One increasingly prevalent crime, originating particularly in countries in West Africa, and targeting women in Europe and the US, is online dating scams, whereby fraudsters post bogus photographs and establish relationships with vulnerable victims (sometimes over several months) before persuading them to send them money. In addition, the past few years has seen a massive rise in incidents of so-called 'phishing', in which communications purporting to come from legitimate organizations such as banks and building societies target Internet users, inducing them to voluntarily surrender sensitive financial information which can then be used to defraud them. The extent of such fraud solicitation has reached such levels that the EU has recently launched the Consumer Protection Cooperation Network in an attempt to tackle cross-border Internet scams (Espiner, 2007).

The law also offers protection to individuals whose reputation is slurred by defamatory Internet content. Teachers and lecturers seem particularly vulnerable to such attacks. In 2000, Demon paid over £230,000 to a British university lecturer who claimed that the ISP had failed to remove two anonymous Internet postings defaming him, while in America a 'teacher review' site set up by students at the City College of San Francisco resulted in one teacher filing a lawsuit against the site, denouncing it as a 'disgusting, lie-filled, destructive force' (Curzon-Brown 2000: 91). Since Facebook became the primary mode of communication for many young people, the site has had to respond to many requests from teachers, lecturers and other professionals for unkind and potentially libellous material to be removed.

In providing a forum for discussion among discrete groups (such as the present and past students of a particular teacher) the Internet inevitably makes public what might be assumed to be private, as some students have discovered when fined by their universities for 'breaking the rules' on post-exam celebrations and posting photographic 'evidence' on Facebook. In addition, staff at several universities have reportedly checked personal profiles on networking sites to make decisions about whether or not to admit individual students. Teachers themselves have to be cautious when they make public what they assume might be relatively private statements. In 2006, a former Conservative Party politician successfully sued Tracy Williams, a college lecturer, who had accused him of being a 'Nazi' in an online discussion forum relating to the Iraq war; Williams was ordered to pay at total of £17,200 in damages and costs (Gibson, 2006). Even email is subject to public scrutiny as a case at the Climatic Research Unit at the University of East Anglia in 2009 demonstrated. Following suspicions that leading scientists had misled politicians and the public on aspects of climate change and devised 'tricks' to combat the arguments of climate change sceptics, the Freedom of Information Act (FOI) was used to gain access to thousands of university email communications and other documents.

Another cybercrime related to privacy is the theft of personal identity, a practice that has dramatically increased in the last few years. In 2007, the US

Federal Trade Commission reported that 8.3 million Americans had been victims of identity theft over a 12-month period. Meanwhile, the UK credit-checking agency Experian reported a 69 per cent increase in identity theft over the same period. According to UK government figures, identity theft now costs the British economy £1.7 billion per annum (Home Office, 2006, see http://www.identitytheft.org.uk). Identity theft encompasses a full range of offences from the appropriation and use of credit card numbers to the wholesale adoption of someone else's persona. It can be mundane and opportunistic; for example, many identity thieves rummage through dustbins for discarded credit card statements or pick up receipts left at bank ATMs. However, more high-tech versions include hacking into an individual's personal computer in order to steal his or her bank and credit card details, using software programs designed to work out or randomly generate PIN numbers, and 'skimming' credit cards in shops and restaurants to produce a near perfect copy of the original card. Apart from financial fraud, identity theft has come to be viewed as an important 'precursor' enabling a range of further offences, including illegal immigration and human trafficking using stolen identities (see http://www.met.police.uk/op_maxim/).

Concern over the growth of identity theft has inspired initiatives such as the UK Government's Identity Fraud Steering Committee, which brings together police, government and financial bodies in an attempt to develop a coordinated response. Meanwhile, financial services providers such as banks and credit card companies now routinely offer customers 'identity theft insurance' intended to protect individuals against the consequences of having their identity stolen and used to defraud them. There may be a generational divide in levels of public anxiety, however. On the whole, fears about possible identity theft appear to be more strongly experienced by older people (illustrated, perhaps by the fact that in 2004 sales of shredders increased by 50 per cent at one international supplies company, with 1.3 million units sold in a single year; Jewkes and Yar, 2010). But as Smith (2010) points out, although young people may be more cavalier about their potential for victimization, the expansion in social networking sites has left young people at greater risk of identity crime. By way of example, he notes that one in seven users on Facebook log into their profile virtually all the time during office hours, rendering both themselves and their organizations open to criminal activity.

eBay fraud

Identity theft clearly can be a prelude to fraud, but fraud can be perpetrated via the Internet without recourse to stealing someone else's bank account details, credit card number, or other aspects of their documentary identities. A growing number of criminal offences are facilitated via online auction site

eBay, including the sale of knives and other weapons, metabolic steroids, hard-core pornography and abusive images of children. More mundanely, however, it is goods that are counterfeit, or which breach intellectual copyright laws or are knowingly stolen, faulty or damaged that make up the bulk of the criminal transactions that occur on eBay. Most individual consumers do not pursue legal action when the 'designer' goods they purchase arrive and are clearly not genuine. But the global corporations that trade on their luxury brand names have the finance and motivations to act when they feel their brand has been damaged. In a landmark legal ruling in 2008 a French court ordered eBay to pay 19.28 million to Louis Vuitton Malletier and 17.3 million to its sister company Christian Dior Couture for damage to their brand images and for causing 'moral harm'. Damages were sought over two issues: first it was argued that eBay had committed 'serious errors' by not doing enough to prevent the sales of fake goods, including Louis Vuitton bags; second, it was argued that eBay had allowed unauthorized sales of perfume brands owned by the group. The company's view was that, whether the perfumes are real or fake, an offence has been committed because the sale of real goods and perfumes on eBay violates the company's authorized distribution network which only allows sales through specialist dealers (*Guardian*, 1 July 2008).

While these kinds of offences can cost luxury brand companies millions, more pervasive in terms of perpetration and victimization, are offences involving handling stolen goods, financial fraud, obtaining property by deception or instances where sellers simply fail to provide goods to buyers. According to newspaper reports, the police in England and Wales investigate one alleged eBay scam every hour, some of which have moved beyond the cyber-realm and precipitated 'real world' crimes including burglary, assault, possession of firearms offences, civil disputes, harassment and an arson attack (*Daily Mail*, 8 October 2008). Users of the auction website reported an estimated total of more than 8,000 crimes in 2007 prompting eBay to respond by offering training to 2,000 police officers to tackle suspected Internet fraud. Cases that came to court in 2007 included that of a woman in South Wales who made more than £13,000 from photographs bearing forged signatures of celebrities and was given a 42-week suspended jail term, and a man from Yorkshire who was given a 26-week suspended sentence and 180 hours community service after selling £40,000 worth of fake *Take That* tickets to 270 victims on eBay (*Daily Mail*, 8 October 2008).

Hacking and loss of sensitive data

eBay has also been the target of hackers. In May 2014 the auction site was forced to ask 145 million users to change their passwords when it was revealed that hackers had stolen email addresses, birth dates and other identity information in a significant data breach. As this book goes to press, there appear to

> enormous damage to the computer systems of the United States government, and in so doing he has threatened the safety of every single American citizen. In the immediate aftermath of the September 11 terrorist attacks, McKinnon intentionally caused a network in the Washington DC area to shut down, resulting in the total loss of internet access and email service to approximately 2,000 users for three days at a cost of $900,000 (£544,000)... (cited ibid.)

McKinnon admited the hacking, but strenuously denied having malevolent motives of the kind suspected by the US authorities. Described by Ronson as 'essentially an idiotic but harmless conspiracy theorist who spent far too long on the internet because he was too nerdy to make it on the outside' Gary McKinnon may be simply a 'social type US prosecutors don't recognize' (ibid.).

Another illustration of the vulnerability of supposedly secure systems is the data lost or stolen from various government departments that is said to be worth billions to potential criminals. More than 1,000 laptops have gone missing from UK Government departments according to figures released in 2007, including 13 from the Cabinet Office. One of the most notorious and newsworthy cases was reported in 2007 when HM Revenue and Customs mislaid two CDs containing the Child Benefit database on which the names, addresses, dates of birth, National Insurance numbers and bank account details of 25 million people were stored. As if this were not shocking enough, it was revealed that the discs also contained the real names and new identities of up to 350 people who had been placed on the witness protection scheme after giving evidence against serious criminals.

Child pornography and online grooming

Pornography is a subject that provokes fear and fascination in equal measure and, while online porn (depicting adults and children) was the force that propelled the rapid growth of the Internet and demonstrated its commercial potential, equally it was child pornography that precipitated the establishment of some of the most high-profile organizations which police the Net. 'Adult' cyber-porn has ***democratized*** sexual gratification and provided greater freedom of access to women, as well as its traditional customers, men (Jewkes and Sharp, 2003), yet at the same time it has reignited debates about the exploitation of women and the relationship between pornography and sexual assault, and provoked a significant degree of technological determinism whereby blame is attributed to the Internet itself. The death of music teacher Jane Longhurst, who was sexually assaulted and murdered by an acquaintance who reportedly downloaded images and accounts of necrophilia and asphyxiation to fuel his deviant sexual desires, was reported in the UK under the sensational headline 'Killed by the Internet' (*Daily Mirror*, 4 February 2004; see Jewkes, 2007).

Characterized by Yar (2010) as a 'signal crime', the mediated public outcry following this case led to legislation criminalizing the possession of 'violent pornography' which is now punishable by up to three years imprisonment.

Despite such alarmism, which invariably reinvigorates debates about greater self-regulation, tougher legislation, and even censorship of the Internet, reported cases involving adult victims are extremely rare and the most intensive focus continues to fall upon pornography featuring children. It has been argued elsewhere in this volume that paedophilia constitutes *the* moral panic of our age (although that ascription has also been problematized) with all the attendant implications that moral panics tend to have on government and policing priorities. In common with broader news values, the issue is largely kept in the public eye through cases involving high-profile 'offenders' including celebrities and newsworthy 'victims'.

Many believe that the police have taken too long to address the problem of online child sexual abuse and have, for many years been playing catch-up with online offenders. Limited resources, lack of technological expertise, a tendency to target 'low hanging fruit' and an occupational culture resistant to new challenges are among the impediments to successfully policing online abuse of children (Jewkes and Andrews, 2005; Jewkes, 2010a) but, thankfully law enforcement is now beginning to reflect the changing technological and cultural landscape. The launch of the Child Exploitation and Online Protection (CEOP) Centre in 2006 underlines the UK police's commitment to stemming the global Internet trade in child pornography. One of their achievements has been to develop a pro-active strategy based on specialist intelligence. An initiative that has proved reasonably successful is the employment of undercover officers posing as children on fake websites and in chat rooms to lure paedophiles, although investigators are hampered somewhat by the law. However, the charge of 'grooming' has caused concern among civil liberties groups because it is designed to target adults who meet a child after contact has been made on the Internet but *before* any offence has taken place, raising the question of whether *thinking* about sexual acts is the same as committing them. Even if a case reaches court, proving intent is notoriously difficult for the police and prosecutors. This legislation enables the police to carry out 'sting' operations by posing as children in Internet chat rooms and then arranging to meet the unsuspecting groomers at a 'real' location, but they are not legally entitled to entrap a suspect.

Childhood, cyberspace and social retreat

Interestingly, anxieties about crime and safety, especially of children, have been significant factors in many aspects of life becoming isolated and atomized

activities. Numerous forms of 'social retreat' have become commonplace, including the growing numbers of gated communities, ownership of four wheel drive vehicles, the popularity of home leisure systems including social gaming platforms, and many others. For young people new social trends including the all-pervasiveness of the Internet and the tendency for parents to accompany their children in every public sphere constitute profound changes in the way that identities are shaped and social skills learned. At the same time – and partly as a consequence – of this privatization of social discourse and interaction, the Internet has become something of a scapegoat for a myriad of deviant human behaviours and conditions from sexual aggression and homicidal urges to attention deficit disorder and obesity. Unsurprisingly, it is children and young people who are considered most vulnerable to the potentially harmful effects of 'new' media technologies and most likely to be victims of predators wishing to exploit or abuse them.

As noted in Chapters 3 and 4 childhood has been transformed, especially since the paedophile emerged to haunt our collective imagination in the mid-1990s. In the 21st century adventure is for many children a virtual pleasure; competitiveness is honed at the games console rather than on the sports field; and sexual development occurs in chat rooms, on social networking sites and via mobile phones (Jewkes, 2010a). Unfortunately this means that some children and young people put themselves at risk of victimization and engage in more 'extreme' behaviours online than they would in the 'real' world. Among the 'risky' behaviours to emerge in recent years is 'sexting', where an individual sends nude or suggestive photos of themselves over their mobile phone. While such pictures are usually sent by young women to their boyfriends, Kent police report that predatory adults are taking advantage of the willingness of young people to experiment with their sexuality over the Net by engaging in sexually explicit chat and by exposing their bodies in front of a webcam (http://tinyurl.com/agfq2j). In the United States, a survey carried out by the National Campaign to Prevent Teen and Unplanned Pregnancy found that one in five teenagers had sent or posted online nude or semi-nude pictures of themselves and 39 per cent had sent or posted sexually suggestive messages (http://uk.reuters.com). So widely reported has 'sexting' since become (including stories of young celebrities who have found their 'private' photos posted online) that Australia's state government of New South Wales launched an education campaign in May 2009 to try to educate young people about the dangers of the practice and warn them of the consequences which can include bullying, harassment, sexual assault and, in one case in Cincinnati, USA, the suicide of an 18-year-old woman following months of taunting and bullying after nude images of herself that she had sent to her boyfriend were circulated, first across her high school and subsequently far beyond.

The 'normality' of ***cybersurveillance*** and the apparent willingness of children to take risks with their online activities, and to flaunt their emerging