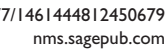
Article

new media & society
14(8) 1251–1268

DOI: 10.1177/1461444812450679
nms.sagepub.com



Identification and the practices of identity and privacy in everyday digital communication

Bridgette Wessels
University of Sheffield, UK

Abstract
The growth of e-services and social networking sites is generating popular online participation in which pre-digital ways of securing the privacy of individual identity are undermined. The characteristics of digital communication mean technology developers, policymakers, service providers and individuals are rethinking senses of identity, processes of identification and what privacy means in everyday life. To ensure that identity and privacy are respected in communication raises two issues. One, there is a gap between social context of communication practice and the technological feasibility of privacy tools. Two, the concept of privacy is not fully adapted and refined for use in the digital networked age. This paper outlines the way in which privacy in digital communication is being interpreted, and discusses the ways in which identification is a useful concept in developing knowledge and systems to support contemporary practices of privacy.

Keywords
e-services, identification, identity, privacy, social networking sites

Introduction

The growth of e-services and social networking sites (SNS) is generating online participation in which pre-digital ways of securing the privacy of individual identity are

Corresponding author:
Bridgette Wessels, Department of Sociological Studies, Elmfield Building, University of Sheffield, Sheffield S10 2TU, UK
Email: b.wessels@sheffield.ac.uk

undermined. The characteristics of digital communication mean technology developers, policymakers, service providers and individuals are rethinking identity, identification and what privacy means in everyday life. The focus on identity and privacy is important in ensuring that e-services and SNS are trustworthy (Cullen and Reilly, 2007; Dwyer et al., 2007; Fukuyama, 1996). This involves designing identification into services, supporting privacy policies and developing the informed and responsible use of e-services. The different perspectives from industry,[1] policy-service providers[2] and people[3] influence how identity and privacy is understood and addressed (Nissenbaum, 2004).

This paper draws on a project called 'Identity and Privacy in Digital Contexts' (IPDC), which explores perceptions of identity and privacy by technology developers, policy-service providers and people in everyday life. The structure of the paper is, first, the research context; second, a discussion of identity and privacy in communication; third, an overview of the research design of IPDC; fourth, a discussion of IPDC findings; and, last, the conclusion.

Context

There is consensus that privacy needs to be addressed in digital communication, taking into account the perspectives of developers, policy-service providers and ordinary people in developing interdisciplinary and intersectoral knowledge (RISEPTIS Group, 2010). A key issue is how to create concrete links between the social and technological aspects of privacy. Part of the process of aligning and integrating technological and social aspects of privacy and identity is identification. This, the RISEPTIS Group (2010) argues, needs to be understood contextually within the social relations of digital communication.

The analytical framework for exploring privacy and identity in e-services and SNS is based on the point that communication is located in the routines of everyday life (Silverstone, 2005b). In everyday communication people work with identification, senses of identity and privacy with varying levels of awareness. E-services and SNS span many domains, each with their own norms and values. This means taking into account the perspectives and practices of organizations and individuals in e-services. The two themes of the framework are the social relations of communication and the practices of communication. The social relations involve understanding the perspectives of actors that frame privacy and identity in digital communication, namely the computer industry, policy-service providers and end-users. These are explored in the research project and are reported below. The practices of communication involve questions of identity, identification and privacy in everyday digital communication, which is discussed in the next section.

The research landscape on privacy and identity is diverse. boyd and Hargittai (2010) within information studies address young people's work with privacy settings on Facebook. Brands (2001) focuses on privacy within infrastructures and methodologies for obtaining digital signatures within public-key cryptosystems. In relation to threats to privacy, surveillance studies scholars consider transparency and accountability in large-scale public and private systems (Edwards, 2005; Norris, 2009). These studies contribute

to knowledge about privacy in either design or end-user contexts but pay less attention to the links between the two. Computer-Supported Co-operative Work (CSCW) researchers undertake more integrative approaches by gathering perspectives from industry, policy-service providers and people in everyday life.

Ackerman (2000) argues that the social-technical gap[4] identified in CSCW work is especially problematic in linking the social and technological aspects of privacy online. Ackerman (2000) sought to use Altman's (1975) theory of privacy in developing privacy tools. Altman (1975) sees privacy as a process involving a rich palette of individual and social behaviour that defines privacy. Ackerman (2000), however, found that the level of abstraction in Altman's (1975) definition makes it difficult to apply to concrete design. Ackerman (2000) says that without 'concrete links' between social and technical understandings of privacy it is difficult to reconcile Altman's (1975) ideas with privacy systems. The difficulties of integrating design and use also affect the issue of aligning everyday communication practices with policy-service providers and industry approaches to privacy.

A characteristic of digital communication is that it is a many-to-many networked environment. Digital communication allows communication between people and across organizational boundaries – it is an open and dynamic way of communicating. It is the context for 'mass self-communication' (Castells, 2009: 63–70). This differs from mass media whose communication role opens up cultural democracy, but is a one-to-many model of communication based on hierarchical structures (Thompson, 1995). The difficulty of aligning technology design with people's everyday communication practices is significant because everyday practices are central in shaping online communication (Haddon, 2004). Furthermore, privacy is mediated through the interaction of digital technology, institutions and everyday communication practices (cf. Silverstone, 2005a).

Identity and privacy in digital communication

People's senses of identity interact with the ways they communicate in social networks. Lievrouw and Livingstone (2006) argue that research needs to address identities as well as the roles and practices of users. Scholars address the reflexive construction of self-identity, the fluidity of identity and individualization (Beck and Beck-Gernstein, 2002; Giddens, 1991). Some feminist writers undertake deconstructivist approaches to gender identity (Butler, 1990). Castells (1997) notes the meaningfulness of identity in negotiations of nationalisms, religious and cultural identities and gender and ethnic identities in global networked society. These approaches illustrate that identity is constructed and reflexive in late modernity. Jenkins (2002), however, identifies a 'black box' in identity studies. He points out that the relationship between individual unique identity and shared collective identity is left relatively unexplored, which results in gaps in 'how identity works or is worked, and of what it is' (Jenkins, 2002: 19).

The model Jenkins (2002) provides for identity is an: 'internal–external dialectic of *identification* as the *process* whereby all identities – individual and collective – are constituted' (Jenkins, 2002: 20, emphasis added). The interplay of internal senses of identity and external aspects of identity bridges the analytical gap between individual and

society, including that between the digital network and users. Identity holds attributes of embodied individuals, which are socially constituted, sometimes as a high level of abstraction, as seen in digital identity systems. The institutional order is part of a network of identities and routinized practices for allocating positions (i.e. identities) to individuals. The process of identification points to the way in which individuals seek to identify themselves with broad external markers such as norms, legal frameworks, cultural mores and social institutions in developing identity (Jenkins, 2002). Institutions, in turn, organize identity through the way in which their identification process operates in categorizing people. Jenkins (2002) argues that individuals continually craft identity out of sociality, institutional identification, private and public senses of selves, and, as Poster (1990) also notes, through communication.

Turkle (1985) argues that digital communication offers a way for people to represent themselves and think about their social and psychological selves. She asserts that the interface between computers and cyberspace symbolizes identity and social interactions. For instance, the Windows interface represents the fragmentation of the self in relation to different networks mediated through ICT, with each window situating individuals within specific sets of social relations. Turkle (1995) extends these ideas further by arguing that computers provide the basis for a reconsideration of human identity. Digital communication involves virtual and anonymous dimensions and offers opportunities for online identity play (Stern, 2004; Valkenburg and Peter, 2008). More recent research focuses on identity that is 'nonymous', which means that users are no longer anonymous and are identified and accountable in online communication (Zhao et al., 2008). These studies highlight the way online identity is a self-conscious activity. However, online identity is also shaped by the mundane practicalities of offline identity, everyday life and the routines of daily digital communication (Wessels, 2010). In these daily contexts identity and privacy, as mundanely understood, are negotiated in practical terms.

One aspect of practical online identity is that individuals have less control over what is deemed 'public' and 'private' (RISEPTIS Group, 2010). The lack of co-presence markers of identity (cf. Goffman, 1959) means that e-service-providers and e-service-users need to be authenticated so that identity can be verified. And in informal online communication participants use an array of resources to present and secure identity to develop trust and rapport in social networks (Wessels, 2010). Both of these processes mean that individuals and organizations share aspects of identity that intrude into the private sphere. Addressing identity as it is mediated through the social relations of communication points to changing social forms, such as networked individualism (Wellman and Haythornthwaite, 2002), which are part of an informational, mediated and surveillance society (Lyon, 2001).

Privacy is a complex and socially constructed phenomenon. The 'right to privacy' (Marwick et al., 2010) is protected in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It is part of modern democratic life (Westin, 1967) and it seeks to balance privacy with the rights and freedoms of others (European Convention of Human Rights, 1950). In the UK, the Human Rights Act (1998) gives individuals greater scope to use the law to protect their privacy. Article 8, for example, addresses the right to privacy for family and home life, and for correspondence. The right to privacy is constructed in the following domains:

- *Information privacy,* which involves the establishment of rules governing the collection and handling of personal data such as credit information, medical and government records.
- *Privacy of communications*, which covers the security and privacy of mail, telephones, e-mail and other forms of communication.
- *Territorial privacy*, which concerns the setting of limits on intrusion into domestic and other environments such as the workplace or public space.

It is difficult, however, to define the concept of privacy (Marwick et al., 2010). Solove (2002) argues that conceptualizations of privacy can be divided into six headings: (1) the right to be left alone; (2) limited access to the self, or the ability to shield oneself from unwanted others; (3) secrecy, or the concealment of certain matters from others; (4) control over personal information about oneself; (5) personhood, or the protection of one's personality, individuality and dignity; and (6) intimacy, which is to say control over, or limited access to, one's intimate relationships or aspects of life. These conceptual headings illustrate the overlap between 'rights to privacy' and the practices and areas of privacy. Solove and Schwartz (2009) argue that concepts of privacy are ambiguous, which relates to the way actors often create a practical understanding of privacy according to their cultural mores and social conventions (Cullen and Reilly, 2007).

To address the specific characteristics of privacy in digital communication, Nissenbaum (2004) argues for a contextual approach. She points out that traditional approaches to privacy such as limiting surveillance, restricting access to sensitive information and curtailing intrusion into private places do not have the analytical rigour to address the complexity of privacy in digital worlds. She suggests that attention needs to be paid to the concept of 'contextual integrity', which recognizes the rich and comprehensive parameters in which privacy is negotiated. She writes:

> The changing contexts of privacy due to digitization need to be analysed in terms of their governing norms of appropriateness and flow. This includes addressing the nature of information in question and its relationship to the context, the roles involved in the context, the relationships among the roles. (Nissenbaum, 2004: 153)

Fieschi (2007) expands this contextual approach by considering the role of privacy as a marker in sociability. Privacy is a marker that enables humans to 'thrive and survive through exchange and whose needs can be fulfilled through a form of interdependence that entails knowledge of each other and various forms of trust' (Fieschi, 2007: 33). She argues that the dichotomy posited by liberal political thought between the public and the private is outmoded because established spaces and boundaries are dissolving due to the networked flows of information via digital technologies. Fieschi (2007) proposes that a reconsideration of privacy as a regulatory mechanism between new versions of the private (including the personal) and the public could act as a tool to negotiate the fluidities of networks in digital communication. She models privacy in terms of its exchange value in that people exchange aspects of their privacy for services and other communication goods.

Nissenbaum's (2004) work highlights the fluidities that are emerging around understanding, defining and practising privacy in different contexts of communication. Fieschi

(2007) questions the way in which aspects of identity as privacy markers are exchanged in digital communication. The everyday contextual and exchange aspects of privacy are factors in exploring concrete links between privacy and identity in communication.

Research design of the IPDC project

An interpretive and inductive research approach was used to understand how policymakers, industry and people think about identity and privacy. The research included qualitative interviews, focus groups and document analysis based on purposive samples of policy-service providers, working people and students, and industry literature.

Policy-service providers

The sample is:

- Get Safe Online, the main internet safety-awareness-raising organization in the UK.[5] In-depth interviews were carried out at its office with its Heads of Policy, Public Engagement, and Communication to explore its public awareness strategy.
- The UK government's unit on privacy and digital services, the Information Commissioners Office (ICO). In-depth interviews and focus groups were conducted (at its office) with the Unit's three core civil servants, focusing on how to develop policy that is relevant to citizens and organizations.
- Twelve policy-service providers who were working on privacy in a regional public sector privacy strategy (UK). In-depth interviews (at the regional public sector office) were conducted to explore the issues of privacy in implementing public sector e-services; we undertook participant observation of six regional e-forum meetings on e-services and privacy (at its regional office).

The expert interviews with the policy-service providers were semi-structured and lasted one hour each (Meuser and Nagel, 2002). Respondent validation was undertaken by the researcher and respondents discussing the transcribed interviews (Kirk and Miller, 1986). The interviews were coded line by line (Charmaz, 2006) and analysed in terms of grounded theory. Coding, concepts and categories were reviewed by the project advisory group (Denzin and Lincoln, 2005).

The focus groups functioned as 'group discussions' (Blumer, 1969). These were used to explore the ways in which identity and privacy are understood, how opinions are formed about this area, as well as how some of the perceived problems might be solved. The group from the ICO are what can be termed a 'natural group' (Flick, 2009) because its members work together within the same unit. These focus groups were recorded and transcribed. The transcripts were analysed in the same way as the interviews.

The researcher had undertaking research of the regional e-forum for two years prior to the IPDC project. Her 'persistent observation' (Lincoln and Guba, 1985) over this period of time meant that she was accepted as a participant observer into the e-forums. The meetings were selected on agendas that were primarily focused on identity and

privacy in e-services. They were interactive and allowed the researcher to clarify some of the points made. These meetings were recorded and transcribed. The transcripts were analysed in the same way as the interviews.

Working people and students

The sample is:

- Twenty-four adults who are employed and are married/cohabiting with children (12 female and 12 male aged between 35 and 65 years; UK socio-economic classification B and C1). Four focus groups were undertaken (three females and three males in each), which addressed privacy and identity in everyday life. The groups were conducted at two regional community centres.
- Twenty-four students undertaking fulltime study who have family and friendship networks (12 female and 12 male aged between 19 and 21 years). Four focus groups were undertaken (three females and three males in each), which addressed privacy and identity in everyday life. The groups were conducted in rooms at the University of Sheffield.

The focus groups functioned as described above. The groups were artificial groups in that they were constructed out of a set of criteria − see selection criteria below (Flick, 2009). The groups were moderated by the researcher with steering topics that related to perceptions of communication, privacy and identity. The recording, transcription and analysis are as described above. The recruitment of working people was done through the regional public services research recruitment service and the recruitment of students was done through the Student Union's research unit. The criteria for selection were age, gender, socio-economic and cohabiting/married status, and single students in their second or third year of undergraduate study. The decision to use these groups was based on gaining an understanding of communication across a broad age range within two types of everyday lifestyles as contexts for everyday digital communication. These are: working and family life; and studying and single young people's lives.

Industry

The sample is:

- A selection of three technology developers based on reference rates in policy and industry documents (resulting in 20 documents) to identify key aspects of privacy discourse in product and policy development.

The document analysis (Scott, 1990; Wolff, 2004) of the grey literature provided insights into the way in which industry is formulating its thoughts about privacy and identity. The documents gathered are classed as official and open published documents (Scott, 1990). The analysis was based on an interpretative approach to documentary analysis. This means that the documents were considered in terms of their focus within

a particular community and thus they were considered in relation to their wider context, which in this case is the computer industry. The analysis consists of identifying the key themes of industry debates and identifying where the current state of knowledge lies in this sector.

The 'quality of qualitative research' (Seale, 1999) was addressed in the following ways. First, University Ethical Approval was gained. The participants were fully informed about the project, and they were given consent forms to sign and told that their participation was confidential and anonymous. The data and analysis were reviewed by the advisory broad in order to keep the problem of 'selective plausibilization' at bay (Buhler-Niederberger, 1985). Internal validity was checked by discussion with research participants as well as the advisory group. External validity was checked in two European Union e-forum workshops, a regional public sector e-forum and private sector workshop, and a user group forum. Direct quotations by lay participants are included in the text as these voices are not represented in policy or industry documentation. Policy service-providers' perspectives are paraphrased as well as directly quoted as they represent group consensus. The analysis of the grey literature is mainly represented by summary reports of published documents; quotations from publications are used to illustrate particular issues.

Findings: aspects of design, policy and use in e-services

System Design Perspectives

Cameron (2005), working from a computer industry perspective, finds that digital identity exists in a world without synergy because of identity silos. He notes that enterprises and governments prefer one-offs to help them maintain control and individuals often overlook safety in return for convenience and/or to appear 'cool' as well as lacking awareness of privacy issues. To counter these types of silos, Cameron (2005) suggests developing a digital fabric, which involves:

> *digital identity:* a set of claims made by one digital subject about itself or another digital subject;
> *digital subject:* a person or thing represented in the digital realm which is being described or dealt with (devices, computers, resources, policies, relationships);
> *claim:* an assertion of the truth of something, typically one that is doubted or disputed (an identifier, personally identifying information, membership of a given group, or a capability) (see Cameron, 2005 and www.identityblog.com/stories/2004/12/09/thelaws.html).

To ensure privacy and transparency, the computing community argues that people need control over information that is shared about them, and that sharing should be done on the principle of minimal disclosure for limited use, with the sharing of identity restricted to justifiable parties (Atkinson et al., 2007). Digital identity systems need to limit the disclosure of identifying information to parties who have a necessary and justifiable place in any given identity relationship (www.identityblog.com/stories/2004/12/09/

thelaws.html). In terms of an identity fabric, as a unifying identity meta-system, the human user is a component in human–machine communication: identity is a 'thing' on the desktop that individuals can see, inspect, add and delete (Cameron, 2005). Cameron's approach operationalizes identity within computer systems. It recognizes institutional aspects of identification amongst identities, subjects and claims in communication. There is less focus on the process of identity and identification.

The social and contextual aspects of privacy systems are considered in the policy discourse of identity management. Fishenden (2005) argues that 'identity and electronic identity are key issues for e-commerce and for public e-services' (Fishenden, 2005: 529). He claims that 'identity spans many different contexts and purposes: for example, individuals have multiple individual identity relationships (e.g. one with their employer, one with their banks, several with the many different parts of government)' (Fishenden, 2005: 532). These are role-based identities related to individuals' current employment or position and group identities ranging from families through to companies. From this view, identity is context-sensitive and multi-dimensional. Fishenden's approach does not, however, emphasize the way identity is a process of identification between internal senses of self and external definitions of selves.

These perspectives show that attention is being paid to the security of communication and to the protection of individuals and their data. Each demonstrates an awareness of the complexity of the identity–identification–privacy relationship. They consider identity, roles and contexts, and produce technological and managerial solutions. The ICO, however, raises the issue that securing privacy and identity in online communication requires going beyond managerial and technological solutions to address digital communication in the flow of everyday life.

The ICO civil servants' consensus is that 'most people have busy everyday lives and therefore have only limited time (and interest) to manage their digital identities'. The civil servants jointly state that a 'balance needs to be struck between how much people should be protected online and how much people should protect their own identity and privacy'. A key area from the ICO policy perspective is to consider how technology can be used in a less privacy-evasive way. The ICO's argument is based on the premise that service providers do not need to know *who* a person is, they only need to be able to *identify* the individual as 'xxxx' in order for the participating actors in the transaction to access, account for interaction, and identify the actors.

The ICO sees this as an issue of identity assurance (IA). They see the logic of IA as one that enables navigation through an information maze. Authentication is part of this system, in which identity can be strongly authenticated to the point where an identity claim can be verified with a high degree of reliability or, conversely, can be weakly authenticated. The optimal strength of authentication depends on the nature of the transaction. If an identity system is a necessary part of the digital communication, then the question of whether the authentication mechanism properly balances reliability with privacy protection arises (ICO focus group consensus). Within IA there is some recognition of a contextual integrity of privacy with its varying levels of authentication according to the character of the transaction. However, people's identity and roles are reduced to online identification markers rather than identity and identification as process.

Policy-service provider perspectives

From the point of view of policy-service providers, a system based on laws of identity and authentication is important in developing services. Regional policy-service providers, however, argue that it is important to understand that identity and privacy cut across technology, social issues, policy frameworks and services, as well as personal responsibility. A director of ICT Strategy and Services expresses this view by arguing for 'integrating digital responsibility within citizenship – as the rights and responsibilities of citizens and the state'. This raises the issue of how to integrate the way people manage identity meaningfully with the ways policy-service providers manage identity in services.

One of the policy-service providers argues that 'the use of entitlement cards would address the management of privacy from service provider and citizen points of view'. He points out that 'we don't really need to know who the person is, just that s/he is entitled to be on the system and undertake whatever transaction'. This approach tends to mould itself on a transactional model in which the focus is on identification and not people's perceptions of identity, roles and responsibilities. The abstraction away from people's senses of identity in relation to services may limit the development of trust and responsibility in e-services. This is significant because the regional policy-service providers stress that the basis of trusted services is a confidence that data and identity are protected.

Industry and policy-service provider perspectives recognize that people undertake different transactions that have different levels of privacy embedded within them. This is seen in terms of a rational actor model rather than by people in their everyday culture. The ICO perspective points out that contemporary celebrity culture and sensationalist media reporting blurs public and private domains. The ICO argues that this trend and the growth of SNS when combined with a lack of knowledge about people's communication practices makes the development of privacy policy difficult. These observations link to the difficulty of setting a regulatory framework because there is no one 'perfect consumer' on which to model policy.[6] One way to overcome some of the difficulties noted by the ICO in ensuring people manage their privacy in everyday practices is through raising public awareness of the risks of digital communication.

Get Safe Online[7] undertakes public awareness programmes that focus on people's responsibility for securing privacy in digital communication.[8] Its research (2007) shows that 88 per cent of internet users have some form of internet security software, such as a firewall, up-to-date anti-spyware or anti-virus protection. However, Get Safe Online (2007) also finds that many internet users are unwittingly exposing themselves to new areas of risk. Get Safe Online finds that one in four of the 10.8 million people across the UK registered on social networking sites posted confidential or personal information, which makes them vulnerable to identity fraud. The organization's director says:

> The popularity of social networking and other sites means that we are much more open about ourselves and our lives online. Although some of these details may seem harmless, they actually provide rich pickings for criminals. Your date of birth and where you live is enough for someone to set up a credit card in your name. So, whilst most people wouldn't give this information to a stranger in real life, they will happily post it online where people they don't know can see it.

These observations underpin the organization's mission to raise awareness that personal details and representations make information available about an individual's identity to other people, which can be used in various ways.

The perspectives of policy-service providers highlight three main concerns: first, the requirements for developing IA in digital communication; second, the decisions service providers face in deciding how to model access to e-services; and, third, how broader cultural change and everyday practices of communication are generating a changing environment in which the boundaries of privacy are negotiated. Underpinning these observations is the priority that systems need to be perceived as trustworthy to ensure a transparent, secure and well-used communication environment. Technological and service responsibilities are linked with responsible use of digital communication by members of the public. The question of how to link system and use is still unclear. There are still gaps in knowledge about how people practically understand their identity and privacy in mundane communication practice. The next section describes the way people understand and practice identity, identification and privacy.

Everyday life

Working people

The respondents use email, Skype, online shopping, online banking, eBay, online doctors' appointments and they use online communication to organize travel and surprise events for the family. The respondents agree with what one respondent says, which is that 'there is not a typical user – there is diversity across the population' (female health worker, 35), and this is also recognized by the ICO. All the respondents feel that 'online is the way to engage' in social life and that it helps them to organize their offline lives. It is therefore 'key to get a feel of online communication, but this is not part of your identity' (35-year-old male, teacher). The construction of an online identity is seen as part of having an online presence, and online identity is defined as having a range of different passwords, pin numbers and access codes – thus being part of the digital identification system – rather than a form of individual or social identity.

The participants feel that online information is private but agree that there are different levels of privacy, with online chat having little privacy when compared to online banking which is encrypted on several levels. One participant comments that:

> I think about whether the information I exchange online is private, in particular any details surrounding banking and finance, which I always try to keep secure and private. I consider this to be different from information I share with friends and family, and I sometimes post on open forums on social networking sites where anyone can read my comments. However, there are also some communications with my friends and family that I like to keep more private, and so will send a personal email or communicate via a hidden group on a social networking website which is not accessible by anyone else. However, this is not as secure as I would keep my internet banking details, which I do not divulge to anyone. (male retail worker, 52)

Another participant says that, to protect privacy, he has 'two accounts and two online identities – Mr *** @**.**, which has my name and is personal, and a coded account

that isn't personal acy@8***.**'. He expands on his strategy by saying: 'for instance, if I want to write to the local paper I will use my anonymous account, although my identity can be traced through the service provider' (male retail worker, 43).

There is a good basic understanding of security issues, with general agreement with one participant's observation that he is: 'aware of varying levels of security. I use a browser well known for its security features and keep it updated often. I constantly update all antivirus and firewall programs at the first opportunity' (teacher, 59). However, many of the participants note that managing security is complex, one woman (retail worker, 37) stating that she has:

> Numerous passwords and pin numbers (over 10). These passwords are managed only in my brain but use varying clues to remind me if I were to forget. I prefer to have a different one for each account as then I am able to discover which account may have been compromised and change just that one password rather than having to change all of them and running the risk of all my accounts being compromised.

One woman (health worker, 56) says that she has 40 passwords and the only way she manages them is to put them on a spreadsheet. Another participant also says that he uses 'an Excel spreadsheet to keep all my passwords and pin numbers on' (part-time retail worker, 64). A male teacher discussed the security issues of protecting schoolchildren such as not putting photographs of named students on the school website. Although the participants try to find methods to manage privacy and security, there are times when, as one woman (teacher, 53) says: 'I can be a bit blasé at home about privacy, relax with a glass of wine, and look for a holiday online, without thinking about security.'

In general terms, the participants agree that passwords are necessary to keep certain information safe, for example when banking online or using online store and service cards. They all agree with the participant who says that you 'need to look for the padlock for security' and learn to encrypt too. The participants think that: 'Any system is only as good as the people who use it.' They feel that most people would benefit from being informed about the risks and benefits of online communication, and that 'we can learn but we need to keep up, as things keep changing'. One woman (health service manager, 49) comments that there are 'lots of advantages to online communication systems – it's convenient, flexible, and so on' and feels that these advantages outweigh some of the risks to privacy. She is taking an exchange approach to privacy as noted by Fieschi (2007). There is ambiguity about privacy among the respondents in that they take security in financial transactions seriously but in informal communication they are less concerned with privacy. Only one respondent protects his privacy and personal identity by having two email accounts, whereas the other respondents are more concerned about managing their online identification processes.

Students

The students use SNS for communication and to organize their social lives. They use Facebook (FB) to keep in contact with friends who live locally to arrange social gatherings and to keep in touch with friends who live further away. They explain that many events like birthday parties are organized through FB.

In general terms students see 'social networking as accessible identity'. They consider 'social identity as the overarching identity that we associate with' and that 'identity is important in enabling you to stand out from others'. They say that they think about their virtual identity on SNS, but not about all the other various virtual identities they have in other online environments, such as banking, health and shopping. One student articulates a common understanding among them about identity online, which is a distinction between:

> FB [where] you can put your own interests, you can make up your age; you can put whatever online, in a sense you have a FB identity and a real identity. You also have a banking identity, but in this context questions are asked, and it is personal to enter your online account and view bank details.

Another student suggests that 'you have different identities depending on whom you are engaging with, and what you are doing – it's multifaceted – different ways of interacting with different people'.

The students show a variety of responses to the issue of privacy. As a group they did not think about privacy in general terms: for instance, one student says, 'privacy is not really an issue, not thought about it'. However, when addressing specific questions they show that they do consider aspects of privacy. For instance, one student says, 'privacy is important in bank details, in disclosing personal information on FB'. Identification is understood primarily as a way of accessing sites and securing data: for example, one student says, 'you do have mechanical ways to protect your own data, such as pin-locks on mobiles, and computers and laptops all have passwords'.

Many of the students see similarities in the way they practise privacy in the online and offline world. For example, one student says, 'you are selective with what you choose to disclose to people depending on the closeness of your relationship – what to tell different friends about the different aspects of yourself'. Students say that 'offline and online issues of privacy overlap as you are conscious not to tell people information that you don't want on FB – information travels much faster now FB is so widespread'. They comment that they are 'more likely to be private now due to online banking fraud and potential employers looking on FB'. However, this was not the case for everyone. One student says, 'I don't think about anything privacy issues-wise – I'd need someone to possibly "hack" my account before I seriously consider privacy'.

The students want to protect 'personal issues, such as who you are dating, when you are going out, tagging pictures, and going places'. Many students say they take emails off, set profiles to private, and delete history. Two students say, 'we both consider privacy – neither of us has personal details such as telephone numbers, addresses, etc. on FB'. Student consensus is that some people feel pressured to put personal information on because FB provides such an option. Two female friends say that 'privacy is very important' but vary in how they manage it. One says that her profile is only visible to her friends, whereas the other says that she has hers open to anyone in the network.

Another student raises the point of 'privacy in terms of contact – we want to have control over who contacts us, e.g. spam, unsolicited friend request'. Another student noted that there are also threats to privacy through some of the tools such as the Friend

Finder tool. Students pointed out that this tool is good for finding friends (full names/common names) but it also allows anyone to contact you. There is consensus among students that 'despite being able to restrict privacy settings, your identity is never entirely private on social networking sites – there is always a way people can find something about you' (male student).

In general terms, students think that 'online privacy is offline commonsense in online social networking' (female student). They feel that 'privacy is invaded on FB' and assert that: 'you need a level of knowledge and awareness of what you can do' (male student). One male student feels that 'we are the generation of hit and miss about privacy – awareness − knowledge', which was supported by the other students who reached a consensus that they have a lack of understanding about the management of privacy and the management of identity.

Conclusion

Identity, privacy and online identification are dealt with in the flow of everyday life. Working people and students see online identification as a means to access e-services and SNS; policy-service providers see it as ascertaining eligibility for e-services and authentication of service-users; and technology developers consider identification technically in designing privacy systems. What has emerged from the data is the existence of a gap in knowledge of how identification links people's internal senses of identity with external senses of networks and privacy in both technological and social terms. Working people do not see themselves as having an online identity; rather, identification markers are used to secure personal data. Students are more concerned with how they develop an online identity and a credible reputation than with online identification protocols. Policy-service providers understand identity in terms of entitlement and people's roles in privacy systems, and seek to educate people to self-manage identity and privacy. They do not relate this to identification as a process and as a way of continually crafting identity within e-services. Technology developers see identity as a digital fabric made up of the components 'digital identity', 'subject' and 'claim' to enable secure communication across networks. They do not address the way identification as a social process could link the aspects of a digital fabric, which may support a more dynamic and intuitive technological solution. To summarize, the groups of the social relations of communication understand identification in a mechanical way, rather than being part of a process of identity. The gap between technological and social aspects of identity and privacy occurs at the conceptual level of identification understood in sociological terms.

There is ambiguity about the way identification links with identity in digital communication. This relates to the way people practise identity and in how they understand public−private boundaries. If identification becomes understood as involving an 'internal−external dialectic' (Jenkins, 2002) between system and users, then senses of context and exchanges of privacy will be more transparent and accountable. However, currently, everyday users do not explicitly relate identification with the internal and external process of identity in communication practices. Industry and policy-service providers also do not focus on the social process of identification as part of identity. Understanding the relationship between the internal and external aspects of identity in

online contexts would inform the design of concrete links between social and technological understandings of privacy and identity. The main recommendation of this paper is that sociological understandings of identification should be explored in relation to identity and privacy in digital communication.

Further research is needed to address how aspects of privacy are exchanged in relation to senses of identity through identification. This requires deconstructing online identification and its relation to the process of identity, and designing this process and practice into technological systems. Case study research needs to support this to address the everyday contextual aspects of privacy. Research needs to be located within a multidisciplinary research team with strong connections to actors in the social relations of communication. This means links with industry, policy-service providers and lay people. A further recommendation is that the specialist knowledge of legal privacy experts and identity studies experts should be included in these types of research teams and partnerships. This would help to ensure that the different perspectives are integrated into consumer products, service provision, online safety policy and general public awareness. Attention should be paid to ensuring research findings are fed into public awareness campaigns.

Some progress is being made in terms of the main recommendation, in that it is being addressed in the EU-funded STORK 2 project.[9] This project addresses contexts of identity and identification. For example, the way youth workers in their career paths give consent to be authenticated in the context of creating 'safer chat' for young people. Another example is professional identification processes for authenticating qualifications in transnational careers. Other areas include the way young people represent their identity in social enterprise web services, which they validate through identification processes; and the way young mothers understand identification in web support services for returning to work and how that relates to their sense of identity in self-help groups. These examples cover self-identity and professional identity, social and technological identification processes, policy-service frameworks, and privacy technologies within different contexts of online privacy.

Funding

The project was funded by Sheffield University Devolved Fund (no. 305863).

Acknowledgments

The author wishes to thank the anonymous reviewers for comments that helped improve the paper.

Notes

1. Technology developers are situated in industry in this project; the terms are interchanged in the text.
2. Policymakers and service providers were working closely in this field at the time of the study, and are called policy-service providers in this study.
3. Lievrouw and Livingstone (2006) argue that the term 'people' is an advance on the term 'user'. Using the term 'people' rather than 'user' in social science and engineering evokes human interests, concerns, knowledge and rights. They argue that it seems odd to talk about the civic potential of audiences, the rights of users, or the creativity of consumers. On the

other hand, using the term ‘people’ captures their individuality and collectivity; the word is neutral about their abilities and interests but advances their needs and rights and takes plurality and diversity for granted.

4. Researchers from the CSCW field point to the difficulties of linking user requirements with the design of technically feasible products and services. They call this the social−technical gap. For many this is seen as the intellectual challenge to CSCW in which the gap is to be addressed in theoretical and empirical terms.
5. Other organizations are not directly relevant and some were not established at the time of the project: the Child Exploitation and Online Protection Centre (CEOP) focuses on child protection; specialized programmes such as the North West Grid for Internet Safety were not established until 2009, the UK Council for Child Internet Safety (UKCIS) focuses on children and was formed in 2008, UK Safer Internet Centre started 2011; the Internet Watch Foundation (1996) addresses child sexual abuse and obscene adult content on the web.
6. There are also different cultural contexts: for instance, Austria has a federated ID system and Belgium has a centralized system, whereas there is popular resistance to any type of identity card in the UK.
7. Its perspective is that, although industry and governments have some responsibilities, personal responsibility is also vital − both in terms of technology solutions (e.g. anti-virus software), and also in terms of behaviour (e.g. understanding the risks involved in adding personal details to a networking site, and the benefits of actively using privacy settings rather than relying on defaults).
8. The Get Safe Online campaign started in 2005. It is a joint initiative between government and the Serious Organized Crime Agency (SOCA) and private sector sponsors from the technology, retail and finance sectors. Its primary aim is to educate, inform, and raise awareness of internet security issues amongst consumers and micro-businesses (companies with less than 10 employees and sole traders). Since the end of the project cross-cutting public awareness agencies are being established. For example UKCISS (with a special remit for young people) seeks to link the spheres of the environment.
9. The precursor to STORK 2 is: https://www.eidstork.eu/index.php?option=com_processes&; act=list_documents&s=1&Itemid=60&id=312

References

Ackerman MS (2000) The intellectual challenge of CSCW: the gap between social requirements and technical feasibility. *Human-Computer Interaction* 15(2): 179–203.

Altman I (1975) *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole Publishing.

Atkinson S, Johnson C and Phippen A (2007) Improving protection mechanisms by understanding online risk. *Information Management & Computer Security* 15(5): 382–393.

Beck U and Beck-Gernstein E (2002) *Individualization*. London: SAGE.

Blumer H (1969) *Symbolic Interactionism: Perspective and Method*. Berkeley, CA: University of California Press.

Boyd D and Hargittai E (2010) Facebook privacy settings: who cares? First Monday 15(8). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/3086/2589 (accessed February 2011).

Brands SA (2001) *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA: MIT Press.

Buhler-Niederberger D (1985) Analytische Inducktion als Verfahren qualitativer Methodologie. *Zeitschrift fur Sozologie* 14: 475–485.

Butler J (1990) *Gender Trouble: Feminism and the Subversion of Identity*. London: Routledge.

Cameron K. (2005) Laws of identity. Available at: www.identityblog.com/stories/2004/12/09/thelaws.html (accessed May 2010).
Castells M (1997) *The Power of Identity*. Malden, MA: Blackwell Publishers.
Castells M (2009) *Communication Power*. Oxford: Oxford University Press.
Charmaz K (2006) *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. London: SAGE.
Cullen R and Reilly P (2007) Information privacy and trust in government: a citizen-based perspective from New Zealand. *Journal of Information Technology and Politics* 4(3):61−80.
Denzin N and Lincoln YS (eds) (2005) *Handbook of Qualitative Research*, 2nd edn. London: SAGE.
Dwyer C, Hiltz SR and Passerini K (2007) Trust and privacy concerns within social networking sites: a comparison of Facebook and MySpace. In: *Proceedings of AMCIS 2007: Reaching New Heights*, 10−12 August, Keystone, CO. Red Hook, NY: Curran Associates.
Edwards L (ed.) (2005) *The New Legal Framework for e-Commerce in Europe*. Oxford: Hart.
Fieschi C (2007) An open society depends on individuals rediscovering the social value of privacy. Demos, UK Confidential Report. Available at: www.demos.co.uk/publications/ukconfidential (accessed May 2010).
Fishenden J (2005) eID – Identity management in an online world. In: *European Conference on e-Government*, Antwerp, 16−17 June. Reading: Academic Conferences Ltd, pp. 529–540.
Flick U (2009) *An Introduction to Qualitative Research*. London: SAGE.
Fukuyama F (1996) Trust still counts in a virtual world. *Forbes*, 2 December.
Giddens A (1991) *Modernity and Self-Identity in the Late Modern Age*. Cambridge: Polity Press.
Goffman E (1959) *The Presentation of Self in Everyday Life*. London: Penguin.
Haddon L (2004) *Information and Communication Technologies and Everyday Life*. Oxford: Berg.
Jenkins R (2002) *Social Identity*. London: Routledge.
Kirk JL and Miller M (1986) *Reliability and Validity in Qualitative Research*. Beverly Hills, CA: SAGE.
Lievrouw L and Livingstone S (2006) *The Handbook of New Media*. London: SAGE.
Lincoln YS and Guba EG (1985) *Naturalistic Inquiry*. London: SAGE.
Lyon D (2001) *Surveillance Society*. Buckingham: Open University Press.
Marwick E, Diaz DM and Palfrey J (2010) *Youth, privacy and reputation*. Harvard Law School Public Law and Legal Theory Working Paper Series No 10–29. Cambridge, MA: Harvard University.
Meuser M and Nagel U (2002) Expertlnneninterviews – vielfach erpobt, wenig bedacht. In: Bogner A, Littig B and Menz W (eds) *Das Experteninterview*. Opladen: Leske and Budrich, pp. 71–95.
Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119–158.
Norris C (2009) *A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe*. Brussels: European Parliament.
Poster M (1990) *The Mode of Information: Post-Structuralism and Social Context*. Cambridge: Polity Press.
RISEPTIS Group (2010) *Trust in the Information Society*. Brussels: European Commission and ThinkTrust.
Scott J (1990) *A Matter of Record: Documentary Sources in Social Research*. Cambridge: Polity Press.
Seale C (1999) Quality in qualitative research. *Qualitative Inquiry* 5(4): 465–478.
Silverstone R (2005a) The sociology of mediation and communication. In: Calhoun C, Rojek C and Turner BS (eds) *The Sage Handbook of Sociology*. London: SAGE, pp. 188–207.
Silverstone R (ed.) (2005b) *Media Technology and Everyday Life in Europe*. Aldershot: Ashgate.
Solove D (2002) Conceptualising privacy. *California Law Review* 90: 1087.

Solove D and Schwartz P (2009) *Information Privacy Law*. New York: Aspen Publishers.
Stern SR (2004) Expressions of identity online: prominent features and gender differences in adolescents' World Wide Web home pages. *Journal of Broadcasting & Electronic Media* 48(2): 218–243.
Thompson JB (1995) *The Media and Modernity: A Social Theory of the Media*. Stanford, CA: Stanford University Press.
Turkle S (1985) *The Second Self: Computers and the Human Spirit*. New York: Simon & Schuster.
Turkle S (1995) *Life on the Screen: Identity in the Age of the Internet*. London: Phoenix.
Valkenburg PM and Peter J (2008) Adolescent's identity experiments on the internet: consequences for social competence and self-concept unity. *Communication Research* 35(2): 208–231.
Wellman B and Haythornthwaite C (eds) (2002) *The Internet in Everyday Life*. Malden, MA: Blackwell Publishing.
Wessels B (2010) *Understanding the Internet: A Socio-Cultural Perspective*. Basingstoke: Palgrave.
Westin AF (1967) *Privacy and Freedom*. New York: Athenaeum Press.
Wolff S (2004) Analysis of documents and records. In: Flick U, Kardoff E and Steinke I (eds) *A Companion to Qualitative Research*. London: SAGE, pp. 284–290.
Zhao S, Grasmuck S and Martin J (2008) Identity construction on Facebook: digital empowerment in anchored relationships. *Computers in Human Behaviour* 24(5): 1816–1836.

Bridgette Wessels is Director of the Centre of Interdisciplinary Research in Socio-Digital Worlds and Senior Lecturer in Sociology at the University of Sheffield. Her current projects are: mainstreaming telehealth (ESRC and TSB); participating in search design: a study of George Thomason's Newsbooks (AHRC); augmenting participation in the arts (DCMS and KT). Her books include *Inside the Digital Revolution: Policing and Changing Communication with the Public* (2007) and *Understanding the Internet: A Socio-Cultural Perspective* (2010).