Jones, S. (2017) "Doing Social Network Ethics: A Critical, Interdisciplinary Approach" *Information Technology and People*, Vol 30, Issue 4. [Author accepted final manuscript] https://doi.org/10.1108/ITP-04-2016-0093

# Doing Social Network Ethics: A Critical, Interdisciplinary Approach

Dr Simon Jones
Department of Computer Science, Middlesex University

## Purpose
This paper proposes an inter-disciplinary approach to the ethics of social networking services (SNS) that connects critical analysis with the *doing* of ethics in terms of both pedagogic and technological practice.

## Methodology/Approach
Primarily conceptual and discursive, drawing on theoretical concepts from a broad, inter-disciplinary field. These concepts are integrated into a multi-dimensional framework that proceeds through four sequential stages; socio-economic, ethical, legal and practical/professional. Particular instances of SNS are used as illustrative examples.

## Findings
The evaluation of ethical issues can be enriched by broader, holistic approaches that take account of the socio-economic, technical and legal contexts in which SNS technologies are designed, deployed and used. Inter-disciplinary approaches have the potential to generate new connections and possibilities for both the teaching and the professional practice of ethics.

## Practical implications
Applied ethics are used to consider practical solutions that explore regulatory measures and envision alternative models of social networking. The approach proposed has practical value for teachers and students of computer ethics, as well as for IT practitioners.

## Originality/value
This paper synthesises elements from media, communication and cultural studies, science and technology, information systems and computer science. The paper offers a strategy of inquiry to understand various aspects of SNS ethics—legal, socio-economic and technical. It presents a methodology for thinking about and doing ethics which can be used by IT practitioners.

## Keywords
Social Networking Analysis, Ethics, Socio-Technical Theory, Privacy, Surveillance, Power, Legal Aspects of IT, Practice.

# 1. Introduction

Social Networking Services (SNS) continue to attract a high level of attention across academic disciplines, amongst students, teachers and researchers alike. This paper considers some of the ethical issues raised by SNS, and offers a framework for teaching and thinking critically about these issues. The paper begins by reviewing some existing approaches to SNS ethics, and considers their respective strengths and shortcomings. The remaining sections combine elements of these approaches into an inter-disciplinary framework comprised of four key stages; the social and economic context in which SNS are designed and implemented, the

ethical issues arising from these contexts, legal and regulatory issues, and practical solutions and alternatives. This paper focuses on some, but not all, ethically problematic aspects of SNS, particularly privacy and transparency. It also looks beyond the customary topics of ICT ethics to open up other, less visible but equally profound issues around power, freedom and exploitation. The paper focuses on a particular mode of SNS, best exemplified by Facebook which remains by far the most popular social networking platform in term of active users, globally (Greenwood et al, 2016). This paper follows boyd and Ellison (2008) in defining SNS as web 2.0-based online communication platforms that allow their users to construct a profile within a bounded system, and to share connections with others.

## 2. Theorising SNS

A significant body of the academic literature about SNS is concentrated in the fields of *communication, media and cultural studies*. This work has explored a range of culturally specific and socially differentiated uses of SNS. Studies have looked at the significance of SNS as forms of computer-mediated communication used to create new kinds of "networked publics", particularly amongst young people (boyd and Ellison, 2008). The question of "identity" and the ways in which personality formation are shaped through digital self-expression and disclosure have been a major focus (Eiselauer, 2013; Mehdizadeh, 2010; Suler, 2004). SNS are seen as sites of online performance through which digital personae are constructed and manipulated (Brake, 2014). A recurring theme in this work has been the relation between online and offline sociality. A key question has been whether SNS have enriched offline social practices, identities and relationships, or detracted from them (Van Dijk, 2013; Turkle, 2011). Much of the research in these fields offers a broadly positive reading of the empowering, participatory potential of SNS. By blurring the boundaries between public and private space, it is argued, SNS have opened up possibilities for identity (re)formation and cultural creativity amongst their users (Papacharissi, 2011).

This body of work has been critiqued, however, for over-emphasising the extent to which SNS technologies are open to different meanings and uses (Lovink, 2011). Such uses are more shaped by economic structures and technological practices than is suggested. The technological and computational systems that underpin SNS are often taken as given, without calling into question their mediating role (Van Dijk, 2013). What is missing from these accounts are the power relations involved in the ownership, operation and control of SNS, and the unequal distribution of material benefits that flow from them. Critics have argued that the content production of SNS users represents a form of unpaid labour from which monetary value is created (Fuchs, 2014). A further problem with many critiques of SNS in the humanities and social sciences generally, is that such studies rarely connect their analyses to the practice of designing and implementing technical solutions or alternatives. When considered from the perspective of teaching future practitioners and professionals, this is a major limitation.

Much of the discussion of ethical issues around SNS has taken place in fields such as *computer ethics* and the *philosophy of technology*, where SNS is covered in many of the core textbooks (Baase, 2013; Quinn, 2010; Reynolds, 2012; Tavani, 2013). The standard approach in computer ethics is to evaluate morally problematic uses of Information and Communication Technologies (ICTs) through the lens of different ethical theories and moral philosophies. The main theoretical resources used are virtue ethics and variants of kantianism, consequentialism and utilitarianism (Jones, 2016). Ethical dilemmas are also considered from the perspectives of legal compliance and adherence to professional codes of

conduct. Computer ethics tends to be clustered around established topics such as privacy, security, free expression and intellectual property. Standard approaches to SNS ethics tend to focus on instances of unethical behaviour, such as identity theft, fake profiles, online abuse, hate speech, cyberbullying and various forms of predatory sexual behaviour.

In focussing on these more visible *uses* and *abuses*, standard approaches to computer ethics can miss some of the ethical implications embedded in the properties and features of technologies themselves (Brey, 2010). While ICTs may function increasingly without human intervention, they are nevertheless human-made artefacts, designed for specific purposes, to achieve particular goals (Johnson, 2009). Technology design always occurs within specific social, economic and historical contexts (Nissenbaum, 2010). Engineering and design decisions involve judgements about what is important, and what is not, and, as such, have an inherently ethical dimension (Friedman et al, 2008; Stahl et al, 2014).

Fields such as *Science and Technology Studies* provide ways of thinking about technologies and understanding how people and ICTs interact and co-shape one another in mutually constitutive, non-deterministic ways (Johnson, 2009). Values get baked into computer systems at each stage of the technology development lifecycle. Requirements, for example, are defined in reference to imagined potential users, and shaped by prevailing assumptions about their desires and capabilities. The interpretation of these requirements informs notions of usability and shapes interface design. "Choice architectures" shape the decisions that users are able to make by privileging certain defaults, and presenting users with a particular order and structure of options (Thaler and Sunstein, 2007). Values are embedded in the most detailed, fine-grained code, in class libraries and objects that name and model real-world phenomena, and in rules and patterns of reasoning inscribed into algorithms (Fuller, 2008).

In all these ways, ICTs play a configuring role. Different technologies have inherent material functionalities and "affordances" which constrain the ways they can be used, by delimiting the conditions of possibility for actions with them (Hutchby, 2001). Some of these affordances are consciously engineered into technological artefacts by their designers. Technology developers and marketers seek to impose certain preferred meanings on ICTs, and to constrain the range of possible interpretations open to their users (Hutchby, 2001). Technologies are therefore always accompanied by particular *discourses* which frame the ways in which they are represented and experienced. These processes have an ideological dimension. They work through modes of thought, concepts and representations which present aspects of social existence as unchangeable and universal (Hall, 1982). Ideologies become naturalized, disguising their underlying premises, and hiding vested economic and political interests. In doing so, they help to reproduce and legitimize power relations and inequalities.

In the field of SNS, ideologies work in this way to "naturalize" particular technological arrangements, architectures and interfaces. These appear as fixed and unchangeable, rather than being a function of conscious design and implementation decisions. The task of critical discourse analysis is to identify such ideologies, deconstruct their assumptions and partial narratives, and reveal how they maintain relations of power and dominance. This involves prising open the disparities between the publically-stated policies of SNS providers and their concrete actions (Stahl, 2008). It also means exploring how preferred uses are contested, and how the conceptual models of SNS designers can clash with those of their users. This work also entails scrutinising ideologies that are circulated through popular media in various narratives, mythologies and "moral panics" about SNS. This means cultivating an awareness

of how some SNS issues are driven by sensationalising media coverage which "blames" SNS for causing morally problematic behaviour.

Ethical analysis, then, involves making visible or "disclosing" (Brey, 2010) the values, priorities and interests that are embedded in ICTs. Ethical issues emerge where core ethical principles and rights are at stake, or are violated, by the design, implementation or use of ICTs (Jones, 2016). As a necessary prerequisite to such ethical analysis, however, SNS technologies first need to be situated within a broader social and economic context. A critical analysis of SNS has to be grounded in an understanding of the economic drivers, strategic goals and business models of the major corporate actors in this field.

# 3. Contextualising SNS

The SNS market is dominated by a handful of privately-owned global corporations, of which Facebook is by far the largest, with 1.44 billion active monthly users (Facebook, 2015). Facebook's primary strategic goal is to deliver a financial profit and return on investment to its major corporate shareholders and investors. Senior managers and executives are responsive to the interests of these shareholders and investors (Skeggs and Yuill, 2016). Facebook is an oligopoly that exhibits many traditional strategies of media conglomeration. These can be observed through its acquisitions and diversifications into related telecommunications and digital entertainment services, and its various partnerships with other media and technology companies. Facebook has a particular business model. Its profits are derived from selling financialized stock, extracting rents and commissions from micro-payments and transactions that occur through its platform, and from various deals and tie-ins with third parties. Facebook serves as a gateway for numerous secondary providers of goods and services who piggyback on its platform, and from whom it takes a proportion of revenue (Skeggs and Yuill, 2016).

Central to Facebook's capital accumulation model is advertising, which accounted for 93% of its revenue in the first quarter of 2015 (Facebook, 2015). Facebook provides advertisers with cost-effective opportunities to identify and target specific groups of consumers. Working through its network of user affiliations, recommendations, opinion formers and sponsored pages, advertisers have the opportunity to shape the perception of their products, services and brands (Turow, 2011). In this attention economy, advertising costs are determined by precise metrics. These can include the size and type of ad, the number of clicks per ad, the numbers of ad or page views, click through rates, and the size and characteristics of the target group.

The engine of this value creation, and the chief commodity in the SNS business model, is the activity and content of users themselves. Data about users is gathered in different forms, and at several different points (Scheier, 2015). *Service data*, for example, is given at the point of registration, including name and age. *User-disclosed data* includes posts, messages, comments, photographs, and communications between users, while *incidental data* is information posted, created or uploaded by other users. *Behavioural data* about users' activities and habits is acquired through activities such as tagging, rating and liking. *Derived data* is data inferred from all the above categories, for example a user's sexual orientation inferred from the identities of their friends. *Transactional data* is captured from online purchases and forms. *Metadata* may include data about the device used to access a platform, such as its IP address, operating system, date and time of page requests, and other unique identifiers. Such metadata might also include data about media files such as uploaded

photographs. *Location data* is data acquired from mobile-phone applications and platform features.

These data streams also extend to user activity outside of the Facebook platform through their interactions with affiliated sites and services. Facebook maintains profiles of non-users, compiled from the contacts of already-registered users, tagged photos, and other external information obtained from third parties. As the company has expanded horizontally and vertically, so these data sources have expanded. The shift towards single logins with a common user ID has enabled Facebook to access personal data from across its various services and platforms. Taken together, these data streams form a detailed record, or "digital footprint" of users' online activities. Access to this data is sold not only to advertising companies, but to a range of third parties that include direct marketing companies, retail and financial corporations, fundraisers, political parties, and large data brokers. Together, these make up a vast data analytics and profiling industry (Schneier, 2015). Personal data derived from disparate sources is aggregated then analysed for intelligence about consumers. This enables users to be targeted with granular precision based on standard demographic variables such as age, gender, income and geographical location, as well as other metrics, such as religious and political affiliations, sexual orientation, relationship status and education level. Content is then filtered and personalised for various different consumer types and lifestyle groups, not only in advertising, but also in news and entertainment content, and political campaign messages (Turow, 2011; Rubinstein, 2013).

The economic drivers that comprise this business model prioritise key operations and fundamentally shape the constituent technologies of the Facebook platform. Through the activities of programmers, engineers and designers who create and maintain that platform, they are materialised in particular algorithms, protocols, interfaces and network architectures. This entails the construction of an environment in which usage activity can be tracked, stored, assessed and monetised at every point. From the point of registration onwards, users are continually prompted to fill in more background details and add more depth to their profiles. On creating a new profile, the visibility of personal information is set to open, and searchable both within and outside the platform. The use of anonymous or pseudonymous identities is prevented by the requirement to register with real names. Privacy settings are made available only after users have registered (Light and McGrath, 2010). Facebook has stealthily and incrementally made more personal data openly available by default. Interfaces configure navigability and options by rendering certain icons, links and buttons more prominent than others. Choice architectures work to steer and cajole users along preferred pathways.

Facebook profiles have a particular standardised content architecture that serves to contain user activity within tightly structured, non-optional templates. Personal characteristics, tastes and preferences are broken down into a set of discrete data points which facilitate data extraction and quantitative measurement (Dainow, 2016). This content architecture maps onto recognised formats and standards in the digital advertising industry, standards which have been developed to gauge the success of online advertising expenditure and optimise returns on investment (Gehl, 2014). These include the standardisation of advertisement sizes, shapes, types and behaviours. The power of advertisers, as Facebook's primary customers, is materialised in the data-processing metrics used by the company which have been shaped in response to the needs of advertising networks (Gehl, 2014).

The flow of information within the platform is controlled through protocols and algorithms which pre-format user activity into a set of scripted and computable actions. These include

ranking and filtering mechanisms built into protocols for handling these actions and syndicating data between devices and platforms. Proprietary machine-learning algorithms pre-select the content seen by users in their feeds by ranking messages and updates according to user affinity and relevance (McGhee, 2013).

Various tracking technologies are used to gather and monitor users' clickstream data, include robot software, cookies and web beacons. Cookies remain one of the most pervasive inter-site tracking technologies in SNS. While traditional cookies typically log passwords and user names, pages visited, and various user actions within a webpage, they have been joined by a newer generation of "flash cookies." Also known as Local Shared Objects (LSOs) "flash cookies" are so-named because they are used on websites where Adobe's Flash Player is required in order to view multimedia content. They store data on a user's computer and can be used to track that user's internet activity, but they are generally harder to identify, manage and delete than browser-based cookies (Sipior et al, 2011).

Once retrieved from a user's device, such cookie data can be shared across advertising networks that may consist of affiliate sites and services numbering in the thousands. Beacons are typically small invisible graphics embedded in a webpage, typically one pixel in size and containing blocks of code. They are designed to track users on a particular page and transfer cookie data to advertising networks (Turow, 2011). Plug-in applications, such as Facebook's "like" button, create a two-way link between a third party or application and a user's profile data. This becomes a channel for "sponsored" news stories which are fed through to the user and their friends. It also enables the "liked" party to collect profile data from the user and from those in their network. Facebook is thereby able to track its users across any of the millions of external websites that have installed the button, whether they are logged into the platform or not, and whether they are active Facebook users or not. Features such as instant personalisation also facilitate the sharing of profile data with Facebook's various business partners, while its Application Programming Interface (API) provides third parties with a means to extract structured data from the platform, and develop applications for it.

The data streams that circulate through SNS platforms have been expanded not only through the integration of location data from smartphones, but also through wearable personal sensing devices such as fitness monitors and health trackers. These provide additional means for inferring details about the physiological state, activity and location of individuals. Wireless and geo-spatial technologies enable personal data from previously offline behaviour to be incorporated into SNS (Turow, 2011). Location-based social networking applications, for example, provide new opportunities for advertisers to reach people in the physical world by featuring products and services in close proximity to them. As SNS become integrated with a range of sensors and intelligent objects embedded in everyday social environments, the potential for this kind of ubiquitous collection of personal data has increased.

These developments have resulted in an exponential increase in both the quantity and qualitative detail of harvested data. The ability to make sense of this data requires the deployment of data mining and analytics tools. For these tasks, SNS providers use their own computational tools and bespoke data analytics systems. These allow different streams of data to be processed and analysed, for knowledge to be extracted, and for various correlations and patterns to be discovered.

The large-scale processing and storage of data that is involved in these content delivery and distribution systems depends on a particular network infrastructure. The recording of user

activity and personal data requires the maintenance of server activity logs and access records, and the retention of vast data archives of textual, photographic and video data.
Taken together, these technologies and business processes amount to mass commercial surveillance that is specifically designed to facilitate the storage, aggregation and analysis of personal data by platform operators and their third-party clients (Dainow, 2016). These technology deployments and business priorities, however, also have a discursive dimension. They are supported and legitimized by a specific set of ideologies. In Facebook's case, these can be identified in the company's public relations output, statements by its CEO, and in its various terms of service, privacy and data use policies. These act to construct subject positions for users. These positions are comprised of social connections, tastes and consumption patterns through which users are prompted to express preferences and rank services, products and people. A close inspection of Facebook's various policies reveals certain recurring themes and discourses. The notion of "sharing" for example, is a dominant theme articulated in public pronouncements by CEO Mark Zuckerberg, and in the company's mission statement "to give people the power to share and make the world more open and connected" (Facebook, 2016a). A close reading of Facebook's policies, however, reveals an elision between the virtues of sharing personal information between users, and sharing information with third parties, the latter being a euphemism for the capturing and selling of users' personal data (Van Dijk, 2013). Targeted advertising is not something that can be turned off or disabled in any of its settings. The rationale for data collection and tracking is to allow users to be served with tailored, localised ads that are "more relevant" to them (Facebook, 2016b).

# 4. Evaluating SNS Ethics

***Privacy*** has been identified as the issue of greatest public concern amongst users of SNS (COMRES, 2016; Rainie, 2016). It is an issue that has received extensive coverage in academic discussions of SNS. Most studies agree that privacy is an inherent human right and core ethical value. Privacy represents a space of autonomous thought and action that needs to be protected against interference and unwarranted intrusion by others (Clarke, 2006). However, what privacy actually means, in the context of SNS, has been the source of considerable debate. Privacy is a fluid, multi-dimensional category that can be approached from various social, psychological and philosophical perspectives (Clarke, 2006).

Much of the discussion of privacy issues regarding SNS has focussed on information disclosures between individual users. Users' privacy concerns typically revolve around the reputational damage arising from such disclosures, particularly from the fact that photos, comments and conversations intended for limited audiences can quickly proliferate in an uncontrolled manner (boyd and Ellison, 2008). A common point of departure in many studies is the "privacy paradox". This refers to the discrepancy between concerns articulated by SNS users about online privacy in general, and the apparently low value attached to privacy implied by their actual behaviour (Hull, 2015). One explanation for this paradox is that participants treat SNS as public not private spaces, and often make sophisticated evaluations and trade-offs of their potential intrusiveness against the perceived benefits of free services (Burkell et al, 2014). Nissenbaum (2010) suggests that privacy expectations and limits are governed by context-specific norms of appropriateness. Privacy violations occur when these norms are breached. This tends to occur where personal data that is presumed to be "private" is in fact publically shared in ways that have not been agreed to. Privacy, in this sense, is the right to control and limit the flow of personal information.

Most theories of privacy in the mainstream literature on SNS are premised on informational, control-based definitions. Here, loss of privacy means a loss of power to control how one is presented, and of the ability to make free, autonomous choices. However, this conceptualisation of privacy, some critics have argued, reduces privacy to an individual, interpersonal issue (Hull, 2015). Proposed solutions to such issues invariably revolve around enhancing privacy awareness amongst users. They often focus on users modifying their self-disclosure behaviour and making better use of privacy settings. By doing so, such proposals tend to echo Facebook's own privacy regime which places the responsibility for privacy management on the individual user. By focussing on user-to-user privacy issues, such approaches tend to overlook issues that arise from the service provider-to-user relationship. Facebook's privacy settings allow users only to select which information is visible to other users. Users cannot select which data to show to advertisers. Advertising is therefore excluded from being a considered a privacy issue.

What is absent from these discussions of privacy are the social and economic power relations between citizens/consumers, and private corporations and state institutions. The distribution of privacy rights in these relations is fundamentally asymmetrical (Andrejevic, 2007). Privacy, in this view, is inseparable from questions of property in modern capitalist societies (Fuchs, 2014). In dominant neo-liberal discourses, privacy is upheld as a universal value for protecting private property interests. In the ICT sector, it is used to defend ownership claims on intellectual property such as archived data, patents and proprietary software. Privacy is also invoked as a right to keep corporate information about wealth and profits secret and shielded from public knowledge. Thus while private corporations and government agencies have gained considerable amounts of privacy, individuals have lost privacy. The ideology of privacy helps hide and legitimise these power asymmetries and inequalities. Surveillance works to protect the privacy of dominant groups, while being used as a form of disciplinary power against citizens, workers and consumers (Fuchs, 2014). In this light, privacy represents a set of *collective* rights to be defended and protected from both corporate and state domination. It is an intrinsic ethical value in its own right, one that should not be trumped by security, and or given up for free online services.

A major focus of privacy concerns has been the access to SNS data by government and state agencies, including law enforcement, immigration and border control, security and intelligence (Schneier, 2015). The Snowden revelations revealed the nature and extent of this access, most notably the existence of systems which involve the bulk collection of internet metadata through covert surveillance programs. Such blanket forms of surveillance grant unrestricted access to personal data in ways that not only infringe the privacy rights of individual citizens, but result in the general erosion of freedoms and liberties for all. The knowledge that surveillance is occurring has been shown to have a restricting and intimidating effect on people's online activities, thereby undermining freedom of expression and association (Marthews and Tucker, 2015).

While the threat to privacy posed by *state* surveillance is widely recognised, less attention has been paid to that posed by *commercial* surveillance, and by the relationship between the two. Corporate and state surveillance have been shown to support each other in a public-private partnership that involves collaboration between multiple state intelligence agencies, private security companies and corporations (Schneier, 2015). Government surveillance piggybacks on corporate capabilities, enabling the state to access quantities of personal data on a scale that most nation states cannot generate. In some instances, corporations work willingly with state agencies, through arrangements which may involve payment to access bulk surveillance

data. In other instances, SNS companies are commandeered by law to hand over data through subpoenas or high court orders. Where no agreements exist, agencies can tap into network infrastructures covertly through back-door systems (Schneier, 2015).

***Transparency*** is a key enabler of privacy, and a foundational ethical principle that underpins core values of honesty, trust and integrity. Transparency is a fundamental prerequisite for justice, accountability and the right to know, allowing citizens to know both "what is going on" and "what is going wrong" (McBride, 2014). Transparency has a particular resonance for ICT. It was James Moor who first drew attention to the ethical implications of the "invisibility factor" implicit in computer technology (Moor, 1985). Moor's observation that the operations of most computer systems, due to their complexity, are hidden from view to most people most of the time, remains as pertinent as ever in a digital world that is increasingly pervaded with unknown entities gathering unknown information for unknown purposes. Many of the technologies that underpin SNS operate in the background. The techniques by which personal data is collected, logged, tracked and analysed are increasingly opaque. How this data is used, by whom, and what value is extracted from it, are impervious to most users. The algorithms and computational tools that are deployed in these processes are largely invisible. While users are increasingly transparent to such surveillance, the organisations undertaking the surveillance are increasingly protected by a shield of privacy. The watchers don't want to be watched (Andrejevic, 2007). Where exploitative or unjust practices are hidden from public scrutiny, they cannot be judged, opposed or changed. Here, secrecy and lack of transparency can increase power imbalances between people and institutions.

Facebook's ideology of consumer sovereignty and free exchange between service-provider and service-user conceals the unequal ownership rights which structure those exchanges. User content creation is conducted on the company's terms as specified in its End User License Agreement (EULA) and its various privacy and data use policies. The terms and conditions of these policies are complex, lengthy and written in language that is often ambiguous, occasionally misleading, and subject to change without notification. Empirical studies have shown that such policies are frequently either misunderstood, passively agreed to, or unread (Beninger et al, 2014). The terms of service in these policies grant Facebook the right to use, copy, display, reformat, translate, and distribute user content for any purpose. Facebook makes no distinction between personal information that is disclosed by users themselves, and information that *it* collects *about* users, both within and beyond the platform (Facebook, 2016b). Facebook asserts the right to collect both categories of information for marketing purposes and treats them as proprietary information that it owns, and can exploit as it sees fit. While, according to Facebook, users "own their data", this is only a fraction of the archived data that has been shared with other users and services. That users must agree to Facebook's EULA, and submit to commercial surveillance as a condition of access to the platform, represents a subtle form of coercion (Dainow, 2016).

Facebook's centralised architecture, its lack of interoperability with competing platforms, and its critical mass of users, combine to create a *lock-in* effect which discourages switching to other providers. Its content architecture and interfaces also raise usability and accessibility issues. Interface elements which are designed to manipulate users into taking particular actions, such as disclosing private information, or which prevent them from making informed choices, are ethically problematic (Conti and Sobiesk, 2010). Interfaces that target and exploit human cognition and perception disproportionately affect certain classes of users, including the elderly, young, and cognitively or sensory impaired. These include various

techniques that put the designers' objectives ahead of the users' through confusion (by asking the user questions or providing information they do not understand) distraction (by diverting attention away from, or interrupting, users' tasks) or obfuscation (by hiding desired information). These features apply to many of the privacy settings in Facebook, such as procedures for opting-out of cookie use, which are often complex and inaccessible. Successive changes to these privacy settings have made them difficult to locate and complicated to navigate.

The ancillary uses of social networking personal data have ethical implications that reverberate well beyond the environments from which they are harvested. This is particularly the case where such data is used to classify, categorise and differentiate between specific social groups, whether in social policy, marketing, or security measures. Where data mining and analytics is used to make decisions about groups of people, the consequences can lead to those affected being deprived of rights and opportunities. Profiling based on class, age, race, religion, nationality, sexual orientation or other characteristics can lead to discriminatory and unequal treatment of already disadvantaged groups. Attempts to predict behaviour can lead to spurious correlations and assumptions which can affect interactions with a range of institutions, including government agencies, banks, insurance companies, and employers. Such profiling can lead to discriminatory employment decisions, exploitive marketing practices and being offered less favourable prices, loans, mortgages or insurance policies. They can result in people being detained at an airport for "special screening", treated as a potential security threat, or questioned by the police. Technologies that identify, classify, then allocate opportunities on the basis of discriminatory models, represent forms of social sorting which reinforce social and economic divisions and power relations (Lyon, 2007).

While users possess the means for generating content for SNS, they do not own or control the technical resources for sharing that content. The processing power, technical infrastructure and data archives on which this depends are privately owned and operated (Gehl, 2014). They exist in centralized locations out of the reach of users. This results in an architecture where large, powerful servers housed in data centres are situated at the centre of the network, and relatively powerless "clients" are positioned at the edge. Access is through applications, platforms and devices, like smartphones, which have been progressively disempowered and thinned. This produces a series of power dichotomies and hierarchies, with users and *data have-nots* on one side, and *data-haves* on the other. The *data-haves* include service owners with the means to collect data, and a small elite of knowledge workers with the technical expertise to analyze that data and define how it will be used (boyd & Crawford, 2012; Zwitter, 2014). User activity, while presented and experienced as pleasurable entertainment, represents a form of exploited "playbour" from which profit is derived (Fuchs, 2014).

SNS trade on fundamental human needs to be valued, and to connect and communicate with others. The funnelling of these needs into prescribed templates acts to restrict the diversity of social life into atomised silos, and subsumes the complexity of human expression into narrow commercial interests and categories tuned to advertising. Rich qualitative expressions of affection, emotion and friendship are flattened into quantitative values and relationships with digital objects and fetishised brands. The cultivation of digital personae as repositories of social capital, and the imperative to curate and add value to them as personal brands, can be seen as part of a wider ideology of neoliberalism that seeks to bring all human action and expressions of individual worth into the domain of the market (Skeggs and Yuill, 2016). It is one facet of that ideology's colonisation of moral consciousness and of the socio-cultural sphere that Habermas calls the "lifeworld" (Habermas, 2001).

SNS nevertheless remain a site of conflict and struggle against these trends, variously expressed in resistance to privacy practices, surveillance and unannounced changes to services and policies. These have been a constant source of tension between platform providers and users. Resistance has manifested itself in periodic backlashes against Facebook, in various organised campaigns of collective action by disgruntled users, such as petitions and boycotts, and in attempts to block protocols, interfere with Facebook's interface, or publish scripts that allow plug-ins to be dismantled. Protests have been also been articulated by high-profile activists like Richard Stallman whose critique remains one of the most comprehensive inventories of ethical and political issues raised by Facebook (Stallman, 2013).

# 5. Legislating SNS

Laws are key regulating forces exerted on the operational domain of SNS (Lessig, 2006). Laws, however, have an ambiguous relationship with ethics, upholding and embodying some ethical principles, while undermining and threatening others (Jones, 2016). Few laws are socially or economically neutral. Some are weighted in favour of state interests, or protect the economic interests of private corporations, while others are designed to protect the rights of citizens. Of particular relevance here are those surveillance laws which grant the State significant powers to intercept and monitor social networking activity. In the UK, these include sections of the *Human Rights Act*, 1998, which waives privacy rights under certain conditions specified in Article 8, and the *Regulation of Investigatory Powers Act*, 2000. SNS providers can be legally obliged to comply with access requests from government agencies to profile data in criminal or intelligence investigations. Concerns have persistently been raised that the pretexts and terms of this access under current and proposed legislation are too broad and sufficiently vague as to permit unlimited surveillance under any circumstances. The scope and scale of intelligence gathering by different authorities is characterised by a fundamental lack of transparency, and of impartial, independent judicial oversight (Schneier, 2015).

Data protection is a field where clear regulatory frameworks exist in many nation states, most notably in the EU, whose framework articulates core principles for the collection and processing of personal data. In practice, however, enforcement of these principles has been weak, and levels of compliance low. Despite modifications and updates, data protection has failed to keep pace with the expansion of technological capabilities, and the challenges posed by globalisation (Rubinstein, 2013). Most of these core principles are undermined by the surveillance practices of SNS companies. Data minimization and purpose limitation principles, for example, are undercut by the merging of data from various sources for a range of unspecified purposes. Data subjects are invariably not informed when data is first disclosed for secondary marketing purposes, and are unable to prevent such processing. Data mining techniques afford an even greater capacity to aggregate and correlate pieces of information gathered from disparate sources in order to positively identify users and construct detailed dossiers about them. Multiple, individually-benign, pieces of information are routinely aggregated to reveal previously unknown characteristics or patterns of behaviour that were never intended to be disclosed. The ease with which identifying information can be inferred from "anonymous" data casts doubt on the distinction between personal data and non-personal data. Much of the data that routinely flows through SNS could rightly be considered "sensitive" given that it represents information about who people are, what they

do, their interests, lifestyles, habits and affiliations, as well as their locations, past and present.

The surreptitious nature of much personal data monitoring, which occurs without users' knowledge or agreement, also jeopardises the principle of informed consent. Where informed consent is sought through agreement to EULAs and data use policies, it is often invalidated by incomplete or withheld information, or by a lack of genuine free choice, where users are not able to withdraw consent without detriment. Data subjects' rights of access, rectification and deletion are seriously undermined where individuals are not able to retrieve or erase personal information. Facebook has consistently attempted to push users into "deactivating" rather than deleting their accounts. While this stops data being publically shared, it has allowed the company to continue using the data stored on its servers.

The transnational nature of SNS data processing presents major jurisdictional barriers to the regulation of data flows between countries. It exposes the fundamental contradictions between the spatially-bound powers of nation states and commercial information flows which are global and fluid. Inconsistencies between data protection standards in different countries and regions also form major barriers to multi-lateral implementation and enforcement. The data practices of companies such as Facebook have come under scrutiny from EU regulators in this regard. Attempts by EU legislators to limit the scope of these practices have been vigorously contested by corporate lobbying. The spatial mobility of global companies like Facebook have enabled them to evade national data protection laws as well as corporate taxation regimes. The size of such corporations, some have argued, is so great that their power to lobby politicians and influence nation states poses a threat to democratic governance (McChesney, 2014).

In the light of these issues, state bodies, at national and regional levels, continue to have a crucial role to play in regulating corporations. Various groups, including internet activist and privacy watchdog organisations have called for additional measures to protect consumers and defend public interests against corporate and state surveillance. Such proposals include mandated transparency about data collection, analysis and monitoring by SNS, including "truth in product" laws where profit is derived from personal data (Scheier, 2015). Where algorithms hold power over people, they should be open, public and audited for fairness. Campaigns for the "right to be forgotten" and the right to data deletion have called for SNS users to be given greater control over their personal information (Mayer-Schőnberger, 2011). This right should be extended to all individuals whose data is held, whether registered users or not of an SNS, and should include data gathered and aggregated by third parties such as data brokers. The implementation of anti-archival systems have been proposed in which data storage is minimised according to specified time limits before being purged (Gehl, 2014). Categories of sensitive data that ought *not* to be collected require revision and extension. Property and ownership rights might be established for specific categories of personal data affording them legal and technical protection in a manner similar to DRM systems for intellectual property. More radical proposals have included placing some internet services such as SNS in the public domain, and treated as public utilities (McChesney, 2014). These are envisioned as part of wider policy goals to provide public spaces in the internet commons free from control by private entities.

Ethical issues, however, cannot and perhaps should not be solved by statutory or regulatory means alone. Self-regulation and internal governance regimes must also be recognised as central components in the implementation of privacy and data protection measures. Such

regimes can be effective when supported voluntarily by SNS providers themselves, or by professional bodies in fields such as digital advertising, and particularly when reinforced by appropriate sanctions for non-compliance. Self-regulation, however, can have its limits. Voluntary self-governance regimes which entrust regulation to corporations who have vested interests in resisting such regulation reveal the shortcomings of search approaches. Passing and imposing legislation are partial and imperfect solutions, and insufficient guarantors of ethical design or use of ICTs. The speed of technology innovation means that laws will always tend to lag behind emerging technologies. Solutions to these issues need to be developed, not only through policy, law and regulation, but also through the design, development and implementation of technologies themselves.

# 6. Practicing SNS

While the legal and ethical issues around SNS can be identified, and their underlying principles disclosed, these principles need to be put into practice if ethics is to be *applied* in any meaningful sense. Ethical principles need to be translated into concrete measures that can be implemented by designers, developers and engineers. This final section therefore considers some of the implications of the above discussion for the sorts of questions, possibilities and alternatives that might be raised in the context of teaching and practising SNS ethics.

A useful point of departure is to consider some of the emerging codes of practice of key technical actors involved in SNS, whether developers and engineers or data analysts and designers. Embryonic codes of conduct in fields such as data science, to take just one example, offer some clues about what such codes of ethics might look like (Data Science Association, 2016; Digital Analytics Association, 2016). These acknowledge some of the specific harms and risks involved in data analytics, and outline a set of domain-specific codes of practice.

Alternative methodologies of design and software development can be considered which invert the dominant, top-down models of innovation. User-centric approaches, for example, attempt to develop solutions that are responsive to the needs of users, and in which users are active participants in the design process. Value-sensitive design similarly seeks to incorporate ethical values into projects from the outset, embedding them into every stage of the development lifecycle, from requirements gathering and design, to evaluation, prototyping and implementation (Friedman et al., 2008). Responsible innovation and research aims to develop greater accountability in the innovation lifecycle and sees this as a transparent, interactive process in which users and innovators are mutually responsive (Stahl et al, 2014). These methodologies provide ways of embedding ethical principles into technical requirements and specifications in actual projects. Alternative approaches to interface design also need to be considered, which incorporate accessibility principles and which attempt to transcend hierarchies and divisions around technical skills and expertise (Gehl, 2014).

At the architectural level, alternatives to the dominant network infrastructure underpinning SNS need to be envisioned. Some have suggested re-architecting the hegemonic client-server model towards a distributed network based on peerage and interconnected nodes without over-arching hierarchical control (Moglen, 2010). In this vision, "servers" are relocated to the edge of the network. This involves reviving the concept of the personal web server, "a server you can put in your pocket" as Moglen puts it (Moglen, 2010). In hardware terms, this might

take the form of a cheap mobile cloud storage device (or "freedom box") that can be loaded with free and open source software and protocols.

This model offers a number of potential advantages in terms of personal data management. Crucially, it permits users to house their data in devices that they own, control, can carry or access remotely. Users can operate their own data stores, individually or collectively, with the ability to impose their own usage and storage limitations. Services such as these would allow users to selectively disclose specific clusters of personal data, giving them greater control over what data is accessed, what it can be used for and who it can be shared with. This would also facilitate data-portability by enabling the transfer of data between SNS providers using standard formats and interface protocols.

In the field of privacy management a paradigm shift is required, away from privacy as the sovereign responsibility of the individual user through self-managed tools and applications, towards more preventative, privacy-by-design models that are built into the very operation and architecture of computer systems. Clarke (2001) makes a useful distinction between *Privacy-Invasive Technologies* (PITs) that intrude into privacy, and *Privacy-Enhancing Technologies* (PETs) which protect privacy interests, for example, by providing varying levels of anonymity and pseudonymity. PETs include tools such as identity management protocols (Torres et al, 2013). PETs can be used to minimise the collection of personal data, and reduce privacy risk through such tools. Thus, while individuals may have a unique identifier as an SNS user, this would contain no personally identifiable information. Allowing SNS users to have multiple, pseudonymous IDs might, in turn, reduce the risks of data aggregation. Existing anonymising systems which enable users to avoid being tracked online, could be extended into a comprehensive set of applications which would allow personal data to be selectively anonymised by the user for different types of services. If personal data has value, some have suggested that service providers should pay for it in the form of automatic micro-royalties for access to users' personal data. Such a system would create a data economy around the gathering and usage of personal data, with the potential for intermediate layers of vendors trading data on the user's behalf (Dainow, 2016).

Finally, alternative models of online social communication need to be envisioned that do not entail submission to commercial surveillance. Here, it is important to challenge the assumption that the only form online sociability can take must be constituted as a proprietary, market-based activity founded on privately-owned resources. This means exploring the possibilities of non-profit and non-hierarchical models founded on principles of collaboration, social reciprocity and information-sharing. Wikipedia is invariably held up as one such model. It demonstrates that large-scale forms of peer production and collaborative authorship of knowledge, founded on free software, and not dependent on advertising, are possible. However, there are numerous, smaller-scale, less visible sites of innovation around social networking that have emerged at grassroots level, from various local groups, communities of practice and small start-ups. Examples include open source software development, co-operative social projects, volunteer networks, and news outlets that bypass traditional mass media channels. A host of alternative social media platforms also exists, such as Ello, Family Leaf, ConnectMe, Budypress, Crabgrass, Cryptocat, Elgg, Friendica, Lorea, N-1, Occupii, kaioo and Diaspora. Many are advertising free, built on open-source software, run on a non-profit basis, and do not track their users. Diaspora, for example, is a decentralised SNS that enables its users to set up their own server (or "pod") and operate their own data node that they control (Diaspora, 2016).

Alternative SNS nevertheless face a number of challenges, including sustainable funding models for development, hosting and administration, scaling-up of services and building a critical mass of users in the face of lock-in strategies by the dominant SNS players. However, these alternative services offer some clues, in their embryonic features, about what ethical SNS might look like. They point to the potential of alternative models of direct financing based on blockchain technologies and crowdfunding. They suggest the possibilities of hybrid business models situated between traditional ecommerce and the non-profit models of the sharing economy. This may require a rethinking of concepts of value and exchange in SNS. It may also require the development of new forms of ethical and democratic governance premised on transparency, as exemplified in the peer production of privacy policies by some SNS which are debated and co-written by users and administrators. Alternative SNS might also have a pedagogic dimension, one that involves teaching users to become more active contributors to design, development and implementation, whether as coders, technicians or administrators.

Alternative SNS anticipate a commons-based Internet that is not based on capital accumulation and the attention economy of advertising, one that values social communication, knowledge-sharing and collaboration for their own sake. Future research needs to focus on all these above areas, and develop further the emergent links between academic researchers and technical practitioners, and between activist groups and SNS users.

# 7. Conclusion

This paper has presented a strategy of inquiry to understand various aspects of SNS ethics. It has proposed an inter-disciplinary approach to SNS ethics that connects critical analysis with pedagogic and technological practice. A multi-dimensional framework has been proposed and demonstrated. This framework proceeds through four sequential stages; socio-economic, ethical, legal and practical/professional. A critical analysis of SNS ethics has to be grounded in an understanding of the economic drivers and the technological and social practices at work in this domain. The paper has demonstrated that it is these driving forces and practices that generate some of the central ethical issues around SNS, particularly around privacy and transparency. It has shown that ethical issues tend to emerge where core ethical principles are at stake, or are violated, by the design, implementation or use of SNS technologies.

The framework elaborated above suggests the potential of a holistic, multi-dimensional approach to teaching ICT ethics, one that might be applied to other domains beyond SNS. This framework also points to the potential of future approaches to draw on different theoretical resources to generate new connections and insights across disciplinary boundaries. As ICTs become ubiquitous across all areas of human activity, so their social and ethical implications will become increasingly widespread and profound. Multi-faceted phenomena such as SNS cannot be grasped with the confines of any single discipline. This paper points to the urgency of breaking down some of the knowledge silos of academic practice, not only between computer scientists, critical cultural theorists and social scientists, but also between academics and IT practitioners working in field of social networking.

The evaluation of ethical issues, and the practical responses to those issues, can be enriched when founded on a broader understanding of the socio-economic, technical and legal contexts in which SNS are designed and used. Disclosing the ethical consequences of ICTs and making their social and economic power visible is an important ethical practice in its own

right. A key part of this pedagogy is to foster reflexivity and to encourage a sense of agency amongst students, as future prospective IT practitioners. This means exploring and imagining what ethical alternatives might look like, technically, aesthetically and economically. As the recent history of SNS demonstrates, this is a field littered with failed ventures and companies that once looked impregnable. There is a simple, but powerful, pedagogical point here, namely that how SNS are designed, implemented and used are subject to change. They are not set in stone. They can be designed and used quite differently, according to different ethical principles.

# References

Andrejevic, M. (2007), *iSpy: Surveillance and Power in the Interactive Era*, University Press of Kansas, Lawrence, Kan.

Andrejevic , M. (2011), "Social Network Exploitation", in Papacharissi, Z. (Ed.), *A Networked Self: Identity, Community and Culture on Social Network Sites*, Routledge, London, pp. 82-101.

Baase, S. (2013), *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet*, Pearson, Upper Saddle River, NJ.

Beninger, K., Fry,A., Jago, N., Lepps,H. Nass, L. and Silvester, H. (2014), *Research using Social Media; Users' Views,* NatCen Social Research, London.

boyd, d. and Ellison, N. (2008), "Social Networking Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, Vol 13 No. 1, pp. 210-230.

boyd, d. and Crawford, K. (2012), "Critical Questions for Big Data", *Information, Communication and Society*, Vol 15 No. 5, pp. 662-679.

Brake, D. (2014), *Sharing our Lives Online: Risks and Exposure in Social Media*, Palgrave Macmillan, Basingstoke.

Brey, P. (2010), "Values in Technology and Disclosive Computer Ethics", in Floridi, L. (Ed.), *Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, Cambridge, pp. 41-58.

Burkell, J., Fortier, A., Yeung, L. and Simpson, J. (2014), "Facebook: Public Space, or Private Space?", *Information, Communication and Society*, Vol. 17, No. 8, pp. 974-985

Clarke, R. (2001), "Introducing PITs and PETs: Technologies Affecting Privacy", available at: http://www.rogerclarke.com/DV/PITsPETs.html (accessed 13th December 2016).

Clarke, R. (2006), What's 'Privacy'?, available at: http://www.rogerclarke.com/DV/Privacy.html (accessed 13th December 2016).

COMRES (2015), *Big Brother Watch*; *UK Public Research—Online Privacy*, Comres, London, available at: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/03/Big-Brother-Watch-Polling-Results.pdf (accessed 24th April 2016).

Conti, G. and Sobiesk, E. (2010), "Malicious Interface Design: Exploiting the User", Proceedings of the International World Wide Web Conference, April 26–30th, Raleigh, USA, ACM, New York, NY, pp. 271-280.

Dainow, B. (2016) "Digital Alienation as the Foundation of Online Privacy Concerns", *ACM SIGCAS Computers and Society*, Vol. 45 No. 3, pp.109-117.

Data Science Association (2016), "Data Science Code of Professional Conduct", available at: http://www.datascienceassn.org/sites/default/files/datasciencecodeofprofessionalconduct.pdf (accessed 24th April 2016).

Diaspora (2016) "How Does Diaspora Work?", available at: https://diasporafoundation.org/about#host (accessed 24th April 2016)

Digital Analytics Association (2016), "The Web Analyst's Code of Ethics", available at: http://www.digitalanalyticsassociation.org/codeofethics (accessed 24th April 2016).

Eisenlauer, V. (2013), *A Critical Hypertext Analysis of Social Media: The True Colours of Facebook*, Bloomsbury, London.

Facebook (2015) "Facebook Reports First Quarter 2015 Results", available at: http://investor.fb.com/releasedetail.cfm?ReleaseID=908022 (accessed 24th April 2016).

Facebook (2016a) "About Facebook", available at: https://www.facebook.com/facebook/info?tab=page_info (accessed 24th April 2016)

Facebook (2016b) "Data Policy", available at: https://www.facebook.com/about/privacy/advertising (accessed 24th April 2016)

Friedman, B., Kahn, P. and Borning, A. (2008), "Value Sensitive Design and Information Systems", in Himma, K. and Tavani, H. (Eds.), *The Handbook of Information and Computer Ethics*, John Wiley, Hoboken, NJ, pp. 69-101.
Fuchs, C. (2014), *Social Media: A Critical Introduction*, Sage, London.
Fuller, M., (Ed.) (2008), *Software Studies: A Lexicon*, MIT Press, Cambridge, MA.
Gehl, R. (2014), *Reverse Engineering Social Media: Software, Culture and Political Economy in New Media Capitalism*, Temple University Press, Philadelphia.
Greenwood, S., Perrin, A. and Duggan, M. (2016), "Social Media Update 2016", Pew Research Center, available at: http://www.pewinternet.org/2016/11/11/social-media-update-2016 (accessed 13th December, 2016)
Hall, S. (1982). "The Rediscovery of 'Ideology': Return of the Repressed in Media Studies" in Bennett, T., Curran, J., Gurevitch, G. and Wollacott, J. (Eds.) *Culture, Society and the Media*. Methuen, New York, NY, pp. 56-90.
Habermas, J. (2001) *Moral Conciousness and Communicative Action*, MIT Press, Cambridge, MA
Hull, G., Lipford, H. and Latulipe, C. (2011), "Contextual Gaps: Privacy Issues on Facebook", *Ethics and Information Technology*, No 13 Vol. 4, pp. 289–302.
Hull, G. (2015) "Successful Failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data", *Ethics and Information Technology*, Vol. 17 No. 2, pp 89-101.
Hutchby, I. (2001), "Technologies, Texts and Affordances", *Sociology*, Vol. 35, No. 2, pp. 441–456.
Johnson, D. (2009), *Computer Ethics: Analyzing Information Technology*, Pearson, Upper Saddle River, NJ.
Jones, S. (2016) "Doing the Right Thing: Computer Ethics Pedagogy Revisited", *Journal of Information, Communication and Ethics in Society*, Vol. 14 No. 1, pp. 33-48.
Lessig, L. (2006), *Code: Version 2.0*, Basic Books, New York, NY.
Light, B. and McGrath, K. (2010),"Ethics and Social Networking Sites: A Disclosive Analysis of Facebook", *Information Technology and People*, Vol. 23 No. 4 pp. 290-311.
Lovink, G. (2011), *Networks Without a Cause: A Critique of Social Media*, Polity Press, Cambridge.
Lyon, D. (2007), *Surveillance Studies: An Overview*, Polity Press, Cambridge.
McBride, N. (2014), "ACTIVE Ethics: An Information Systems Ethics for the Internet Age", *Journal of Information, Communication and Ethics in Society*, Vol. 12 No. 1, pp. 21-44.
McChesney, R. (2014). "Be Realistic, Demand the Impossible: Three Radically Democratic Internet Policies", *Critical Studies in Media Communication*, Vol. 31 No. 2, pp. 92–99.
McGee, M. (2013), "EdgeRank is Dead: Facebook's News Feed Algorithm now has close to 100K Weight Factors", *Marketing Land*, 16 August, available at: http://marketingland.com/edgerank-is-dead-facebooks-news-feed-algorithm-now-has-close-to-100k-weight-factors-55908 (accessed 24th April 2016)
Marthews, A. and Tucker, C. (2015), "Government Surveillance and Internet Search Behavior", *Social Science Research Network*, Rochester, NY, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564 (accessed 24th April 2016)
Mayer-Schőnberger, V. (2011) *Delete: The virtue of forgetting in the digital age*, Princeton University Press, Princeton, NJ.
Mehdizadeh, S. (2010), "Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook", *Cyberpsychology, Behavior and Social Networking*, Vol. 13 No. 4, pp. 357–364.
Moglen, E. (2010), *Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing*, presentation to The Internet Society (New York) 5 February,

2010. Transcription available at: https://www.softwarefreedom.org/events/2010/isoc-ny/FreedomInTheCloud-transcript.html (accessed 24th April 2016)
Moor, J. (1985), "What is Computer Ethics?", *Metaphilosophy*, Vol 16, pp. 266-275.
Nissenbaum, H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford, California
Papacharissi, Z. (Ed.) (2011), *A Networked Self: Identity, Community and Culture on Social Network Sites*, Routledge, London.
Rainie, L. (2016), "The State of Privacy in America: What we learned", Pew Research Center, Washington DC, available at: http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/ (accessed 24th April 2016)
Quinn, M. (2010), *Ethics for the Information Age*, Addison-Wesley, London.
Reynolds, G. (2012), *Ethics in information technology*, Cengage, Boston, MA.
Rubinstein, I. (2013), "Big Data: The end of privacy or a new beginning?", *International Data Privacy Law*, Vol 3 No.2, pp. 74- 87.
Schneier, B. (2015), *Data and Goliath: The hidden battles to capture your data and control your world*, W.W.Norton, New York, NY.
Sipior, J., Ward, B., and Mendoza, R. (2011), "Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons". *Journal of Internet Commerce*. Vol. 10 No. 1, pp.1-16.
Skeggs, B. and Yuill, S. (2016), "Capital Experimentation with Person/a Formation: How Facebook's monetization refigures the relationship between property, personhood and protest", *Information, Communication and Society*, Vol. 19 No. 3, pp. 380-396.
Stahl, B. (2008), *Information Systems: Critical Perspectives*, Routledge, London.
Stahl, B., Eden, G., Jirotka, M. and Coeckelbergh, M. (2014), "From Computer Ethics to Responsible Research and Innovation in ICT", *Information and Management*, Vol. 51 No. 6, pp. 810–818.
Stallman, R. (2013), "Reasons not to use Facebook", available at: https://stallman.org/facebook.html (accessed 13 th July, 2016)
Suler, J. (2004), "The Online Disinhibition Effect", CyberPsychology and Behavior, Vol. 7 No. 3, pp. 321–326.
Tavani, H. (2013), *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*, John Wiley, Hoboken, NJ.
Thaler, R., Sunstein, C. and Balz, J. (2010), "Choice Architecture", *Social Science Research Network*, Rochester, NY, available at: http://ssrn.com/abstract=1583509 (accessed 24th April 2016).
Torres, J., Nogueira, M. and Pujolle, G. (2013), "A Survey on Identity Management for the Future Network", *IEEE Communications Surveys & Tutorials*, Vol. 15 No. 2, pp.787-802.
Turkle, S. (2011), *Alone Together: Why we expect more from Technology and less from each other*, Basic Books, New York, NY.
Turow, J. (2011), *The Daily You: How the new Advertising Industry is defining your identity and your world*, Yale University Press, New Haven, CT.
Van Dijk, J. (2013), *The Culture of Connectivity: A Critical History of Social Media*, Oxford University Press, Oxford.
Zwitter, A. (2014) "Big Data Ethics", *Big Data and Society*, July–December, pp. 1-6.