook's Terms of use for individuals require you not to "*create an account for anyone other than yourself without permission.*" However, the system does not validate a registrant's name, age or contact details when setting up a new user account. You automatically accept Facebook's Terms of use and Privacy policy (discussed later) by clicking 'Sign Up' on the Welcome page – there is no separate tick box to indicate that you have read and understood these conditions (Terms of use and Privacy policy are accessed via small text links on the Welcome page, and all other site pages, and together are over 10,000 words long).

Following 'Sign Up', Facebook asks you to confirm your email address by picking up a message from your email account and following the link it contains. This link directs you to the Facebook site. Here, a message informs you that someone/thing wants to add you as a friend. The Facebook application selects this friend. In the case of one of the authors, *Medics Index* wanted to be his friend. The author knew nothing of *Medics Index*, but accepted the friend request since he could not see any way to avoid it. On the next page, he realized that, in contrast to the large blue button for accepting whatever was being asked of him at that time, the word 'skip' appeared at the top of the page in small plain text, allowing him to decline particular requests. This page offered him the opportunity to find other friends, suggesting that he enter his email account details and password, if he had a Yahoo account or AOL instant messenger account. The application then accessed the address book of his email account, found people who were already users of Facebook, added them as friends, and gave him the option to invite others who were not Facebook users to join. The next screen prompted him to enter personal details, including the schools and universities he attended with dates, and the name of his current

---

[2] Here we refer to primary users – those who create an account. We are aware that secondary forms of user exist, such as those that may not have an account, but 'piggyback' on other users to access the system.

employer. A message states: "*This information will help you find your friends on Facebook.*" The next prompt asked him to join a town or city's network. These requests can be skipped, but it does require the user to identify this possibility. The interface draws you to the large blue 'submit' button rather than the distant 'skip' feature. At this point, the registration process is complete and the software directs you to your profile. In summary, users may not realize that they are creating a profile during this process, believing instead that they are merely registering for the system. Rather, they are populating their profiles with personal data and signalling initial agreement to privacy settings which are, by default, set for a high degree of openness (see the following sections for further detail on this point).

3.2   Enhancing One's Profile

A basic Facebook profile includes a number of hyperlinked sections which appear as discrete 'application blocks' on the user's page. The basic blocks are shown in Table 1. Aside from name, e-mail address, and user status, all data fields on Facebook may be left blank, so the creation of a very thin Facebook profile is possible. Profile details comprise what an individual is willing to enter into the system and make public, content generated by friends and content generated by Facebook applications. To friend with other members of the network, you need to action the "add to friends" application (by entering someone's surname and/or forename) to link your profile with others on the website. The application then searches the Facebook database of profiles. Users may 'friend' other things too, but we shall consider this in greater detail later. Users can also add applications to their profile to network and play with their friends. All applications require your permission to "*know who you are and access your information*". A message warns you against disabling this feature when installing an application, stating that "*Granting access to information is **required** to add applications. If you are not willing to grant access to your information, **do not add this application**.*" What is less transparent in this interaction is how these data will be shared. Potentially, applications are able to access diverse data for a huge user base (depending upon the popularity of a given application), and then share them with the developers of the application and those for whom they have developed it.

3.3   Sharing Content

The notion of making things public is central to the operation of Facebook. Thus, even though users may choose to be selective in what they share, it is important to consider the default settings that a new user will receive. When examining the privacy settings, we noted that the Facebook application gave every piece of information that could be shared the default setting of being permissible for sharing with 'only friends'. With the exception of the profile itself which must be set to allow access to 'only friends' or 'friends of friends', all other features of the system can be further customized to allow different people varying access to personal information. However this is a lengthy, complicated process. The only applications that have the option to render invisible to everyone in the drop down menu ('no one'), and thus give easy access to global privacy, are a user's online status and the wall. Even though one of the authors has used Facebook on an almost daily basis for two years, he has found few users adopting these settings. Thus, it seems that many users either find the privacy settings difficult or clumsy to use, or alternatively have not even considered the issue of privacy or do not believe it is an issue.

Beyond the access friends and friends of friends may have, there are broader issues regarding a person's visibility. Again, the application sets these by default to align with the spirit of openness. For example, a person's visibility in searches undertaken within and outside of the site is set to 'everyone', and upon profile creation Facebook automatically submits your profile to other search engines. In this regard, the display on the privacy settings page states:

> "*Your public search listing consists of your name and the thumbnail version of your profile picture. This listing will be shown to people who search for your name when they are not logged in to Facebook [i.e. when they are using external search engines]. Use your search privacy settings to control whether your public search listing appears in searches from Facebook's Welcome page or external search engines. Changes you make will take effect*

immediately on Facebook, but there may be a delay before search engines are updated as well."

This information is only made available by the application once users have registered and only then if they look at the privacy settings rather than taking up the many, and seemingly more interesting, invitations that the profile offers – to add applications, add friends, post content and the like. Thus, users may post content before they examine the fundamental workings of the site.

Table 1: Basic Building Blocks of a Facebook Profile

Block	Information It Can Contain
Information	Basic – age, gender, religious and political views; Contact – telephone, address; Relationships – your status and what you are looking for – you can link profiles with your partner here; Personal – details of hobbies and interests; Education – where you have studied; Work – current and past places of employment; Picture – a place to store pictures you want to use as your profile image.
Status	A place to write what a user is currently doing/thinking.
Friends	A listing of 6 of a user's friends and their profile pictures and a link to a page displaying all of your friends. The listing of 6 friends is randomized by a Facebook application.
Friends in Other Networks	A list providing an analysis of the networks you have friends in.
Photos	A list of user created photo albums generated via an application that allows a user to upload photographs to their profile. Photographs in which a user has been 'tagged' that are part of another user's profile are also listed here. Typically, a user adds a name (a tag) of those individuals who appear in the photographs. The tags attached to each photograph can be searched via a dedicated search dialogue box. Individuals do not have to give permission for their name to be used in the tagging process and if they want their name removed, they have to either remove it manually or request that their friend removes the photograph. Users cannot prevent other users from tagging them in photographs. There is also a facility to comment upon photographs. Non-users of Facebook can be tagged in photographs, but they cannot be searched for using the search feature.
Video	A facility to post videos to a profile.
Notes	A place to write notes and import them from other spaces on the web, such as blogs.
Groups	A list of Facebook groups a user belongs to.
The Wall	A bulletin board where friends can leave messages, notes, good wishes and other comments.

3.4   Publicizing Activity

Publicizing activity is a necessary part of networking on Facebook. Upon logging into your account, Facebook displays your home page. This is an administration page that informs you about activity that has taken place since you last logged on and acts as a reminder of notifications not dealt with in the last session. Such notifications include requests from friends and other members of Facebook, for example, to add an application that a friend has on their profile or to add a friend. The page also reports things other members have done to you, such as who has poked [virtually prodded] you (and invites you to poke them back) and gives a list of recent friend status updates. This latter activity data is time stamped by the application, which makes the data publicly available unless the users concerned have enabled particular privacy settings for the News Feed and Mini-Feed applications. A further application suggests other members of Facebook you might want to be friends with. This

feature was released in April 2008 and operates by making recommendations based on who you have friended already and who your friends have friended. While it is commonplace in online environments for applications to run automatically, monitor activity and send unsolicited messages to users, what Facebook does is to enable such processes to happen more rapidly, in a more *ad hoc* fashion, and for the results of such activity to be available to a wider audience.

Publicity can also be a problem for one's friends. For example, it is possible to install an application called 'Top Friends'. The application explains its purpose as: "*Show your friends some love! Add your BFFs [Best Friends Forever] to your profile! Each of your pals is just one-click away! No more searching through pages of friends just to check up on them. The only question now is: Who's in your Top Friends?*" The application requires you to select 32 people in your list of friends to become 'Top Friends'. Thus, the application invites you to play according to the norms of social networking activity – doing things with friends. When selected, the application places these 32 people in a block of their own on your profile page, thereby separating them from friends who are not deemed 'Top'. However, the application also has the facility to populate the 32 available spaces itself, automatically. You choose one of three approaches – taking a psychometric test, performing a test indicating how 'hot' your friends are, or opting for a random shuffle. In each case, the application draws upon another application to create the 32 Top Friends. Such delegation work complicates notions of friendship in that, for example, who you perceive to be a Top Friend may not be the one you believe is hot! The application also gives you access to your overall ranking in your circle of friends and this is displayed as a statement about your popularity such as "*people like you*". Applications such as this are often received by a user via an invitation from another user, since applications ask users to forward them to their friends. Often it is very difficult to see how you can choose not to do this. Furthermore, such invitations often contain standard unmodifiable text that plays upon notions of friendship and networking (see Figure 1). These publicly articulated, universalistic ideas about doing things with friends may be just play for some users, but can be threatening to others.
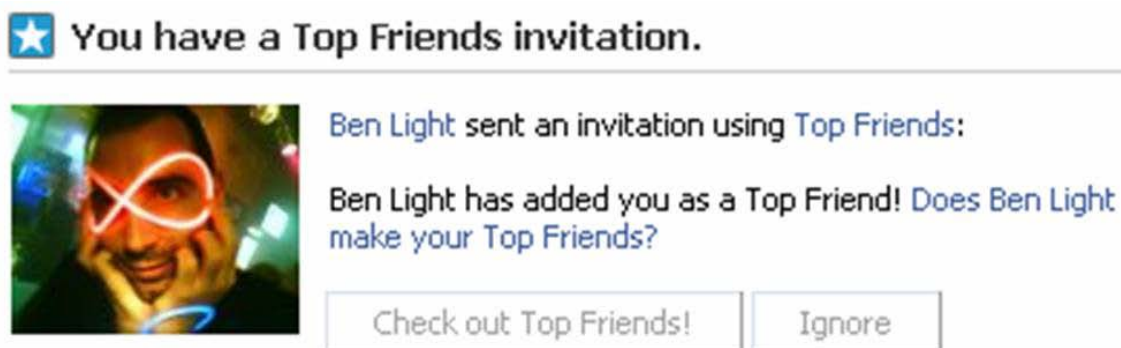

Figure 1: Example of a Top Friends Invitation

4   Discussion

Disclosing what happens in Facebook reveals many ethical issues. For the purposes of this paper, we identify these issues as concerned with privacy, security and identity arising out of the processes of creating and maintaining profiles, publicizing activity and the way that these data and images may be interpreted. Of course, these three areas overlap, are interconnected and in no way provide a complete disclosure (which of course is impossible).

4.1   Creating and Maintaining Profiles

By contrast with the way that YouTube enables users to manage privacy through the clever deployment of technological features (Lange 2007), we highlight how Facebook interweaves the creation of an initial profile with registration so that users may provide a good deal of personal data about themselves before they understand the consequences of their actions. In particular, we note that

the registration application defaults a user's privacy settings to a high level of openness. Once registered, of course, the user can change some of these settings to enable a greater degree of privacy, but our own and other research suggests that the default settings generally remain (Gross and Acquisti 2005; Sophos 2007). Indeed, users often think of such sites as safe and closed worlds where they can publish provocative and controversial material, unaware of the potential consequences (Donath 2007; Jagatic et al. 2007; Tow et al. 2010). Importantly though, there is more at work here than a user's more or less informed decision to publish. Once users are registered, they are instantly bombarded with pokes, friend requests, invitations from applications such as News Feed, Mini-Feed and search engine results. These invitations can seem more appealing and more pressing to deal with than the apparently mundane and time consuming backstage administration associated with configuring privacy settings. Even where users are interested in limiting access to their profiles, the way the site has evolved over the past few years has not always been helpful to this process.

For example, following the launch of a revised site in August 2008, the link named 'privacy' on the user's Welcome page was demoted to a menu that only appeared when you held a mouse over it (see Figure 2). This menu was labelled 'Settings' and appeared with a padlock logo next to it. In February 2010, the site was again revised in this area. The menu was labelled 'Account' and 'Privacy settings' became one of seven options to choose from on a drop down menu. The padlock logo (arguably a sign synonymous with security) was also removed. What we see is the ability to mediate privacy becoming more distant. By way of contextualizing this point, we note that the images shown in Figure 2 represent a very small area of the overall interface, which further obscures the path to mediating a user's profile. It has been interesting to observe the confusion experienced by users during these times of 'upgrade'. In the latest round of changes, Facebook has taken a staged approach (bundling the change with a more general review of the site's look and feel), which has meant that users were engaging different versions of the interface at the same time. Many people reported losing posts and, in one case we are aware of, their whole profile. The confusion brought about by the upgrade 'not working' meant that the software further mediated the environment in ways that were unpredictable – some posts never appeared, some appeared multiple times, certain actions were not possible and features did not work.
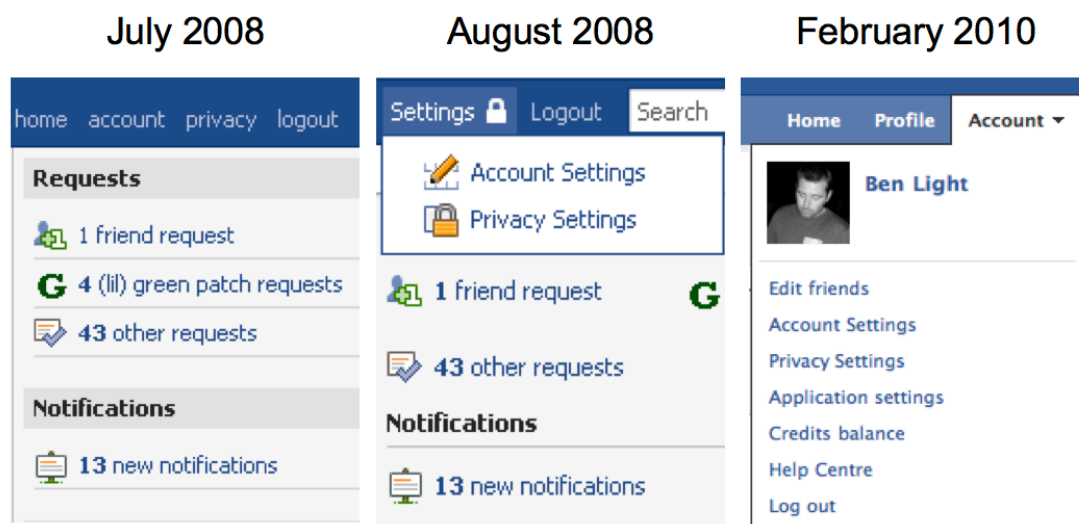

Figure 2: Privacy Interface Changes

Our findings also point to the indeterminate location of morality in such sites. The images in Figure 2 show Facebook's attempts to improve the user interface, but these efforts appear to have made it more difficult to manage privacy. Indeed, in August 2008, users may be been reassured by the message on

the opening registration page which stated "Use Facebook to … control privacy online". However, in February 2010 the message changed, downplaying the ability of the site to control online privacy and rather positioning it as enabling you to "connect and share with the people in your life". The above examples highlight the role of *technology as a mediator* rather than an intermediary (Latour 2005). In these cases information technology acts to make a difference; it does not simply transport the scripts of the developers or users of the network, it mediates intentions through the intensity of the experience it makes possible. One may argue that Facebook users and applications require and thrive upon openness of access to one another. However, this openness has consequences in terms of the public and private activities it enables, as we go on to discuss.

We highlight the lack of validation work by the Facebook registration application which presents users with an opportunity to create fake or bogus profiles affording them privacy – or more accurately anonymity. Such affordances need not necessarily be seen in a negative fashion. Fake profiles are often friended as informational objects – they are integral to identity work. For example, fans may friend a pop star, celebrity, politician or fictional character, knowing full well that they are not adding the genuine profile of that person or character (this is particularly the case for fictional characters!). However, such a lack of validation work during registration also allows for arguably less positive activity to take place. Given the prevalence of data about everyday people on the web due to the rise of blogs, organizationally based personal home pages and the like, it is relatively easy to create fictitious profiles about individuals or Facebook groups about them. These profiles and groups can be further enhanced by engaging software such as Photoshop to manipulate the digital images. The ends for such applications can be seen as part of the experience of playing with Facebook. Indeed, the Facebook Group application requires that users enter a reason for the group when they engage the software to create it. Often, when such groups are made about an individual, the criterion is 'Just for Fun.' Clearly though, the software has the potential to provide cover so that users can engage in cyberstalking and identity theft. Users can easily make a bogus profile to do both, owing to a lack of validation processes. In the first case, an anonymous profile can be created and then used for cyberstalking because Facebook does not, by default, record and communicate to a user who has looked at their profile. Identity theft is possible because users may friend non-human objects or fictitious characters and leave their privacy settings open. The actualities of the outcomes are obviously subject to how actors share, interpret and respond to the available content, but clearly the security of such sites is a significant issue, as several high profile cases have shown (BBC News 2010). Crucially, we have to remember that Facebook is part of a much wider network of actors – something not always accounted for in 'single site' studies of social networking. Indeed, the *nature of actions* (Latour 2005) is such that identities created in Facebook for a particular purpose may end up being negotiated in other different spaces of the Internet by actors we do not know and/or in ways we do not choose (Light 2009; Light et al. 2008).

4.2   Publicizing Activity

Facebook merges with various aspects of people's lives and allows different aspects of people's lives to merge with each other. Such merging is not new, however what we disclose is that Facebook accelerates and intensifies such processes, making them available to a wider audience as well as more difficult to manage. Many users of Facebook are not only affiliated with personal networks, they are enrolled in professional ones too. This has come about in light of mass media hype about social networking in general terms and as a vehicle for conducting work and, of course, because many of us work as well as play! Arguably, for many organizations, social networking technology, and social media more generally, have become obligatory passage points in their marketing efforts. For example, many universities have a presence on sites like Facebook and Twitter in order to keep in touch with current students and alumni; they may also use such arrangements to attract new business. In this way, members of staff that already have personal profiles in such spaces may be required to enrol in professional situations – this is our experience. Moreover, those that have registered personally, rather than for work purposes, may find that they are presented to coworkers by, for example, the recommendation software that Facebook now incorporates – because one of their friends works at the same place they do. Rather than reject a coworker's or manager's request to become a friend, they

may feel forced to accept someone into their network and, because of the ways in which Facebook mediates their activities, they may find that their profile constructs a particular view of them that they may not want publicizing in a work context. Our examples here relate to the *nature of groups* (Latour 2005), specifically the conflicting ways in which users can adopt an identity when they join the Facebook network. This identity work starts during creation of the profile, but it is subject to an ongoing series of requests and invitations from other members of the network in which the users and the technology constitute each other. Moral dilemmas can arise when users' personal and professional worlds collide with consequences they did not intend.

Indeed, as social networking sites evolve to mediate a variety of interactions, users increasingly stand the chance of applications revealing aspects of their lives to one another that they have kept separate for good reason. The problems we highlight are further compounded by the reproducability and network connectedness of the Internet (boyd 2008b; Ito 2008). For example, Facebook's software does not allow users to see who has looked at their profile or particular features of it. In this sense, Facebook presents itself as open to anyone without providing ethical guidance for its use in much the same way as unsecured domestic wireless networks offer themselves to, say, neighbours (Small 2007). Yet, such issues of publicizing activity are not restricted to the combining of work and home life. The role of the Top Friends application clearly highlights the difficulty of the mediated public articulation of friendship, particularly where the selection of 'best friends' is made by the application. Such applications make it difficult for users to be vague about the ranking of friends. These examples of being visible on Facebook show how the presence of your open profile can connect you with people you have not sought as friends, exclude you from groups in which you wish to play a part, and have reputational consequences that you did not even consider.

Finally, we argue that it would be simplistic to suggest that ethical responsibility rests solely with the developers of Facebook. The lack of validation functionality makes it easy to join Facebook and, arguably, some users with thoroughly benign intentions might be dissuaded from joining if registration were more cumbersome. Moreover, such functionality may have seemed unnecessary in the initial development stages of Facebook within the Harvard University environment before its rapid expansion on a global scale. As is well understood within Science and Technology Studies, the relationships between development and use are far from predictable and simple – we can only anticipate the ongoing design work put in by 'users as designers', particularly in Web 2.0 user generated environments such as Facebook. So, although gaining entry to this play space is easy, given the nature of the data sharing interactions it mediates, we argue that the issue is not simply about the morality of the designers, or the users, or even the technology itself, but of hybrid entities like the 'technology user' – the user whose goals are mediated by the technology, often in ways other than the designers intended (Latour 1999b). Consequently, ethical responsibility is diffused among those actors who engage with the site (such as programmers, marketers, and account holders) and the technology itself, where each of these entitites should be understood not just in the context of Facebook, but in the wider sense in which any particular SNS is connected to other spaces on the Internet and beyond. In the final section, we return to our research question to highlight the implications of our findings for the theory and practice of social networking.

5   Conclusion

To date a good deal of research on social networking sites has focused on how users domesticate them, thereby overstating the role of human agency. From this perspective, the morality of technology is a matter of the ends to which it is deployed by its designers and users; that is, ethical behaviour is a purely human concern. In this paper, we run counter to the tool view of information technology (Orlikowski and Iacono 2001) and a human-centric focus on ethics to argue that technology mediates (or transforms) the meaning of what it carries, and hence that technologies as well as humans have a moral character that can be opened up to scrutiny. We situate our research within a body of work on disclosive ethics (Brey 2000a; Brey 2000b; Introna 2005; Introna 2007) and engage the methodological potential of ANT as an empirical approach to tracing the actors and disclosing what they do rather than relying upon *a priori* judgements about the nature of right and wrong. To that end,

we provide a case study of Facebook which was conducted over two years, during which time one of the authors used the network on an almost daily basis.

We show that Facebook applications begin shaping the user experience at the very point of registration (and often before, for instance via an email invitation to join the network, the mention of the site in television and film, links with mobile phone advertising, apparel such as the 'I Facebooked Your Mum' range of t-shirts and, of course, other Internet sites). This influence increases 'in-site', where the default position of openness that applications require, combined with the outputs they produce, distract users from the seemingly mundane administration of privacy. Such activities, whilst a necessary and fun feature of Facebook, can place users in difficult positions, although the issues may only surface as they gain experience with the system or face challenges from another source such as friends, foes, potential employers, or even law enforcement agencies. In contrast to prior work, we point out that this is not just a matter of levels of user understanding about SNS or even an issue about the ethics of the designers of such spaces. Facebook applications are also actors in the process, with the potential to divert user attention from matters such as privacy settings and, indeed, to make it difficult – if not impossible – for users to create privacy even if they desire it. Consider how these applications shower users with invitations, requests and advertisements once they have signed up, even when they are still subject to the dangers of an open profile. Consider also how they enable other users to post photographs you are in, and tag (identify) you, even if they are not your 'friends', and even if you do not have a Facebook account, which means that you do not know such photographs have been made public – however embarrassing or compromising! Clearly, some of the consequences of these potentialities were not intended by the designers or the users of these sites. In the first instance, we aim to disclose the implications of some key moments in the user experience, but ultimately we seek an understanding of how actors constitute ethical behaviour in the transformations that take place. Our research to date suggests that such constitutions are diffuse and multiple.

We also show that while Facebook requires openness, it allows anonymity, sometimes simultaneously. Facebook's user validation process makes it easy to create fake profiles which contain applications that share data with other users. Whilst some users might friend fake/fictional profiles to create an image of themselves, the software does not provide the means to distinguish readily between 'genuine fakers' and those that seek to do harm, such as identity fraudsters. Consistent with our methodological approach, we avoided making moral judgements about the actors' motives *a priori*. However, as we progress to the next stage of our research, we suggest that further work is needed to understand how the actors are constituted in such cases, including questions that address the relationship between identity and ethical behaviour, and how power dynamics are understood and come into play in such situations.

To date, our work has been pre-theoretical in the sense outlined in our methodological and ethical stance. Like Brey (2000b), we see scope for a theoretical stage following our initial disclosures, but with less normative intent for applying its outcomes. We suggest that Foucault's ideas about ethics provide a contextually dependent notion of moral conduct that could be used to address the questions we raise above. Radically opposed to the Kantian view of rational, autonomous agents, who act according to moral codes determined *a priori*, Foucault's notion of the ethical subject (Foucault 1985) sees individuals as subjects enmeshed in a network of moral relationships, where ethical behaviour is a matter of judgement constrained by the power dynamics of a person's social circumstances. This network of relationships involves an ensemble of actors, procedures, institutions and mechanisms (technologies or *dispositifs*), which enable specific practices to be related in a particular type of discourse (Foucault 1980). From this perspective, ethical behaviour involves ways of acting that are not purely rational, but also emotional, and concerned with an aesthetic sense of how people want to live their lives. This art of living – or *aesthetics of existence* (Foucault 1985) – is constrained by how individuals perceive their opportunities within their milieu, that is, their capacity to act. Hence multiple constitutions of ethical behaviour are possible.

The perspective we describe holds promise as a means of gaining insight into the diverse population of Facebook users and the multiple roles in which any one user may access the site – as student,

employee, parent, teacher, partner, lover and so on. It also provides scope for understanding the different identities that individuals may have in different spaces on the Internet and the potential problems when such identities collide. Such a collective of humans and non-humans is evident in many social constructivist accounts of technology. Nevertheless, proponents of the ensemble view (Orlikowski and Iacono 2001) have varied in the extent to which they theorize or acknowledge the agency, and indeed the morality, of information technology. In conjunction with the methodological potential of ANT, we suggest that Foucault's perspective on ethics is a powerful way to address the diffuse and multiple notions of moral conduct at work in our case. In a space with such a high level of user involvement, we believe that this understanding is necessary for effective ethical intervention. Furthermore, given the scope within ANT to deploy the actors' vocabulary, and the new challenges in terms of immediacy and intensity of experience made possible by SNS, we suggest that further research along the lines we have outlined is, at the very least, likely to give rise to theory development in the form of new concepts. Comparative research may yield further important results, not least because the field is currently dominated by single site studies, which often generalize from findings that could be enriched, or indeed debunked, if compared across a range of sites.

Turning to the practical implications of our research, we suggest that using Facebook is about more than just making friends; it also involves making associations with a variety of other actors, some of which might not be of our choosing. Thus tracing agency – and hence a capacity for moral conduct – is a complex task, in which blanket policy recommendations requiring the designers of the Facebook site to clean up their act fail to recognize the diffuse nature of ethical responsibility. Our position here is informed by Latour's (1999b) example of a person holding a gun, in which he argues that the issue is not whether people are bad or guns are bad, but rather that we need to consider the entity of 'a person with a gun', that is, the way that a gun mediates the intentions of the person holding it with the consequent implications for how agency, and hence morality, is distributed among the actors. With this in mind, we are sympathetic to work suggesting that a few simple mechanisms could be used to remove some of the ethical ambiguity in online spaces (Small 2007) and provide a degree of ethical guidance – for example, the use of warning messages regarding postings (Ahern et al. 2007). Nevertheless, we argue that, no matter how carefully developers try to imagine use contexts and ethical scenarios during the design process, their efforts will be incomprehensive (Albrechtslund 2007). Our findings suggest the need for an ongoing process of evaluating social networking sites, to which our work contributes. Opening up such sites to scrutiny on a regular basis in a disclosive ethics approach maintains public awareness of the issues. Indeed, while social networking remains a 'hot' topic, researchers may find an audience for their disclosures in a range of media outlets as well as in their published work.

Other agents also have a role to play. For example, site users could lobby for safer transactions using the strengths of the technology to create momentum for a user group. Such efforts are clearly hampered by the proprietary nature of the technology, which restricts access to the code, but in their absence the designers can readily claim that the site is providing what users want. Research councils could also earmark funds for programmes that investigate the detailed operations of such sites. Indeed, Latour (2005) has argued that the visibility of objects is enhanced in the early stages of innovation – when they are approached by users made ignorant or clumsy by distance (in terms of time, space or skills) – and also in the face of accidents or breakdowns. Thus research programmes might study the development and use of technologies before they settle into place and become invisible, or in the case of an established technology, investigate the experiences of novice users. Similarly, flash points in the trajectories of such technologies may also prove useful sites of investigation, as in 2006 when Facebook users protested following the roll out of News Feed and Mini-Feed functionality. And as friends, colleagues and teachers, we can advise others on the workings of these sites. Through such engineering activism (Nissenbaum 2001) we may share the moral implications of information technologies and then strive for more visibility in they way that they function.

6   References

Ahern, S., Eckles, D., Good, N., King, S., Naaman, M. and Nair, R. (2007). Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Rosson, M.B. and Gilmore, D. (eds.), San Jose, USA, pp. 357-366.

Albrechtslund, A. (2007). Ethics and technology design. *Ethics and Information Technology*, 9(1), pp. 63-72.

Bahney, A. (2006). Don't talk to invisible strangers. http://www.nytimes.com/2006/03/09/fashion/thursdaystyles/09parents.html, Accessed 26 November 2007.

BBC News. (2010). Facebook murderer to serve at least 35 years. http://news.bbc.co.uk/1/hi/england/wear/8555221.stm, Accessed 6 April 2010.

Bell, F. and Adam, A. (2004). Whatever happened to information systems ethics?: Caught between the devil and the deep blue sea. In *Information Systems Research: Relevant Theory and Informed Practice,* Kaplan, B., Truex, D., Wastell, D., Wood-Harper, A.T. and DeGross, J. (eds.), Kluwer Academic, Boston, pp. 159-174.

boyd, d. (2004). Friendster and publicly articulated social networks. In *Proceedings of the Conference on Human Factors and Computing Systems - CHI2004*, Vienna, Austria.

boyd, d. (2006). Friends, Friendsters, and Top 8: writing community into being on social network sites. In *First Monday*, http://firstmonday.org/issues/issue11_12/boyd/index.html.

boyd, d. (2008a). Facebook's privacy trainwreck. *Convergence*, 14(1), pp. 13-20.

boyd, d. (2008b). Why youth ♥ social network sites: the role of networked publics in teenage social life. In *Youth Identity and Digital Media,* Buckingham, D. (ed.), MIT Press, Cambridge, pp. 119-142.

Brey, P. (2000a). Disclosive computer ethics. *Computers and Society*, 30(4), pp. 10-16.

Brey, P. (2000b). Method in computer ethics: towards a multi-level interdisciplinary approach. *Ethics and Information Technology*, 2, pp. 125-129.

Byrne, D. (2007). Public discourse, community concerns, and civic engagement: exploring black social networking traditions on BlackPlanet.com. *Journal of Computer-Mediated Communication*, 13(1), pp. 319-340.

CNET. (2008). Exclusive: the next Facebook privacy scandal. http://news.cnet.com/8301-10784_3-9854409-7.html, Accessed 7 April 2010.

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, 13(1), pp. 231-251.

Ellison, N.B., Steinfield, C. and Lampe, C. (2006). Spatially bounded online social networks and social capital: the role of Facebook. In *Proceedings of the 56th Annual Conference of the International Communication Association*, Dresden, Germany.

Facebook. (2010). http://www.facebook.com/press/info.php?statistics, Accessed 6 April 2010.

Fernback, J. and Papacharissi, Z. (2007). Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. *New Media and Society*, 9(5), pp. 715-734.

Foucault, M. (1980). Truth and power. In *Power/Knowledge: Selected Interviews and Other Writings 1972-77,* Gordon, C. (ed.), Prentice Hall, New York, pp. 109-133.

Foucault, M. (1985). *The Use of Pleasure: The History of Sexuality, volume 2*. Penguin, London.

Fox News. (2007). Creator of MySpace sex offender database is excop, Data Expert. http://www.sentryweb.com/articles/myspacefox.pdf, Accessed 28 October 2007.

Golder, S., Wilkinson, D. and Huberman, B. (2007). Rhythms of social interaction: messaging within a massive online network. In *Proceedings of the 3rd International Conference on Communities and Technologies*, Steinfield, C., Pentland, B., Ackerman, M. and Contractor, N. (eds.), Michigan State University, Michigan, pp. 41-66.

Griffiths, M. and Light, B. (2008). Social networking and digital gaming media convergence: Classification and its consequences for appropriation. *Information Systems Frontiers*, 10(4), pp. 447-459.

Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, Atluri, V., De Capitani di Vimercati, S. and Dingledine, R. (eds.), Alexandria, VA, USA, pp. 71-80.

Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication*, 13(1), pp. 276-297.

Introna, L.D. (2005). *Disc*losive ethics and information technology: disclosing facial recognition systems. *Ethics and Information Technology*, 7, pp. 75-86.

Introna, L.D. (2007). Maintaining the reversibility of foldings: making the ethics (politics) of information technology visible. *Ethics and Information Technology*, 9(1), pp. 11-25.

Ito, M. (2008). Introduction. In *Networked Publics,* Varnelis, K. (ed.), The MIT Press, Cambridge, MA, pp. 1-14.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), pp. 94-100.

Johnson, D. (2001). *Computer Ethics*. Prentice-Hall, Upper Saddle River, NJ.

Joinson, A.N. (2008). Looking at, looking up or keeping up with people? Motives and use of Facebook. In *Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems*, Florence, Italy, pp. 1027-1036.

Kendall, L. (2007). 'Shout into the wind, and it shouts back': identity and interactional tensions on LiveJournal. In *First Monday*, http://firstmonday.org/issues/issue12_9/kendall/index.html.

Kim, K.-H. and Yun, H. (2007). Cying for me, cying for us: relational dialectics in a Korean social network site. *Journal of Computer-Mediated Communication*, 13(1), pp. 298-318.

Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology*, 25, pp. 109-125.

Lampe, C., Ellison, N.B. and Steinfield, C. (2006). A Face(book) in the crowd: social searching vs. social browsing. In *Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work*, Banff, Alberta, Canada, pp. 167-170.

Lampe, C., Ellison, N.B. and Steinfield, C. (2007). A familiar Face(book): profile elements as signals in an online social network. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Rosson, M.B. and Gilmore, D. (eds.), San Jose, USA, pp. 435-444.

Lange, P.G. (2007). Publicly private and privately public: social networking on YouTube. *Journal of Computer-Mediated Communication*, 13(1), pp. 361-380.

Larsen, M.C. (2007). Understanding social networking: on young people's construction and co-construction of identity online. *Paper Presented at the Society for Social Studies of Science (4S) Annual Conference*, Montreal, Canada, October.

Latour, B. (1999a). On recalling ANT. In *Actor Network Theory and After,* Law, J. and Hassard, J. (eds.), Blackwell, Oxford, pp. 15-25.

Latour, B. (1999b). *Pandora's Hope: Essays on the Reality of Science Studies*. Harvard University Press, Cambridge, Massachusetts.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press, Oxford.

Light, B. (2007). Introducing masculinity studies to Information Systems research: the case of Gaydar. *European Journal of Information Systems*, 16(5), pp. 658-665.

Light, B. (2009). Gendering social media: shaping masculinities on Gaydar, Facebook and beyond. *Paper Presented at the 10th Annual Conference of the Association of Internet Researchers (AOIR): Internet Critical*, Milwaukee, USA.

Light, B., Fletcher, G. and Adam, A. (2008). Gay men, Gaydar and the commodification of difference. *Information Technology and People*, 21(3), pp. 300-314.

Liu, H. (2007). Social network profiles as taste performances. *Journal of Computer-Mediated Communication*, 13(1), pp. 252-275.

Magnet, S. (2007). Feminist sexualities, race and the Internet: an investigation of Suicidegirls.com. *New Media and Society*, 9(4), pp. 577-602.

Messerly, J. (2007). Disclosive computer ethics? *Computers and Society*, 37(1), pp. 18-21.

Nissenbaum, H. (2001). How computer systems embody values. *Computer*, March, pp. 117-119.

Orlikowski, W. and Iacono, S. (2001). Desperately seeking the "IT" in IT research - a call to theorizing the IT artifact. *Information Systems Research*, 12(2), pp. 121-134.

Petersen, S.M. (2008). Loser generated content: from participation to exploitation. In *First Monday*, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2141/1948.

Röhle, T. (2007). Desperately seeking the consumer: personalized search engines and the commercial exploitation of user data In *First Monday*, http://firstmonday.org/issues/issue12_9/rohle/index.html.

Rothberg, S. (2006). MySpace, Facebook and other social networking sites: friend or foe to employers? , http://www.interbiznet.com/ern/archives/060830.html, Accessed 3 May 2008.

Rothberg, S. (2008). Do employers really hire candidates from Facebook and MySpace? FurstPerson / Sprint does. http://www.collegerecruiter.com/weblog/2008/04/do_employers_re.php#more, Accessed 3 May 2008.

Small, L. (2007). Theft in a wireless world. *Ethics and Information Technology*, 9(3), pp. 179-186.

Sophos. (2007). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html, Accessed 1 April 2008.

Sweney, M. and Gosden, E. (2006). Facebookers protest over privacy. http://www.guardian.co.uk/technology/2006/sep/08/news.newmedia, Accessed 28 January 2008.

Tow, W.N.-F.H., Dell, P. and Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology*, 25, pp. 126-136.

Wellman, B. (1996). Are personal communities local? a Dumptarian consideration. *Social Networks*, 18(4), pp. 347-354.