Finch, E. (2003). "What a tangled web wfeweave: Identity theft and the Internet." InY. Jewkes (ed.), Dot.cons: Crime, deviance, and identity on the Internet, (pp. 86-104). Collompton, England: Willan.

Willan Publishing
c/o International Specialized Book Services
920 NE 58th Street, Suite 300
Portland, OR 97213-3786, USA
Tel: 503 287 3903; Fax: 503 280 8832
e-mail: orders@isbs.com; website: www.isbs.com

Chapter 6

What a tangled web we weave: identity theft and the Internet

Emily Finch

Introduction

Following the news of the Paddington rail crash in October 1999, Lee Simm reported his flatmate, Karl Hackett, missing. According to Simm, Hackett had been due to return from a trip to Cheltenham on the train that crashed. No trace of Hackett's body was found and his family, from whom he had been estranged for more than ten years, were notified and attended a memorial service at the site of the crash. It later transpired that Hackett had not been killed in the train crash; he had not even been on the train. However, it was discovered that his flatmate, Simm, who reported Hackett missing, had been dead for 15 years, hi order to escape his criminal record, Hackett adopted Simm's identity after his friend committed suicide. Hackett went on to live a blameless life using Simm's name and other personal details and would probably have remained undetected had he not decided to 'kill off' his former self in the rail crash *(The Sunday Times* 2000:14).

Such a wholesale and enduring absorption of another's persona provides a relatively uncommon example of identity theft. The Hackett/ Simm case is unusual in that identity theft typically involves a partial and transient adoption of another's identity undertaken in order to facilitate criminal activity. Identity theft spans a wide spectrum of conduct that covers varying degrees of fraudulent behaviour. This chapter will begin with a consideration of the nature of identity, focusing on the disparity between individual, social and legal constructions of identity, and explore what it means for a person's identity to be stolen. Having outlined the various manifestations of identity theft, the chapter will go on to

consider factors that have contributed to the growth of identity theft in recent years, with particular reference to the contribution of the Internet. The chapter will conclude by considering two means by which identity theft may be tackled; first, by technological advances that make the misuse of another's identity more difficult and, secondly, by the creation of a specific criminal offence to encompass conduct that has come to be known as identity theft.

Identity and identifiability

It is necessary to determine at the outset what is meant by 'identity'. From simplistic origins, identity has evolved into a complex and multifaceted concept that plays a central role in delineating the parameters of, *inter alia*, ethnicity, nationality and citizenship, thus generating an immense amount of debate across various disciplines (Gleason 1983; Williams 2001; Bendle 2002). In relation to identity theft, the concern is with identity as a means of ascertaining individuality and establishing personhood rather than as a basis for establishing collective identity or group membership. Even within this narrower sphere, there are competing constructions of identity that jostle for supremacy (Perry 1975; Sider 2001). For the purpose of this discussion, a relatively straightforward tripartite categorisation of identity can be adopted based upon the categorisation used by Goffman, albeit using different terminology: individual identity, social identity and legal identity (Goffman 1963).

Individual identity can be seen as the sense of self that is based upon the internalisation of all that is known about oneself. For Goffman, the key characteristics of what he termed - after Freud - 'id' (or felt) identity are subjectivity and reflexivity. Hence individual identity is more than simply self-perception; rather, it is the subjective construction of the self that is modified by reflections on the views of others and the individual's interactions in the social world. As such, individual identity is not a static construction but one that is constantly evolving and readjusting in line with the individual's life experience. Although individuals do not remain the same, they retain a sense of sameness throughout their lives that is based, according to Locke's (1690) *Essay Concerning Human Understanding*, on the sense of continuity that arises from being able to remember being other than one is at present (in other words, unlike other animals, human beings possess a unique sense of themselves in the past as children or even babies, and can also project forward to envisage themselves in old age; they also understand that they are mortal). Individual identity can be encapsulated as being 'what most of us think of

when we think of the deepest and most enduring features of our unique selves that constitute who we believe ourselves to be' (Williams 2001: 7).

To a certain extent, there is a symbiotic relationship between individual and social identity in that social identity is contingent upon the way in which individuals present themselves while individual identity can be influenced by the way in which an individual is received in society. For Goffman, social identity is based upon the categorisation of an individual to determine the acceptability of the membership of certain social groups. It is concerned with attributes of an individual that may be intrinsic but are not necessarily so. If individual identity is concerned with the question of 'who am I', then social identity is concerned with the question 'what is the nature of this person'. Having qualified for membership of a particular group, certain other characteristics may be ascribed to the individual by virtue of membership regardless of whether or not they are actually possessed by the individual. Social and individual identity will necessarily differ from each other for various reasons, not the least of which is that the internal and external views of the individual are based upon different information. Although both individual and social identity may be affected by identity theft, neither can be stolen. It is the third category of identity - legal identity - that has the potential to be adopted and abused by others; hence it is at the heart of concerns about identity theft.

By way of contrast to the other categories of identity, legal identity tends to be largely fixed and immutable. Goffman describes legal identity in terms of a set of characteristics that are unique to the individual thus providing a way in which one person can be differentiated from another. Similarly, the preoccupation of the law is to 'impose durable identities' (Torpey 2000: 166) in order to ensure that two inter-related questions - 'who is this person?' and 'is this the same person?' - can be answered. Therefore, it is clear that the legal construction of identity gives primacy to factual information regarding an individual; information that is largely unalterable. For example, birth certification is generally viewed as the foundation of legal identity as it records key pieces of information unique to the individual such as his or her sex, date and place of birth and details of his or her parents. Despite strenuous opposition, the English courts have steadfastly maintained that a birth certificate is a historical record of fact that cannot be amended retrospectively at the behest of the individual to whom it relates *(Cossey* v. *United Kingdom* [1991] 2 FLR 492; *Sheffield* v. *United Kingdom* [1998] 2 FLR 928). This illustrates the degree of permanence attached to legal identity and makes it clear that when legal and individual identity conflict, it is legal identity that prevails. As an individual progresses through life, the information on his or her birth

certificate is supplemented by further details, thus contributing to the cumulative mass of facts that constructs the composite legal person. This is described by Foucault as a process that 'places individuals in a field of surveillance [and also] situates them in a network of writing; it engages them in a whole mass of documents that capture and fix them' (Foucault 1979:189).

Foucault's reference to an individual being captured within a network of documents is particularly apt as it suggests that once an individual is enmeshed within this documentary web, it is virtually impossible for him or her to escape. As such, legal identity is more concerned with identifiability rather than identity as it seeks to make the link between a collection of facts and the person to whom they relate. The permanence of legal identity can lead to difficulties where there is significant conflict with individual identity. The clash of two polarised constructions of the identity of the same person can ultimately lead to identity theft if the individual concerned is desperate to escape from some unwanted aspect of his or her legal identity. This was the situation in the Hackett/Simm case where a new identity was adopted in order to escape the implications of an unalterable aspect of the legal identity - a criminal record. However, there are various manifestations of identity theft involving differing levels of absorption of another's identity and numerous motivations for engaging in this conduct. Having explored the nature of identity, the discussion that follows will consider what it means for identity to be stolen and examine the range of situations in which identity theft may occur.

A typology of identity theft

The previous discussion has established that there are different facets of identity that are constructed according to whether a person is viewed from an individual, social or legal perspective; hence it could be said that everyone is simultaneously endowed with three distinct identities. However, not all these identities are capable of forming the subject matter of identity theft. Legal identity differs as, although it lacks a tangible physical presence in the same way as other types of identity, it can be made manifest by the production of documents or the possession of knowledge that substantiates the claim to be the person in question. The tangible 'thing' that is 'stolen' is the personhood of another as manifested by the assertion to be that person, which may or may not be supported by documentary or other evidence. As such, it involves the misuse of information that is specific to an individual in order to convince others

that the impostor *is* the individual, effectively passing oneself off as someone else.

This broad definition encompasses two distinct types of identity theft that can be differentiated on the basis of three inter-related factors: duration, level of immersion and motivation. The duration of identity theft ranges from a single incident lasting only a few minutes to the lifelong use of another's personal information - effectively, living life *as* the victim. Duration is often associated with the level of immersion as long-term identity theft characteristically involves a greater penetration into the victim's personal details than a one-off incident or a short-term impersonation. The level of immersion refers to the depth with which the impostor delves into the victim's life and to the range and extent of the personal details that are misappropriated. Identity theft can result from the possession of the most basic details about an individual, such as name and date of birth, to more complex cases involving a deeper level of immersion whereby the impostor researches the victim to ascertain a range of personal and financial details, such as employment history, education and bank account details in order to masquerade successfully as the victim. Whatever the level of immersion, all these personal identifiers can be found on the Internet, as we will see shortly.

A combination of duration and level of immersion provides a possible basis for establishing a twofold categorisation of identity theft. A permanent adoption of all the details of the victim could be classified as total identity theft while the temporary use of some of the victim's personal details could be more appropriately termed partial identity theft. However, a more useful categorisation is suggested by consideration of a third factor, which is motivation of the impostor. Typically, partial identity theft involves the transient adoption of the victim's identity to the extent that is necessary to facilitate the commission of a criminal offence. This is epitomised by the approach taken to identity theft in the USA where the Identity Theft and Assumption Deterrence Act 1998 makes it an offence to 'knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or aid and abet, any unlawful activity' (18 USC 1028 (a) (7) as amended by the Identity Theft and Assumption Deterrence Act 1998).

This approach clearly limits the parameters of identity theft to the deliberate abuse of another's personal information in order to commit a criminal offence. Certainly, this would appear to be the most prevalent form of identity theft as it accounts for the vast majority of partial identity theft and a significant proportion of cases of total identity theft. The paradigm example of partial identity theft involves the temporary assumption of another's identity in order to gain access to goods and

services in the victim's name; an offence that has been inflated by the growth of online shopping. In this way, the impostor gains the benefits of the transactions while the cost is attributed to the victim. Other examples of partial identity theft involve the impersonation of the victim in order to engage in criminal activity that does not give rise to a direct financial detriment to the victim. Examples of this include the motorist who obtained another driver's licence in order to continue to drive in defiance of a period of disqualification and the shoplifter who used various aliases when she was arrested, ultimately accumulating convictions in over 20 different names (Newman 1999).

The desire to engage in criminal activities may also be the motivation for total identity theft. By adopting a different identity, the offender increases his or her chances of avoiding detection by ensuring that his or her acts are attributed to someone other than him or herself. Even if the victim is able to establish that he or she has been impersonated, this generally leave the authorities with few clues to point them in the direction of the real perpetrator. For example, Terry Rogan was arrested and detained for robbery and murder on five occasions before the police were able to locate and identify the person who had committed these crimes using Rogan's identity *(Rogan* v. *City of Los Angeles* 668 F Supp 1384 CD Cal 1987). Cases in which the usurpation of another's identity (in whole or in part) is motivated by the desire to engage in unlawful activities in the victim's name can be termed 'criminal identity theft'.

The motivation for total identity theft is often more complicated than a straightforward determination to avoid the consequences of participation in criminal activity or to facilitate fraudulent behaviour (Marx 2001). Total identity theft provides a way in which an individual can escape from a life that has gone wrong and obtain an opportunity to make a fresh start (Newman 1999). This urge to reinvent oneself may derive from a general sense of dissatisfaction with one's own identity or be a way to escape from some particularly problematic aspect of life such as debt or a traumatic relationship. Identity theft provides both a practical and symbolic respite from a life that has gone wrong by enabling the individual to escape the problem and to acquire a legal identity that is in accord with his or her perceived or desired individual identity. For example, Karl Hackett no longer regarded himself as a criminal having reached a decision to lead an honest life but he was unable to escape his background due to the provisions of the Rehabilitation of Offenders Act 1974. For that reason, he resorted to identity theft and adopted an identity that was in accord with his view of himself as a non-criminal. Cases such as this in which the overwhelming motivation of the impostor is to establish a new identity in order to avoid any further association

with some aspect of his legal identity can be termed 'escape identity theft'.

The extent to which individuals will go in order to purge themselves of undesired attributes of their legal identity demonstrates the pressure that can be created when a conflict occurs between individual and legal identity. This is exacerbated by the increased range of situations in which people are required to provide various forms of identification in order to access services that often bear no relation to the information that is demanded (Westin and Baker 1972). According to Clarke (1994), this 'information richness' has become an imperative in late modern society and individuals who decline to provide the information are presumed to have 'something to hide'. This can have an exclusionary, stigmatising impact as individuals sometimes feel compelled to avoid seeking access to services that require the disclosure of what might be deemed 'unfavourable' personal information. For example, Marx (2001: 323) concludes that individuals may now feel a need to lie about facets of their lives that in the past were unseen, overlooked or forgotten. The tightening of the information net generates structural pressures to fabricate personal information.

The tightening of the information net

As there appears to be consensus among writers that burgeoning demands for identification have contributed to the increase in identity theft, it is important to examine the genealogy of the state's obsession with recording information about its citizens. Historically, people tended to live in small, self-contained and relatively static communities in which one's character was a matter of public knowledge and identification was automatic. The localisation of assistance for the poor was a disincentive to mobility for many and an itinerant criminal population was not viewed as problematic as punishment was largely immediate and corporeal. Records were kept locally but the lack of a fast and efficient communications system meant that it was not practically possible to share information with other localities. It was accepted that offenders tended to leave prison, change their names and move to another area, presumably to continue offending. Methods were developed that enabled the authorities to 'fix' individuals with an identity, such as anthropometry (that is, measurements of the body, skull, etc.) and photography, but these were not wholly reliable, and storage and distribution of the information remained an impediment to effective enforcement (Torpey 2000: 19). These developments were paralleled by a trend towards removing the

control of information from local institutions, for example, the centralisation of record-keeping introduced by the Births and Deaths Registration Act 1837 and the abolition of the Speenhamland system by the Poor Law Amendment Act 1834 that removed the administration of poor relief from local parishes. This move towards centralised administration was furthered by the creation of measures that contributed towards the evolution of the welfare state, such the introduction of compulsory education, pensions, welfare benefits and free health care. The greater involvement of the state in the lives of the populace led to a more unified and referable system of information that played a significant role in increasing the identifiability of individuals.

An inevitable corollary of this was a growth in the range of situations in which individuals were required to identify themselves in order to establish their entitlement to these various services and benefits. Greater mobility of workers led to rapidly fluctuating community membership which also increased the need for identification as did the expansion of licensing and administration by the authorities. These factors combined to create an ethos of identifiability in which it was commonplace to be required to identify oneself and where an inability or reluctance to do so was increasingly viewed with suspicion (Clarke 1994). As identification became the key with which to access a range of services and benefits, the adoption of fraudulent identity in order to access that to which one was not entitled increased, particularly as organisations rarely looked beyond the documents presented to ascertain their validity. The piecemeal development of the record-keeping system, in particular the absence of effective cross-referencing, meant that there were inadequate safeguards in place to prevent fraud. The growth of fraud put increased pressure on the state to introduce a means of controlling access to benefits that precluded fraudulent claimants, which effectively required the evolution of even more stringent means of establishing legal identity. This in turn made it harder for those with 'spoiled' identities (Goffman 1963) to hide the unfavourable aspects of their identities, hence creating a greater level of exclusion and generating pressure to fabricate a more acceptable self.

Identity theft and the Internet

The incremental growth of the requirement of identifiability undoubtedly contributed towards the escalation in identity theft as some sought to engage in fraudulent behaviour and others saw the theft as the only way to 'escape' their own identity. However, this alone cannot account for the massive upsurge in identity theft that occurred towards

the latter part of the twentieth century, and led the Federal Trade Commission (2000: 5) to label identity theft as 'the fastest growing crime of our time'. As information about the victim is the lifeblood of identity theft, the increased ease with which information can be accessed on the Internet could provide an explanation for the increase in identity theft.

As has been discussed, the 'tightening of the identity net' has led to a situation whereby individuals who are unhappy with an aspect of their legal identity may face a stark choice between disclosure of sensitive, and potentially prejudicial, information or exclusion from the many activities that require identifiability. According to Gary Marx (2001: 323), with contemporary forms of data collection, storage and retrieval, 'elements of the past that tended to be forgotten are now preserved. For better or worse elements of the individual's past cease to be past and instead are passed on'. However, the desire to create a new and unblemished identity would not contribute to the growth of identity theft to such a significant degree if it were not for the relative ease with which the knowledge that forms the foundations of identity can be acquired. In this respect, 'escape' identity theft and 'criminal' identity theft share common ground. Whether the impostor is in search of a new identity in order to escape from his or her own life, to commit criminal offences with impunity, to defraud a victim or even as a means of causing harassment to a victim, it has become a relatively straightforward matter to obtain the information that is needed effectively to adopt the identity of another (Newman 1999).

The Internet provides unparalleled opportunities for those seeking a new identity to access the necessary information. One of the anomalies of Internet use is that although 'it is much more difficult to verify identity and sincerity online...many users appear to be more trusting of those met online than those they encounter in person' (Rowland 1998: un-paginated). This leads Internet users to be far less security-minded in relation to their personal information when they are online than they are in 'real life' situations. Certainly, there is evidence to suggest that many Internet users are cautious about the safety of Internet transactions that require them to provide their debit or credit card details but there appears to be an almost reckless disregard for basic security precautions in relation to publication of any other personal information on the Internet. Detailed information regarding individuals may be available on personal or workplace websites as well as via professional organisations of which the individual is a member. In addition to this, information may be posted about individuals by third parties for a range of reasons and many organisations include searchable databases on their websites that may yield valuable information about potential victims. Information has become a valuable commodity and some websites exist solely for the

purpose of trading in personal information. This situation is more advanced in the USA where information brokers will provide data about an individual's medical records, bank details, credit rating, criminal record, driving licence and vehicle registration documents for a small fee. In short, everything that the impostor needs to select a victim and misappropriate his or her identity is readily available on the Internet (Newman 1999).

Not only is the information-gathering process facilitated by the Internet but the task of selecting a profitable target with a good credit rating and a high income is made easier due to the availability of such wide-ranging personal information. The speed and accuracy of Internet search engines ensure that all references to a particular individual can be accumulated in a matter of seconds, hence accelerating the selection process. It is clear that the Internet provides virtually instantaneous access to the sort of information that would not otherwise be available without conducting a meticulous search into the victim's background. Although it has always been possible to access much of this personal information, it tended to involve visiting various organisations and conducting time-consuming manual searches to obtain just a fragment of information about an individual. The process of researching potential victims and accumulating all the necessary information to adopt their identity was a long and painstaking process that would previously have taken weeks or months. This information is now only a few keystrokes away and can be accessed easily from the impostor's home or office. As the Federal Trade Commission (2000: 5) report on identity theft states: 'The Internet provides access to identifying information, through both illicit and legal means. The global publication of identifying details that previously were available only to a select few increases the potential for misuse of that information.'

The ease with which personal information can be accessed is only one way in which the Net has contributed towards the growth in identity theft. Businesses have responded to the expansion of the Internet by offering online services that provide impostors with the opportunity to engage in fraudulent conduct 'at arms' length'. The Federal Trade Commission has argued that this provides a sense of anonymity that encourages fraudulent activity in individuals who would not risk behaving in this way in person. Thus, for example, an impostor can make an application for a loan, credit card or even a mortgage online or make purchases using a victim's credit card details. This is surely a more attractive option than going into shops and businesses where the fear of detection must be felt more acutely. The opportunity to 'shop from home' in this way enables the impostor to remain within his or her own territory

thus eliminating the perceived sense of danger that is attached to engaging in fraudulent transactions in person. Moreover, there may be a sense of unreality attached to the process as all that is required to escape from what has happened is to switch off the computer in the manner of exiting a role-play game - what Suler (1996) calls the 'disinhibition effect' of the Internet.

In this respect, the Internet provides a distance, both spatially and symbolically, that enables a differentiation to be made between transactions carried out online and the equivalent transactions in real life. The perception that there is a lower risk of detection stems from the commonly held view of the Internet as an enforcement-free zone in which there is minimal legal regulation. This may free users from the constraints that inhibit criminal activity in real life, as there is an appearance of an absence of accountability for one's actions. Moreover, the acceptability of the use of pseudonyms on the Internet and the ease with which users are able to construct multiple identities also contribute to a sense of freedom from the constraints and conventions of everyday life. Marx (2001: 323) considers that the relative anonymity of the Internet is a significant contribution to the rise in Internet-related fraudulent activity as 'individuals are freer to make and remake themselves than ever before'.

It would appear that opportunity is one of the key factors in explaining the growth of identity theft combined, in escape cases, with an incentive to fabricate engendered by the greater emphasis placed on identifiability in today's society. Although it has been described as the 'neoteric crime of the information technology era' (Saunders and Zucker 1999: 184), it is clear that identity theft is not a new type of behaviour but that the Internet has facilitated the construction of fraudulent identities by revolutionising the information-gathering process that is the foundation of identity theft. Ironically, Foucault's 'carceral network' of documentation enmeshing the individual is in some senses subverted by the Internet which promises the identity thief escape from his or her own personhood and offers a plethora of 'new' identities to 'try on'. Moreover, the Internet makes it easy to disassociate from the implications of one's activities. This increase in the prevalence of identity theft is likely to continue unless measures are taken to address these problems and protect individuals from those who would misuse their identity. Two important weapons in the war against identity theft are advances in identification technology that may prevent theft from occurring and the introduction of legal measures to ensure that appropriate penalties are imposed on those who commit identity theft.

Advances in identification technology

Fraudulent activity can place an immense financial burden on institutions and be devastating for individual victims. For example, in 1994, the UK's Department of Social Security suffered an estimated loss of one billion pounds to benefit fraud. On an individual level, victims of identity theft may suffer consequences beyond financial loss such as the problems posed by a bad credit rating or the difficulties of proving that they are not responsible for the acts of the impostor done in their name (Marx 1990). One solution to the problem of identity theft would be to introduce a system of identification that can be more effectively attached to the particular individual to whom it relates. The creation of an effective and accurate method of identifying individuals is essential in terms of increasing the administrative efficiency of institutions and preventing fraud. There are three categories of identification information. First is something that an individual has that is produced as a means of identification such as a security pass or a passport. Secondly, something an individual knows such as mother's maiden name or passwords. The final category of identification is based upon the physical characteristics of the individual. This is known as biometrics and includes such things as fingerprints, DNA and retinal images (Davies 1994).

Forms of identification that fall into the first two categories may prove to be unreliable and particularly amenable to fraudulent misuse. Documents and cards can be lost and information may be forgotten, hence inconveniencing both the individual concerned and the institution that has to issue replacements. Documents and cards are also vulnerable to theft or duplication. These forms of identification may be misused in a straightforward manner, for example, the use of a stolen credit card to purchase goods, or form the basis of a more complex fraud, such as the use of information on a birth certificate to obtain further identification in the victim's name as a basis for total identity theft. Equally, knowledge can fall into the possession of others and be abused, either alone or in conjunction with cards and documents, for example, the use of a bank card (something one has) and a PIN number (something one knows) to withdraw cash from the victim's bank account. Like biographical information, PINs and credit card numbers can be found on websites that randomly generate the sequences of numbers intended to protect genuine credit cards.

Even though many of these forms of identification would not be sufficient to establish a fraudulent identity in isolation, it is important to note that 'a relatively high-integrity identity is constructed by accumulating a collection of low-integrity evidence' (Clarke 1994: 10).

Clarke uses the example of the pensioner who defrauded the Australian Department of Social Security of $40,000 by exploiting the 'entry-point paradox' using 'seed' documents to create multiple identities for the purposes of fraudulent benefit claims. A seed document is one that contains facts relating to a certain event but has nothing intrinsic that associates it with a particular person. A birth certificate, for example, contains detailed information concerning the birth of an individual but there is nothing about it that relates it to the person using it as identification other than an assertion that he or she is the person to whom it relates. Copies of birth certificates are freely available to anyone who is prepared to pay the nominal fee with no restrictions placed upon the categories of person who may obtain a copy. It can be used to obtain various other forms of identification (the entry-point paradox). Hence its role as the seed from which a more complete legal identity can be grown. Unless safeguards are developed to control the misuse of basic forms of personal documentation and to implement more stringent checks when these documents are used to obtain other forms of identification, this type of abuse will continue.

Advances in technology have enabled institutions using documentary and knowledge-based identification systems to overcome some of these pitfalls. In particular, plastic cards have an increased capacity to store information that may make it easier to detect misuse and can carry images of the authorised user and even thumb-print identification. Card readers are able to make speedy checks to ensure that cards that are presented have not been reported stolen, and faster communications systems ensure that records of stolen cards are updated far more frequently than has previously been possible. However, just as advances in technology have assisted organisations to combat fraud, criminals have also gained the benefits of relatively low-priced sophisticated equipment that facilitates the production of high-quality duplicates (Carroll 1991). Even the standard of equipment that is readily available in many homes and offices can be used to make convincing duplicates of documents and cards by those with relatively limited technological expertise (Davies 1994). As such, technological advances could be said simultaneously to prevent and facilitate fraudulent behaviour.

It would appear that documents, cards and knowledge-based methods of identification are inherently vulnerable to abuse. Biometric systems avoid many of the problems encountered by these other methods of identification as they are inherently linked to a particular individual and are extremely difficult to reproduce. But what are biometrics?

> The term 'biometrics' is used to refer to any and all of a variety of identification techniques which are based on some physical and difficult-to-alienate characteristic. They are sometimes referred to as 'positive identification' because they are claimed to provide greater confidence that the identification is accurate.
>
> (Clarke 1994:11)

Biometrics are based upon some physical attribute that is (usually) unique to the individual and which, as such, cannot be removed and misused by an impostor. The most frequently used form of biometric identification is fingerprinting. This has been used to fix identity on offenders since the end of the nineteenth century and has come to be used more recently by some countries for the purposes of controlling immigration (Torpey 2000). Computer systems that store and recognise fingerprints have made the process of identification faster and more certain with one Japanese system claiming to be able to match fingerprints in one second with a 99.9 per cent accuracy rate. But despite the clear potential for the expansion of the use of fingerprints as a means of identification, there is a general reluctance to extend their use for more general identification purposes, possibly due to the connotations of criminality (Clarke 1994).

Among other forms of biometrics being developed with personal identification in mind is hand geometry, a technique used to process frequent travellers to the USA using a system known as INPASS (Immigration and Naturalisation Service Passenger Accelerated Service System). It is a voluntary scheme that allows participants to bypass usual airport procedures thereby reducing processing time to a mere 20 seconds. Participants are required to establish their identity in order to register for this scheme. The palm of the hand is scanned and the image is stored on a smart card. At the airport, the passenger inserts the card into a terminal and places his or her hand on a scanner that compares this with the image stored upon the card. The system has a high accuracy rating and has the potential to be implemented in a range of other situations in which there is a need for a fast and reliable means of establishing identity.

Any system that links identifying information irretrievably with a particular individual has clear benefits for eliminating identity theft. Biometrics are, by and large, unique to an individual. Hence the potential for abuse would appear to be minimal. However, the reliability of any system of identification based upon biometrics could be thwarted by the weaknesses of a registration system based upon documentary identification. As has been outlined earlier, a collection of low-integrity forms of identification can be used to establish a convincing fraudulent legal

identity and unless stringent checks are made there would appear to be little to prevent an impostor registering for a scheme such as INPASS that has the appearance of being a wholly reliable means of ascertaining identity. In this way, the weaknesses of low-integrity identification systems are inherited by high-integrity systems, and their apparent infallibility is undermined and eroded.

That said, biometrics have clear advantages over alternative systems of identification in that they appear to be incapable of being mis-appropriated by impostors as they are linked to a single individual. There is little scope for multiple users of the same biometric identity. Hence such a system has much to offer in terms of reducing the prevalence of identity theft. However, there are also significant disadvantages that require consideration. First, such schemes are expensive to develop and implement. This should not pose a serious impediment to their use due to the potentially immense financial benefits of reducing fraud but it is none the less important to appreciate that the costs of introducing these systems may prove to be prohibitive for smaller organisations. However, the potential for 'function creep', whereby forms of identification are adopted for a variety of originally unplanned purposes, is a more pressing cause for concern. As Davies (1994) acknowledges, the existence of a relatively high-integrity scheme might create irresistible temptations on the part of authorities to apply it widely, and inter-relate many hitherto separate collections of personal information. This can be illustrated by reference to the multiplicity of roles that have developed for the social security number in a range of jurisdictions where it is used in connection with taxation, welfare benefit, person entitlement, health care provision, access to education, financial services and even vehicle registration (Clarke 1994). It seems likely that the introduction of a seemingly unassailable biometric identification system could soon be adopted by a range of institutions until it became the default means of establishing identification.

One problem with this is that a system that has the appearance of providing a determinative means of establishing identity may engender a confidence that is not justified. For example, despite the reverence with which the social security number is viewed as a means of identification in the USA, it is estimated that 4.2 million people have managed to acquire alternative numbers. A system of biometric identification must be based upon a reliable registration system that is subject to stringent scrutiny in order to ensure that the potential for fraudulent abuse is minimised. It has been suggested that the most reliable system of identification would be compulsory DNA registration, which would create a foundation for legal identity that is unique to the individual and which would be immune

from replication or adoption by an impostor. Specially developed equipment has increased the speed of DNA testing in recent years and it is likely that portable testing equipment for use at crime scenes is a possibility in the relatively near future. But despite the fact that DNA provides a unique identifier that cannot be transferred between individuals, it would appear that it has no role in combating identity theft because research has failed to establish an effective way in which DNA could be incorporated into a form of personal identification for everyday use. Moreover, public opinion views the introduction of a national DNA database with suspicion, at least outside the criminal justice arena. This is because DNA does more than establish identity; it provides a complete genetic profile that can identify up to 400 diseases, legitimacy at birth, etc., and there is a growing body of research claiming that specific genes can predict future substance addiction, sexual orientation, and criminal and violent tendencies. As such, a system of identification based upon DNA profiling could lead to the stratification of society, creating a Brave New World based upon genetic elitism that would exacerbate the exclusionary impact of an unavoidable system of identification. At the risk of combining dystopias, such a system would also engender opposition as it would risk giving the state a Big Brother-esque omniscience by facilitating the creation of a unified and comprehensive database of information about individuals that is linked to public fears concerning the creation of an Orwellian surveillance state. The extent of public opposition to a state-controlled multipurpose identification scheme is accepted as one of the greatest impediments to the introduction of the fully cross-referenced and rigorously validated system of identification that would be necessary to eliminate identity theft (Clarke 1994; Davies 1994; Marx 2001). Therefore, while DNA profiling remains an invaluable tool in the identification of offenders, it is unlikely to expand beyond that into everyday use, at least in the near future (Safir and Reinharz 2000).

One theme that has emerged during the course of this chapter concerns the irreconcilable interests that are at stake within the identity discourse. In order to eliminate identity theft, it would be necessary to reconstruct the whole system of identification that is currently in existence. Not only would this be a lengthy, complex and expensive procedure, it would also have unpleasant consequences for individuals who, for whatever reason, feel compromised by some aspect of their legal identity. It is important not to overlook the dichotomy that exists within identity theft in terms of motivation. While society may wish to detect and punish those who engage in fraudulent behaviour, there are also those who have resorted to identity theft in order to escape some aspect of their own identity with which they no longer wish to be associated. The

creation of a widespread and reliable system of identification would increase the pressure on such individuals and force them to choose between disclosure/exposure and exclusion. Moreover, there is evidence to suggest that there would be widespread public opposition to the concentration of personal information in a single system of identification that would be controlled by the state. If the strengthening of the system of identification is not the solution, it may be that the answer to the problems of identity are to be found within the criminal justice system.

The legal response to identity theft

In response to concerns about the growth of identity theft, the Identity Theft and Assumption Deterrence Act 1998 was introduced in the USA. The objectives of this statute were threefold: to ensure that the individuals whose identities were misused were viewed as the primary victims of identity theft; to establish more stringent penalties for offenders; and to empower the Federal Trade Commission to introduce procedures for educating the public, receiving complaints and co-ordinating the enforcement of the law. This tripartite attack on identity theft provides a cohesive response to the problem and has been generally well received as a significant improvement in the law (Saunders and Zucker 1999; Buba 2000). However, one limitation to the scope of the legal protection available in the USA is that the offence of identity theft is only established if it is carried out with the intention of engaging in unlawful activity. It is likely that this excludes escape cases from the remit of the law as such cases would lack the requisite criminal intention. The issue of whether escape cases and criminal identity theft are equally morally reprehensible is a complex one that is outside the scope of this chapter. However, the differing motivations may be of little relevance to the victim of identity theft who has to deal with the inconvenience of reclaiming his or her identity.

Notwithstanding this lacuna, it is clear that legal protection in the USA is vastly superior to that of the English criminal justice system where identity theft is as yet unrecognised as a distinct criminal offence. The offences contained in the Theft Act 1968 are unlikely to cover identity theft per se although there are a number of offences that would encompass fraudulent activity using another's identity, such as obtaining property by deception (s. 15) or obtaining a pecuniary advantage by deception (s. 16). The difficulty of this position is that the law does not focus on the misuse of the identity but on the financial consequences of this misuse. Therefore, if the individual has not carried the financial loss

of the fraudulent transactions, he or she has no status as a victim in criminal law. This fragmentation of identity theft into a series of composite transactions overlooks the harm that can accrue to an individual as a result of the misuse of his or her identity even if it does not involve direct financial loss. The exclusive focus on the pecuniary elements of the conduct also impacts upon the level of penalty that is likely to be imposed on conviction as the seriousness of the conduct is measured in monetary terms. Again, this is different from the position in the USA where the quantum of loss is only one of the factors to be taken into account when determining the severity of the crime for sentencing purposes. Other factors that are considered relevant are the level of planning involved, the level of sophistication of the role of the perpetrator, the number of victims and, crucially, the susceptibility and status of the victim. Although the provisions of the Theft Act 1968 can be used to address certain manifestations of the problem, the absence of a specific offence of identity theft that recognises the impact of the conduct on the individual whose identity is misappropriated is a significant weakness in English law. However, the absence of any recognition of the harm caused, both individually and to society in general, of identity theft suggests that any amendment to the law may be far into the future.

Conclusion

This chapter has outlined the various manifestations of conduct that has come to be labelled identity theft and has explored several explanations that could account for its increase in today's society. It has been suggested that the ease with which it is possible to obtain various forms of identification in another's name has played a significant role in the rising crime of identity theft. In particular, it has been argued that the expansion of the use of the Internet has led to virtually unrestricted access to personal information about other people as well as providing increased opportunities to engage in fraudulent behaviour. This chapter has not sought to engage with the debate regarding the regulation of the Internet (see Chapter 2, this volume), preferring to argue that it may be appropriate to consider placing limitations on the availability of personal information about individuals regardless of their source. However, any privacy-based argument is liable to be countered by an equally compelling assertion based upon the need for the free flow of information in a democratic society, hence illustrating the competing interests that underpin any discussion of identity theft. Suffice it to say that a continued escalation of identity theft may ultimately necessitate a thorough re-

evaluation of the way in which access to personal information used for identification purposes is organised and controlled.

As has been seen, identity theft may also be committed so that an individual can escape his or her own legal identity and adopt another that enables him or her to have a fresh start unencumbered by some troublesome element of his or her past. This type of identity theft has received very little attention in the existing literature. It creates an anomalous situation in which any measures introduced to limit the adoption of another's identity actually increase the pressure on individuals who wish to abandon their own legal identity. This situation is a cause for concern as one way in which identity theft could be reduced is by the introduction of a more stringent system of identification that cannot easily be misappropriated by others. However, such a system would place increased pressure on those with spoiled identities and might ultimately lead to their exclusion from a range of social activities and benefits. The ubiquitous requirement of identifiability has created this tension and raises further questions concerning the individual's right to privacy that need to be addressed in a broader social context.

The chapter concludes by considering the legislative approach to identity theft in the USA and comparing that with the position in the English criminal justice system. Although the creation of a specific criminal offence to address identity theft appears to be a positive measure, it is likely that a criminal law response would not suffice in isolation to address the problem. Institutions engaging in financial transactions, especially Internet transactions, need to become more aware of the dangers of identity theft and may have to question the validity of identification that is presented to them. Individuals need to become more aware of the risk of identity theft and require education that would enable them to adopt sensible security precautions to protect their personal information. Until such a time as measures are taken to address identity theft in the UK, it appears that there is little to prevent an unscrupulous individual accumulating debt or even committing murder while claiming to be you!

References

Abercrombie, N. and Longhurst, B. (1998) Audiences. London: Sage.

Adam, A. and Green, E. (1998) Gender, agency, location and the new information society. In B. Loader (ed.) Cyberspace Divide: Equality, Agency and Policy in the Information Society. London: Routledge.

Aggleton, P. (ed.) (1999) Men Who Sell Sex: International Perspectives on Male Prostitution and HIV/AIDS. London: UCL Press.

Agustin, L. (1999) They speak but who listens? In W. Harcourt (ed.) Women@Internet. London: Zed.

Annandale, E. and Clarke, J. (1996) What is gender? Feminist theory and the sociology of human reproduction. Sociology of Health and Illness 18(1): 17-34.

Arizpe, L. (1999) Freedom to create: women's agenda for cyberspace. In W. Harcourt (ed.) Women@lnternet. London: Zed.

Arnold, E.L. and Plymire, D.C. (2000) The Cherokee Indians and the Internet. In D. Gauntlett (ed.) Web.studies: Rewiring Media Studies for the Digital Age. London: Arnold.

Ashurst, P. and Hall, Z. (1989) Understanding Women in Distress. London: Routledge.

Ault, A. (1999) Ambiguous identity in an unambiguous sex/gender structure: the case of bisexual women. In M. Storr (ed.) Bisexuality: A Critical Reader. London: Routledge.

Barlow, J.P. (1990) Crime and puzzlement. Whole Earth Review, Fall: 44-57.

Barney, D. (2001) Say good-bye to privacy, wzow.networkcomputing.com, 29 October: unpaginated

Baszanger, I. and Dodier, N. (1997) Ethnography: Relating the part to the whole. In D. Silverman (ed.) Qualitative Research Theory Methods and Practice. London: Sage.

Becker, H. (1963) Outsiders: Studies in the Sociology of Deviance. New York: Free Press.

Belausteguigoitia, R.M. (1999) Crosssing borders: from crystal slippers to tennis shoes. In W. Harcourt (ed.) Women@Internet. London: Zed.

Bell, D. and Kennedy, B.M. (eds.) (2000) The Cybercultures Reader. London: Routledge.

Bellos, A. (2001) Alternative views find their place in the sun. Guardian Unlimited, www.guardian.co.uk/archive 27 January: unpaginated.

Bendle, M.F. (2002) The crisis of 'identity' in high modernity. British Journal of Sociology 53:1-18.

Boorsook, P. (2000) Cyberselfish: A Critical Romp through the Terribly Libertarian World of High-Tech. London: Little Brown & Co.

Born, M. (1999) Country's first email stalker is convicted. Electronic Telegraph issue 1398, 24 March (www.intelsec.demon.co.uk/index.htm?ref=stalking/litigate/pha/index.htm).

Bostock, R. (1993) Consumption. London: Routledge.

Branwyn, G. (2000) Compu-sex: erotica for cybernauts. In D. Bell and B. Kennedy (eds.) The Cybercultures Reader. London: Routledge.

Bright, M. (1999) They're watching you. Observer (Guardian Unlimited) www.guardian.co.uk/archive 29 August: unpaginated.

Brooks, J. and Boal, I. (eds.) (1995) Resisting the Virtual Life: The Culture and Politics of Information. San Franciso, CA: City Lights.

Brooks, L. (1999) Private lives. Guardian Unlimited www.guardian.co.uk/archive 2 November: unpaginated.

Buba, N.M. (2000) Waging war against identity theft: should the United States borrow from the European Union's battalion? Suffolk Transnational Law Review 23: 633-65.

Budd, T. and Martinson, J. (2000) The Extent and Nature of Stalking: Findings from the 1998 British Crime Survey. London: Home Office Research, Development and Statistics Directorate.

Butterworth, D. (1993) Wanking in cyberspace. Trouble & Strife 27, Winter: 33-37.

Cant, S. (2001) Courts wrangle over cyberstalking. E-Commerce News 26 March (http://it.mycareer.com.au/e-commerce/20010326/A32026-2001Mar26.html).

Carroll, J.M. (1991) Confidential Information Sources (2nd edn.). New York: Butterworths.

Castells, M. (1996) The Rise of the Network Society. Maiden, MA: Blackwell.

Cavanagh, A. (1999) Behaviour in public? Ethics in online ethnography. Cybersociobgy 6 (www.socio.demon.co.uk): unpaginated.

Chandler, D. (1998) Personal Home Pages and the Construction of Identities

Clarke, R. (1994) Human identification in information systems: management challenges and public policy issues. *Information Technology and People* 7: 6-37.

Clough, B. and Mungo, P. (1992) *Approaching Zero: Data Crime and the Computer Underworld.* London: Faber & Faber.

Cloughlan, S. (2000) Fraud's on the cards. *Guardian Unlimited* (www.guardian.co.uk/archive) 15 July: unpaginated.

CNET Networks (2000) *Cyberstalkers* (http://coverage.cNet.com/Content/ l˙e-atures/Dlife/Dark/ss01a.html).

Cohen, A. (2001) Internet insecurity. *Time 2* July: 44-52.

Cole-man, S., Taylor, J. and van de Donk, W. (1999) *Parliament in the Age of the Internet.* Oxford: Oxford University Press.

Congress 106th (2000) *just Punishment for Cyberstalkers Act of 2000,* s. 2991 (available at http://thomas.loc.gOv/cgi-bin/bdquery/z7dl06:s.02991).

Con ley, V. (1993) *Rethinking Technologies.* Oxford, OH: Miami University Press.

Council, R. (1987) *Gender and Power: Society, the Person and Sexual Politics.* Sydney: Allen & Unwin.

Corea, G., Klein, R.D., Hanmer,]., Holmes, H.B., Hoskins, B., Kishwar, M., Raymond, J., Rowland, R. and Steinbacker, R. (eds.) (1985) *Man-Made Women: How New Reproductive Technologies Affect Women.* London: **Hutchinson.**

Cornwell, R. (2002) Intercepted email traffic points to new al-Qa'ida grouping in remote Pakistan. *Independent* 7 March: 3.

Correll, S. (1997) The ethnography of an electronic bar: the lesbian cafe. *Journal of Contemporary Ethnography* 24(3): **270-98.**

Coupland, D. (1995) *Microserfs.* London: Flamingo.

Curran, J. and Seaton, J. (1991) ***Power without Responsibility: The Press and Broadcasting in Britain*** (4th edn.). London: Routledge.

Curzon-Brown, D. (2000) The teacher review debate part II: the dark side of the **Internet. In D. Gauntlett (ed.)** ***Web.studies: Rewiring Media Studies for the Digital Age.*** London: Arnold.

Cyber-Rights and Cyber-Liberties (UK) Report (1998) Who watches the watchmen part II: accountability and effective self-regulation in the information age. September (available at www.cyber-rights.org.watchmen-ii.htm).

Danet, B. (1996) Text as mask: gender and identity on the Internet. Paper presented at the Masquerade and Gendered Identity conference, Venice, Italy, 21-24 February (available at http://atar.mscc.huji.ac.il/-msdanet/ mask.html).

Dann, J. and Dozois, G. (1996) *Hackers.* New York: Ace Books.

Davies, S.D. (1994) Touching Big Brother: how biometric technology will fuse flesh and machine. *Information Technology and People* 7(4) (available at www.privacy.org/pi/reports/biometric.hhnl): unpaginated.

Davis, K. (1971) Prostitution. In R.K. Merton and R. Nisbet (eds.) *Contemporary Social Problems.* London: Hart-Davies.

Davis, R. (1999) *The Web of Politics. The Internet's Impact on the American Political System.* Oxford: Oxford University Press.

Diani, M. (2001) Social movement networks: virtual and real. In F. Webster (ed.) *Culture and Politics in the Information Age: A New Politics?* London: Routledge.

Di Filipo, J. (2000) Pornography on the web. In D. Gauntlett (ed.) *Web.studies: Rewiring Media Studies for the Digital Age.* London: Arnold.

Di Giovanni, J. (1996) Losing your voice on the Internet. In P. Ludlow (ed.) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace.* Cambridge, MA: MIT Press.

Dobash, R. and Dobash, R. (1980) *Violence against Wives.* Shepton Mallet: Open Books.

Dunne, M. (1997) Southall black sisters. *Third World Network* (www.hartford-hwp.com/archives/61/061 .html).

Dworkin, A. (1981) *Pornography: Men Possessing Women.* London: The Women's Press.

Edwards, S.S.M. (1993) Selling the body, keeping the soul: sexuality, power, the theories and realities of prostitution. In S. Scott and D. Morgan (eds.) *Body Matters: Essays on the Sociology of the Body.* London: Falmer Press.

Ellis, H.H. (1936) *Studies in the Psychology of Sex. Vol.* 3. New York: Random House.

Ellison, L. and Akdeniz, Y. (1998) Cyber-stalking: the regulation of harassment on the Internet. *Criminal Law Review* 29 (special edition, December): 29-48.

Epstein, S. (1997) A queer encounter: sociology and the study of sexuality, hi S. Seidman (ed.) *Queer Theory/Sociology.* Oxford: Blackwell.

Exley, C. and Letherby, G. (2001) Managing a disrupted lifecourse: issues of identity and emotion work. *Health* 5(1): 112-32.

Federal Trade Commission (2000) *Identity Theft.* Washington, DC: Federal Trade Commission.

Federal Trade Commission (2002) *Identity Theft: The FTC's Response.* Washington, DC: Federal Trade Commission.

Fiddy, A (2001) The Internet twins. *Childright* 173 (January/February): 12-13 (available at www2.essex.ac.uk/clc/hi/childright/article/002.htm).

Foucault, M. (1979) ***Discipline and Punish: The Birth of the Prison.*** **New York:** Vintage.

Fox, N. and Roberts, C. (1999) GPs in cyberspace: the sociology of a 'virtual community'. *The Sociological Review* 47(4): 643-71.

Franklin, S. (1990) Deconstructing 'desperateness': the social construction of infertility in popular representations of new reproductive technologies. In M.V. McNeil and S. Yearley (eds.) *The New Reproductive Technologies.* London: Macmillan.

Freundlich, M. and Phillips, R. (2000) Ethical issues in adoption. *Adoption and Fostering* 24(4): 7-17.

George, S. (1999) Extracts from women and bisexuality. In M. Storr (ed.) *Hisexualiti/: A Critical Reader.* London: Routledge.
Gibson, W. (1984) *Neuromancer.* London: Grafton.
Gibson, W. (1986) *Burning Chrome.* London: Grafton.
Giddens, A. (1990) *Consequences of Modernity.* Cambridge: Polity Press.
Gilboa, N. (1996) Elites, lamers, narcs and whores: exploring the computer underground. In L.L. Cherny and E.R. Weise (eds.) *Wired Women: Gender and New Realities in Cyberspace.* Seattle, WA: Seal Press.
Gillespie, T. (2000) Virtual violence? Pornography and violence against women on the Internet. In J. Radford *et al* (eds.) *Women, Violence and Strategies for Action: Feminist Research, Policy and Practice.* Buckingham: Open University Press.
Gillies, J. and Cailliau, R. (2000) *How the Web was Born: The History of the World Wide Web.* Oxford: Oxford University Press.
Gleason, P. (1983) Identifying identity - a semantic history. *Journal of American History* 69: 910-31.
Glodava, M. and Onizuka, R. (1994) *Mail-Order Brides: Women for Sale.* Fort Collins, CO: Alaken.
Goffman, E. (1959) *The Presentation of Self in Everyday Life.* London: Penguin Books.
Goffman, E. (1963) *Stigma: Notes on the Management of Spoiled Identity.* Englewood Cliffs, NJ: Prentice-Hall.
Goffman, E. (1974) *Frame Analysis.* New York: Harper & Row.
Goodwins, R. (1993) Motley bunch hack at the end of the universe. The Independent 13 August: 11.
Grafx-Specs Design and Hosting (1997) Cyberstalking: A Real Life Problem (http: / / grafx-specs.com/News/Cybstlk.html).
Greene, T. (2001) Australia Outlaws Email Forwarding (www.theregister.co.uk/ content/6/).
Gregorie, M.T. (2001) Cyberstalking: The Dark Side of the Information Superhighway. National Center for Victims of Crime (www.ncvc.org/newsltr/networks).

Hamelink, C.J. (2000) The Ethics of Cyberspace. London: Sage.
Hamman, R. (1997) The application of ethnographic methodology in the study of cybersex. Cybersociology 1 (www.socio.demon.co.uk): unpaginated.
Hanmer, J. (1997) Women and reproduction. In V. Robinson and D. Richardson (eds.) Introducing Women's Studies. Basingstoke: Macmillan.
Harcourt, W. (ed.) (1999) Women@Mernet. London: Zed.
Harvey, N. (1998) The Chiapas Rebellion: The Struggle for Land and Democracy. Durham, NC: Duke University Press.
Hay wood, T. (1998) Global networks and the myth of equality: trickle down or trickle away? In B. Loader (ed.) Cyberspace Divide: Equality, Agency and Policy in the Information Society. London: Routledge.
Heikkila, P. (2001) Defacements increase five-fold in 2001 (www.silicon.com) 11 January: unpaginated

Hillyard, P. and Percy-Smith, J. (1988) *The Coercive State: The Decline of Democracy in Britain.* London: Fontana.
Himanen, P. (2001) *The Hacker Ethic and the Spirit of the Information Age.* London: Vintage.
HMSO (1998) *Supporting Families.* London: HMSO.
Holderness, M. (1998) Who are the world's information-poor? In B. Loader (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society.* London: Routledge.
Homan, R. (1991) *The Ethics of Social Research.* Harlow: Longman.
Hopper, I. (2000) Pirated software subject of suit. *Associated Press* 13 November (available at www.bsa.org).
Hothschild, A.R. (1983) *The Managed Heart.* Berkeley, CA: University of California Press.
Houghton, D. and Houghton, P. (1984) *Coping with Childlessness.* London: Unwin Hyman.
Hughes, D. (1998/9) Men@Exploitation.com. *Trouble & Strife* 38 (Winter): 24.
Hyde, S. (1999) A few coppers change. *Journal of Information, Law and Technology* (available at http://elj.warwick.ac.uk/jilt/99-2/hyde.html).

Illingworth, N. (2001) The Internet matters: exploring the use of the Internet as a research tool. Sociological Research Online 6(2) (www.socresonline.org.uk): unpaginated.

Jacobs, S., Jacobson, R. and Marchbank, J. (eds.) (2000) States of Conflict: Gender, Violence and Resistance. London: Zed.
Jordan, T. (1999) Cyberpower: The Culture and Politics of Cyberspace and the Internet. London: Routledge.
Juniper, T. (2002) It's your shout. Guardian Unlimited 13 February (www.guardian.co.uk/archive): unpaginated.

Kaloski, A. (1997) Extracts from bisexuals making out with cyborgs: politics, pleasure, con/fusion. In M. Storr (ed.) Bisexuality: A Critical Reader. London: Routledge.
Karp, H. (2000) Angels online. Reader's Digest: 34-40.
Katz Rothman, B. (1994) Beyond mothers and fathers: ideology in a patriarchal society. In E. Nakono Glenn et al (eds.) Mothering, Experience and Agency. New York: Routledge.
Keck, M.E. and Sikkink, K. (1998) Activists beyond Borders: Transnational Advocacy Networks in International Politics. Ithaca, NY: Cornell University Press.
Keller, L.S. (1988) Machismo and the hacker mentality: some personal observations and speculations. Paper presented to the WiC (Women in Computing) conference.
Kemp, A. (1999) Dark side of the Net is forced into the light. Observer (Guardian Unlimited) (www.guardian.co.uk/archive) 17 October: unpaginated.

Kitzinger, J. (1999) The ultimate neighbour from hell? Stranger danger and the media framing of paedophiles. In B. Franklin (ed.) *Social Policy, the Media and Misrepresentation.* London: Routledge.

Kofman, E., Phizacklea, A., Raghiram, P. and Sales, R. (2000) *Gender and International Migration in Europe: Employment, Welfare and Politics.* London: Routledge.

Kolko, B., Nakamura, L. and Rodman, G.B. (2000) Race in cyberspace: an introduction. In B. Kolko *et al* (eds.) *Race in Cyberspace.* New York: Routledge.

Krafft-Ebing, R. von (1901) *Psychopathia Sexnalis.* London: Rebman.

Krueger M.W. (1991) *Artificial Reality II.* Reading, MA: Addison-Wesley.

Laing, R. (1960) *The Divided Self.* Harmondsworth: Penguin Books,

Langford, D. (1998) Ethics @ the Internet: bilateral procedures in electronic communication. In B. Loader (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society.* London: Routledge.

Lathouwers, R. and Happ, A. (2000) The teacher review debate part I: just what the Internet was made for. In D. Gauntlett (ed.) *Web.studies: Rewiring Media Studies for the Digital Age.* London: Arnold,

Laughren, J. (2000) *Cyberstalking Awareness and Education* (www.ucalgary.ca/~dabrent/380/webproj/jessica.html).

Left, S. (2002) Casting the net for paedophiles. Guardian Unlimited (www.guardian.co.uk/archive) 24 April: unpaginated.

Lenk, K. (1997) The challenge of cyberspatial forms of human interaction to territorial governance and policing. In B. Loader (ed.) The Governance of Cyberspace: Politics, Technology and Global Restructuring. London: Routledge.

Letherby, G. (1994) Mother or not, mother or what: the problem of definition. Women's Studies International Forum 17:524-32.

Letherby, G. (1999) Other than mother and mothers as others: the experience of motherhood and non-motherhood in relation to 'infertility' and 'involuntary childlessness'. Women's Studies International Forum 22(3): 359-72.

Letherby, G. and Williams, C. (1999) Non-motherhood: ambivalent auto-biographies. Feminist Studies 25(3): 719-28.

Levy, S. (1984) Hackers: Heroes of the Computer Revolution. New York: Bantam Doubleday Dell.

Loader, B. (1997) The governance of cyberspace: politics, technology and global restructuring. In B. Loader (ed.) The Governance of Cyberspace: Politics, Technology and Global Restructuring. London: Routledge.

Loader, B. (1998) Cyberspace divide: equality, agency and policy in the information society. In B. Loader (ed.) Cyberspace Divide: Equality, Agency and Policy in the Information Society. London: Routledge.

Lynch, D. (2000) Wired women: it's a guy thing - why are there so few female hackers? ABCNEWS.com (available at http://abcnews.go.com/sections/tech/WiredWomen/wiredwomen000223.html).

Marchbank, J. (2000) Women, Power and Policy: Comparative Studies of Childcare. London: Routledge.

Margolis, M. and Resnick, D. (2000) *Politics as Usual: The Cyberspace Revolution.* Thousand Oaks, CA: Sage.

Marx, G.T. (1990) Fraudulent identification and biography. In D. Altheide (ed.) *Law and Social Control: New Directions in the Study of Justice.* New York: Plenum Publishing.

Marx, G.T. (2001) Identity and anonymity: some conceptual distinctions and issues for research. In J. Caplan and J. Torpey (eds.) *Documenting Individual Identity.* Princeton, NJ: Princeton University Press.

McGibbon, A. (2001) Beware the security enemy within. Network News 13 June (www.vnu.com).

McKeganey, N. and Barnard, M. (1996) *Sex Work on the Streets: Prostitutes and their Clients.* Buckingham: Open University Press.

McLaughlin, M.L., Osborne, K. and Smith, C. (1994) Standards of conduct on *Usenet.* In S.G. Jones (ed.) *Cybersociety: Computer-mediated Communication and Community.* London: Sage.

Melucci, A. (1996) *Challenging Codes: Collective Action in the Information Age.* Cambridge: Cambridge University Press.

Meyrowitz, J. (1985) *No Sense of Place: The Impact of Electronic Media on Social Behaviour*. Oxford: Oxford University Press.

Meyrowitz, J. (1989) The generalised elsewhere. *Critical Studies in Mass Communication* 6(3): 326-34.

Middleton, J. (2000) EC calls for end of anonymous email. Network News 18 April (www.vnunet.com).

Middleton, J. (2001) Hacking could become an act of terrorism. Network News 26 September (www.vnunet.com).

Miller, H. (1995) The presentation of self in electronic life: Goffman on the Internet. Paper presented at the Embodied Knowledge and Virtual Space conference, Goldsmiths' College, University of London, June (available at www.ntu.ac.uk/soc/psydi/miller/goffman.html).

Moreiras, A. (1993) The leap and the lapse: hacking a private site in cyberspace. In V. Conley (ed.) Rethinking Technologies. Oxford, OH: Miami University Press.

Morley, D. and Robins, K. (1995) Space of Identity, Global Media, Electronic Landscapes and Cultural Boundaries. London: Routledge.

Mulgan, G.J. (1994a) Politics in an Antipolitical Age. Cambridge: Polity Press.

Mulgan, G.J. (1994b) After the End of Politics. Occasional Paper 2. Sheffield: University of Sheffield.

Murray, N. (2001) Hyper-nationalism and our dvil liberties. Paper presented at the After September 11: Paths to Peace, Justice and Security conference, organised by the American Friends Service Committee and Tufts University's Peace and Justice Studies Program and Peace Coalition, 7-8 December, Medford, MA (available at www.afsc.org/nero/pesp/murray.htm).

National Center for Victims of Crime (2001) Cyberstalking (wwwjivc.org/spedal/cyber).

Naughton, J. (1999) *A Brief History of the Future: The Origins of the Internet.* I ondon: Phoenix.
Newman, J.Q. (1999) *Identity Theft: The Cybercrime of the Millennium.* Port Townsend: Loompanics.
Norris, P. (2001) *Digital Divide: Civil Engagement, Information, Poverty and the Internet Worldivide.* Cambridge: Cambridge University Press.

O'Connell Davidson, J. (1998) *Prostitution, Power and Freedom.* Cambridge: Polity Press.
Ogilvie, E. (2000) *Cyberstalking* 166. Canberra: Australian Institute of Criminology.

Paglia, C. (1990) *Sexual Personae: Art and Decadence from Nefertiti to Emily Dickinson.* London: Penguin Books.
Patrick, J. (1973) *A Glasgow Gang Observed.* London: Eyre Methuen.
Perry, B. (2001) *In the Name of Hate: Understanding Hate Crimes.* New York: Routledge.
Perry,]. (ed.) (1975) *Personal Identity.* Berkeley, CA: University of California Press.
Petchesky, R. (1987) Fetal images: the power of visual culture in the politics of reproduction. In M. Stanworth (ed.) Reproductive Technologies: Gender, Motherhood and Medicine. Cambridge: Polity Press.
Peterson, J. (Agent Steal) (1997) Everything a hacker needs to know about getting busted by the feds (available at www.grayarea.com/agsteal.html).
Petherick, W. (1999) Cyber-stalking: obsessional pursuit and the digital criminal. The Crime Library (www.crimelibrary.com/crirninology/cyberstalking/ index.html).
Pettman, JJ. (1996) Worlding Women: A Feminist International Politics. London: Routledge.
Pfeffer, N. (1993) The Stork and the Syringe. Cambridge: Polity.
Pheterson, G. (1993) The whore stigma: female dishonour and male unworthiness. Social Text 37: 39-54.
Phizacklea, A. (1996) Women, migration and the state. In S. Rai and G. Iievesley (eds.) Women and the State: International Perspectives. London: Taylor & Francis.
Plant, S. (2000) On the matrix: cyberfeminist simulations. In D. Bell and B.M. Kennedy (eds.) The Cybercultures Reader. London: Routledge.
Plummer, K. (1975) Sexual Stigma. London: Routledge & Kegan Paul.
Plummer, K. (1997) Symbolic interactionism and the forms of homosexuality. In S. Seidman (ed.) Queer Theory I Sociology. Oxford: Blackwell.
Plumridge, E. (2001) Rhetoric, reality and risk outcomes in sex work. Health, Risk and Society 3(2): 199-215.
Plumridge, E., Chewynd, J., Reed, A. and Gifford, S. (1997) Discourses of emotionality in commercial sex: the missing client voice. Feminism and Psychology 7:228-43.
Pryce, A. (2001) Caught in a web of dangerous liaisons (www.independent.co.uk) 1 February: unpaginated.

Ramsay, K. (1998) Electronic stalkers at large: tracking down harassment in cyberspace. *Technological Crime Bulletin* (www.rcmp-grc.gc.ca/html/te-crime2x.htm).
Ravetz, J. (1998) The Internet, virtual reality and real reality. In B. Loader (ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society.* London: Routledge.
Reid, E.M. (1996) Text-based virtual realities: identity and the cyborg body. In P. Ludlow (ed.) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace.* Cambridge, MA: MIT Press.
Rheingold, H. (1994) The Virtual Community: Surfing the Internet. London: Minerva.
Roberts, C, Kippax, S., Waldby, C. and Crawford, J. (1995) Faking it: the story of 'Ohh!' Women's Studies International Forum 18(5/6): 523-32.
Robertson Elliot, F. (1986) The Family: Change or Continuity. Basingstoke: Macmillan.
Rose, D. (2001) Resentful West spurned Sudan's key terror file. Observer (Guardian Unlimited) (www.guardian.co.uk/archive) 30 September: unpaginated.
Roseneil, S. (2000a) Towards an Understanding of Postmodern Transformations of Sexuality and Cathexis (www.leeds.ac.uk/cava/files/).
Roseneil, S. (2000b) Queer tendencies: towards an understanding of post-modern transformations of sexuality. Sociological Research Online 5(3) (www.socresonline.org.uk): unpaginated.
Ross, A. (1991) Strange Weather: Culture, Science and Technology in the Age of Limits. London: Verso.
Rowland, D. (1998) Cyberspace - a contemporary Utopia. Journal of Information, Law and Technology 3 (available at www.law.warwick.ac.uk/jilt/98-3/ rowland.html): unpaginated.
Rutter, J. (2000) Identity is ordinary: presentations of self in everyday life online. Paper presented to the Virtual Society? Get Real! conference, University of Oxford, 4-5 May (available at http://virtualsociety.sbs.ox.ac.uk/).

Safir, H. and Reinharz, P. (2000) DNA testing: the next crime-busting breakthrough. City Journal 10:49-57.
Sagan, S. (1995) Sex, lies and cyberspace. Wired Magazine 3.01 (www.wired.com/ wired/archive/3.01/sex.lies.typing).
Sannicolas, N. (1997) Erving Goffman, dramaturgy, and online relationships. Cybersociology 1 (www.socio.demon.co.uk).
Sansam, M. (1992) Bi-o-logical. In P. McNeil et al (eds.) Women Talk Sex: Auto-biographical Writing on Sex, Sexuality and Sexual Identity. London: Scarlett Press.
Saunders, K.M. and Zucker, B. (1999) Countering identity fraud in the information age; the Identity Theft and Assumption Deterrence Act. International Review of Law Computers and Technology 13:183-92.
Savill, R. (2001) Internet stalker gets seven years. Electronic Telegraph issue 2119 (available at www.telegraph.co.uk/).

Scambler, G. and Scambler, A. (1997) Afterword: rethinking prostitution. **In** (i. Scambler and A. Scambler (eds.) *Rethinking Prostitution: Purchasing Sex in the 1990s*. London: Routledge.
Scambler, G. and Scambler, A. (1999) Health and work in the sex industry. In N. Daykin and L. Doyal (eds.) *Health and Work: Critical Perspectives*. London: Macmillan.
Scannell, P. (1996) *Radio, Television and Modern Life*. Oxford: Blackwell.
Schofield, J. (2002) Can the spam. *Guardian Unlimited* (www.guardian.co.uk/archive) 25 April: unpaginated.
Scholes, RJ. (1999) The 'mail-order bride' industry and its impact on US immigration. Appendix A, INS (Immigration and Naturalization Service) (available at www.ins.usdoj.gov/graphics/aboutins/repsstudies/mobappa.htm).
Sedgwick, E.K. (1991) *Epistemology of the Closet.* Hemel Hempstead: Harvester Wheatsheaf.
Segan, S. (2000a) Part I: hacker women are few **but** strong (available at: http://abcnews.go.com/sections/tech/DailyNews/hackerwomen000602.html#top).
Segan, S. (2000b) Part II: female hackers face challenges (available at: http://abcnews.go.com/sections/tech/DailyNews/hackerwomen000609.html).
Seidman, S. (ed.) (1997) Queer Theory/Sociology. Oxford: Blackwell.
Seidman, S., Meeks, C. and Traschen, F. (1999) Beyond the closet? The changing social meaning of homosexuality in the United States. Sexualities 2(1): 9-34.
Sider, T. (2001) Four Dimensions: An Ontology of Persistence and Time. Oxford: Clarendon Press.
Slattery, M. (1992) Key Ideas in Sociology. London: Macmillan.
Slevin, J. (2000) The Internet and Society. London: Routledge.
Smelik, A. (2000) Die virtuele matrix: het lichaam in cyberpunkfilms. Tijdschrift voor Genderstudies 3(4): 4-13.
Smith, J. (1989) Misogynies. London: Faber & Faber.
Spallone, P. (1989) Beyond Conception: The New Politics of Reproduction. London: Macmillan.
Spender, D. (1995) Nattering on the Net: Women, Power and Cyberspace. Melbourne: Spinifex Press.
Spring, T. (1999) Hacker tool targets windows NT. PC World.com (www.pcworld.com/pcwtoday/article/).
Springer, C. (1996) Electronic Eros: Bodies and Desire in the Postindustrial Age. Austin, TX: University of Texas Press.
Stanko, E.A. (1985) Intimate Intrusions. London: Routledge & Kegan Paul.
Stanley, L. and Wise, S. (1993) Breaking out again: Feminist Ontology and Feminist Epistemology. London: Routledge.
Stanworth, M. (ed.) (1987) Reproductive Technologies: Gender, Motherhood and Medicine. Cambridge: Polity Press.
Stone, A.R. (1995) The War of Desire and Technology at the Close of the Mechanical Age. Cambridge, MA: MIT Press.

Strathern, M. (1992) The meaning of assisted kinship. In M. Stacey (ed.) *Changing Human Reproduction: Social Science Perspectives*. London: Sage.
Suler, J. (1996) *The Psychology of Cyberspace* (www.rider.edu/users/suler/psycyber/disinhibit.html).
The Sunday Times (2000) Invisible man faked death in Paddington rail crash. 6 February: 9.
Sutherland, J. (2000) How the other you could ruin your life. *Guardian Unlimited* (www.guardian.co.uk/archive) 19 June: unpaginated.
Tang, P. (1997) Multimedia information products and services: a need for 'cybercops'? In B. Loader (ed.) *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge.
Tarrow, S. (1998) *Power in Movement: Social Movements and Contentious Politics*. Cambridge: Cambridge University Press.
Taylor, P.A. (1998) Hackers: cyberpunks or microserfs? *Information Communication and Society* 1(4): 401-19.
Taylor, P.A. (1999) Hackers: Crime in the Digital Sublime. London: Routledge.
Taylor, P.A. (2001) Hacktivism: in search of lost ethics? In D.S. Wall (ed.) Crime and the Internet. London: Routledge.
The Communications Act of 1996,47. U.S.C. 223.
Theobald, S. (1999) Modern lovers. Guardian Unlimited (www.guardian.co.uk/archive) 28 June: unpaginated.
Theobald, S. (2000) To bi or not to bi. Guardian Unlimited (www.guardian.co.uk/archive) 30 March: unpaginated.
Torpey, J. (2000) The Invention of the Passport: Surveillance, Citizenship and the State. Cambridge: Cambridge University Press.
Toxic Shock Group (1990) The evil that hackers do. Computer Underground Digest 2(6): file 4.
Tran, M. (2001) Identity crisis. Guardian Unlimited (www.guardian.co.uk/archive) 5 July: unpaginated.
Triseliotis, J. (2000) Intercountry adoption, global trade or global gift? Adoption and Fostering 24(2): 45-54.
Tsang, D. (2000) Notes on queer 'n' Asian virtual sex. In D. Bell and B.M. Kennedy (eds.) The Cybercultures Reader. London: Routledge.
Turkle, S. (1984) The Second Self: Computers and the Human Spirit. London: Granada.
Turkle, S. (1995) Life on the Screen: Identity in the Age of the Internet. New York: Simon & Schuster.
Turkic S. (1996) Who Am We? Wired Magazine 4.01 (www.wired.com/archive/4.01/turkle).
Ullman, E. (1997) Close to the Machine: Technophilia and its Discontents. San Francisco, CA: City Lights Books.
Usher, J.M. (1997) Fantasies of Femininity: Reframing the Boundaries of Sex. Harmondsworfh: Penguin Books.

US Justice Department (1999) *1999 Report on Cyberstalking: A New Challenge for l.im> Enforcement and Industry*. Washington, DC: US Justice Department.

van Zoonen, L. (2002) Gendering the Internet: claims, controversies and cultures. *l.uivpcan journal of Communication* 17(1): 5-23.

Vidal, J. (1999) Anatomy of a very nineties revolution. *Guardian Unlimited* (wwvv.guardian.co.uk/archive) 13 January: unpaginated.

Virilio, P. (2000) *The Information Bomb*. London: Verso.

Wainwright, H. (2002) Ante upped. *Guardian Unlimited* (www.guardian.co.uk/archive) 13 February: unpaginated.

Wajcman, J. (1991) *Feminism Confronts Technology*. Cambridge: Polity Press.

Wakeford, N. (1997) 'Networking women and grrrls with information/communication technology: surfing tales of the world wide web', in J. Terry and M. Calvert (eds) *Processed Lives: Gender and Technology in Everyday Life*. London: Routledge.

Waldby, C, Kippax, S. and Crawford, J. (1993) Heterosexual men and 'safe sex' practice: research note. *The Sociology of Health and Illness* 15: 246-56.

Walkowitz, J.R. (1980) *Prostitution and Victorian Society: Women, Class, and the State*. Cambridge: Cambridge University Press.

Wall, D. (1997) Policing the virtual community: the Internet, cyberspace and cybercrime. In P. Francis el al (eds.) Policing Futures: The Police, Law Enforcement and the Twenty-First Century. Basingstoke: Macmillan.

Wall, D. (1999) On the politics of policing the Internet: striking the right balance. Paper presented at the Cyberspace 1999: Crime, Criminal Justice and the Internet Bileta conference, College of Ripon and York St John, York, 29-30 March (available at www.bileta.ac.uk/99papers/wall.html).

Wall, D. (2001) Cybercrimes and the Internet. In D. Wall (ed.) Crime and the Internet. London: Routledge.

Wall, D. (2002) Insecurity and the policing of cyberspace. In A. Crawford (ed.) Crime and Insecurity. Cullompton: Willan.

Wegar, K. (1997) In search of bad mothers: social constructions of birth and adoptive mothers. Women's Studies International Forum 20: 77-86.

Weizenbaum, J. (1976) Computer Power and Human Reason. San Francisco, CA: Freeman.

Westin, A.F. and Baker, M.A. (1972) Databanks in Free Society. New York: Quadrangle.

Whine, M. (1997) The far right on the Internet. In B. Loader (ed.) The Governance of Cyberspace: Politics, Technology and Global Restructuring. London: Routledge.

Williams, R. (2001) Making Identity Matter - Identity Society and Social Interaction. Durham: Sociology Press.

Willis, P. (1982) Male school counterculture. In U203 Popular Culture. Buckingham: Open University Press.

Wilton, T. (1999) Selling sex, giving care: the construction of AIDS as a workplace hazard. In N. Daykin and L. Doyal (eds.) Health and Work: Critical Perspectives. London: Macmillan.

Wise, P. (1997) Always already virtual: feminist politics in cyberspace. In D. Holmes (ed.) *Virtual Politics: Identity and Community in Cyberspace*. London: Sage.

Working to Halt Online Abuse (2001) *Online Harassment Statistics for 2000* (www.haltabuse.org/resources/laws/).

Worsnop, J. (1990) A re-evaulation of 'the problem of surplus women' in 19th century England, the case of the 1851 Census. *Women's Studies International Forum* 13(1/2): 21-31.

Wright Mills, C. (1956) *The Power Elite*. Oxford: Oxford University Press.

Zickmund, S. (2000) Approaches to the radical other: the discursive culture of cyberhate. In D. Bell and B.M. Kennedy (eds.) *The Cybercultures Reader*. London: Routledge.

Zizek, S. (1999) *The Plague of Fantasies*. London: Verso.