Government Office for Science

Foresight

Future Identities: Changing identities in the UK – the next 10 years

DR 19: Identity Related Crime in the UK

David S. Wall

Durham University

January 2013

This review has been commissioned as part of the UK Government's Foresight project, *Future Identities: Changing identities in the UK – the next 10 years*. The views expressed do not represent policy of any government or organisation

Contents

Identity Related Crime in the UK

The purpose of this paper is to explore the regulative challenges that identity crimes pose for the public, policymakers and law enforcement. The paper accompanies *DR20 The Future Challenge of Identity Crime in the UK* (Wall, 2013) which considers the broader context, politics and futures of Identity Crime. Both papers contribute to the Government Office for Science Foresight project that is investigating how changes in technology, geo-politics, demographics and economics over the next 10 years might affect notions of identity and subsequently impact on behaviour.

1. Introduction

Identity crime[1] is a significant problem for both the UK economy and also its citizens. A much contested term (Wall, 2010a; Anderson *et al*., 2012), it is used here to describe identity theft (or obtaining personal information), creating false identities and identity fraud which is the use of identity information to defraud individuals or businesses (Home Office, 2012). In addition is the emergence of new forms of identity crime against individuals in social network media environments, such as extortion (blackmail), cyber-bullying (trolling) and even defamation (libel[2]).

The National Fraud Authority have estimated that identity fraud, one of the identity crimes discussed in this paper (and also Wall, 2013) costs the UK taxpayer about £1.2 billion per year (NFA, 2012:10) and losses are increasing each year. Others would argue that the problem is worse (see Javelin, 2009, 2010, 2011, 2012) and also point to identity crime being a global problem (Smith, 2010). The Australian Attorney-General Nicola Roxon, for example, recently claimed that identity fraud is one of Australia's fastest growing crimes and victimises one in four Australians (Keane, 2012). Furthermore, the problem appears to be on the increase. Recent data obtained from the UK Information Commissioner's Office through requests under the Freedom of Information Act by Imation Mobile Security suggests a 10 fold increase in lost identity data over the past decade (Leyden, 2012c)[3]. Other research indicates high increases in organisational data loss in other jurisdictions (Wall, 2012a).

Whether malicious or unintended, the fact is that personal and corporate information falls intentionally into criminal hands. Whilst few would deny this link, there is some debate over how much data ends up in criminal hands, what it is used for, but also what the data actually represents. Is it, for example, an identifier (instrument of fraud - see later) or a complete identity? The messages gleaned from the various literatures about identity related crimes are often contradictory. On the one hand, some cyber-security commentators are perceived to argue that identity crimes are rife and threatening (see Menn, 2010; Glenny, 2011; Poulsen, 2011 amongst others). On the other hand we are told by other researchers that they are also over-hyped and not always cyber-related (Wall, 2008; Anderson *et al*. 2012; also Keane, 2012). Books, such as those by Menn (2010), Glenny (2011) and Poulsen (2011) demonstrate the journalist's dilemma. Whilst they are honest, well researched and informative accounts and interesting to read, telling the public something they have a right to know, they are journalistic enterprises – good news stories presented in a dramatic style. The claims they make are limited to specific circumstances and the danger is that without a broader understanding of the issues, they can mislead readers into believing that the true scale of the crimes is much larger than it really is and stoke the fear of (identity) crime. These issues can never be fully resolved, but this paper and Wall (2013), plus the others in the series, will help fill the information gap in identity crime.

This paper and also Wall (2013) argue that although over-hyped, identity crimes will continue to evolve with changes in the technologically driven digital environment of financial, leisure and social service delivery, but at different rates. New forms of crime will emerge with every new convergence of technologies and we do not know what these are yet. Remember that

---

[1] Many thanks to the two anonymous reviewers who made useful and constructive comments upon earlier drafts of this paper.
[2] Libel is not discussed here. For further information about Libel see Milmo *et al*. (2010).
[3] Some of this increase is attributed to changes in reporting mechanisms, but year on year comparisons after the changes still indicate increases.

Facebook (established in 2004) and Twitter (established in 2006) were unheard of 10 years ago, as were botnets for that matter. Whilst experience and reference to the literature shows that identity crimes will never be eradicated, they can, nevertheless be managed by adopting various strategies. But, as one form of crime is brought under control there is the technological inevitability that new forms of service delivery will offer up opportunities for new forms of identity crime, though mainly variations on existing *modus operandi* which the part of this paper explores. It will look at identity theft; the crimes committed when collecting personal information and also selling it on to others. The third part will then look at the creation of false identity and identity manipulation. The fourth part will look at identity fraud; the crimes committed with stolen information to defraud individuals or organisations. The fifth part briefly describes new forms of identity crime arising from social network media. The sixth part explores the curious relationship between identity crime and the law. The seventh part concludes.

2. Identity Theft (theft of personal information)

Identity theft is a precursor to identity fraud (discussed later) because it describes the stage at which criminals obtain personal information from victims. There are currently a number of different ways by which this information can be obtained.

- *Trashing* or 'dumpster diving' has long been the most conventional way that fraudsters have obtained personal information. They would obtain discarded documents from trash cans, or steal personal documents from their owner (during burglaries for example). Trashing is a fairly low yield activity because of its physical nature. Another conventional method of fraud has been the use of trust obtained through family bonds or friendship in order to steal or hijack a victim's identity with a view to defrauding them (see Javelin, 2009). Networked technology, however, acts as a force multiplier by providing the criminal with a global reach. Personal information is, therefore, far more effectively obtained by using technological means. *Phishing* is the most used technique and relies upon common forms communication, such as an email, in order to trick, or 'socially engineer', victims into revealing their personal (and financial) information. Information that is later used to defraud them (see Identity Fraud below). The phishing pattern is widely known and is characterised by the indiscriminate mailing of millions of emails purporting to be from their bank, payment system or other regular form of financial transaction they use, such as eBay or Amazon. With a sense of urgency usually exaggerated by an alleged security breach, the emails typically ask recipients to log onto the web page through the URL given in the email and confirm their personal information details. Whilst the early Phishing expeditions caught many victims unaware, users quickly became savvy following scare stories circulating which recounted individual experiences (Wall, 2007). Remarkably, some of the early style phishing emails still circulate, presumably to catch new users, but information phishers, used here as a collective term for identity thieves, have changed their techniques and tactics in line with developments in technology to increase their yield.

- Phishers have *developed sophisticated social engineering* techniques, for example through 'spear phishing' in which highly personalised emails are sent to specific, rather than blanket, targets – which increases the response rate. Alternatively, they heighten the victims' own fear of victimisation by stating in phishing emails that: 'following illegal attempts to log on to your banking site please confirm your personal information'. FireEye (2012) have conducted research into the Spear Phishers' tactics and found them to be very tactical in terms of exploiting current concerns (also see Leyden, 2012a). Such spear phishing attacks are now displaying an increasing psychological and emotional, in addition to technological sophistication (see Wall, 2010a; RSA, 2011; Stajano and Wilson, 2011). They tailor their attacks to hit profiled groups and deliberately prey upon their victim's desires for goods or services; pressures to make decisions quickly, and also the fact that victims cannot, as yet, reliably check the sender's identity, the validity of a web page or of software they are downloading. Some cyber-security firms do provide warning systems for web sites, but they

are usually reputational based and their effectiveness is time-delayed, plus they also tend to be bundled with commercial security packages[4].

- Phishing has also *evolved* by criminals exploiting advances in technological systems, but the objective always remains the same, to extract valuable personal information. *Pharming*, or DNS cache poisoning or spoofing, contains seemingly 'relevant' information in the sender and subject lines that trick individuals to open the email. Once opened, code in the email automatically directs recipients to the phisher's bogus WWW site. Unlike phishing, pharming does not rely upon 'social engineering' to trick the recipient into clicking on to a WWW site. Instead, it deceives the domain name server into automatically accepting incorrect, or forged, access data (Wall, 2007).

- Subsequent technological developments allow offenders to exploit the new converged mobile technologies. '*Smishing*' is the sending of SMS text messages to potential victims that contain much the same message as in the original phishing emails. They ask victims to reconfirm their 'important security information' immediately by return SMS message, or via a www site. Finally, there is '*Vishing*', which exploits VOIP (voice over internet protocol), again, in much the same way as the phishing and smishing expeditions, but by voice. Victims are tricked into ringing back the number given, or asked to log onto a web address given in the message (Wall, 2007).

- A recent step change in the sophistication of the phishing operation has been the *browser in the middle* (or 'man in the middle') *attack*. In this attack, a sophisticated piece of malware is placed between the computer and the browser, usually following infection by a drive-by-download[5]. When the victim opens his or her banking www site a fake bank page opens imitating the original, but containing additional information slots to receive the users' access data plus more personal information. The pages are otherwise as users would expect to find them. Once the all of the users' data are entered, it is sent to the phishers' database and the browser in the middle is closed down, the correct data is also sent to the bank www site which opens as the victims expects it to and is unaware of the deception. This information has great market value because it is verified live access data. Also significant is with this development is that it demonstrates a shift in the visibility of phishing patterns from overt to stealthy (see Wall, 2010b).

- Identity theft has also evolved through an increased use of illegal spyware. Illegally (and sometimes legally) installed spyware either keeps a log of the victim's keystrokes (including passwords etc.) or it may actively seek out key financial information stored on the hard-drive. In both cases the information is subsequently relayed back to the infector. Zeus for example, is a slick, professionally crafted piece of Malware (malicious software) that is distributed by spammed email or by a 'drive-by-download' (after visiting an infected www site). At first glance, it looks benign, but infects the insecure computers of small businesses and individuals to steal bank login information and has a built in capacity to evade detection. It has evolved through a number of iterations. Earlier versions sought user names and passwords for social networking sites and online services as well as online banking credentials. More sophisticated versions focus solely on collecting banking information which is subsequently sent to a collecting database via encrypted communication (see Wall, 2010b).

[4] See for example, those provided by Symantec and Finjan, and others.
[5] Accessing a 'poisoned' www site infected with malware.

- A milestone in the automation of identity theft was the invention of the *botnet* which comprises of lists of the internet protocol (IP) addresses of 'zombie' computers that have been infected by remote administration tools (malware). They can be controlled remotely to send out messages, but also return information about the user. Botnets are additional force multipliers and therefore valuable commodities because of the added power they can place in the hands of the remote administrators to deliver a range of harmful malicious software. Furthermore, botnets themselves hold value in that they can be hired out, sold, or traded, thus changing the criminal business model. From 2003/4 through to today they have exponentially increased the power of the criminal by increasing the amount computers infected by malicious software (Wall, 2007). Malware, such as Zeus (mentioned above) contains a number of 'attack' functions including infecting other computers, clandestinely searching for user's security information, account numbers, user ID, passwords and additional security information and sending the information to the identity thief. Information, that may provide direct access to the victim's bank account and therefore dispenses with the need to perpetrate an application fraud. Once established, botnets tend to be 'branded' and then managed like a commodity. Some, such as 'Pushdo', have incredible resilience and have survived numerous attempts to take them down (See Leyden, 2012b).

- Three other ways that personal information can be obtained are, firstly, through deliberate data breach by corrupt insiders, (see BBC, 2009), secondly from lost or stolen laptops (BBC, 2010) thirdly from second hand data storage devices that have been discarded, but not been wiped clean (BBC, 2012a; see discussion in Wall, 2012).

- Finally, there exists a brisk trade in the sale of illegally acquired personal information obtained through identity theft tactics, such information is mostly identifiers that facilitate fraud, but other key identifiers are also available to the would-be fraudster (BBC, 2012d). There are at any one time a numerous websites that sell this information. One particularly well known site was *Carder Planet*[6], now shut down, which used to trade in credit card information. See generally, Casciani (2008), Branton (2010), BBC (2012b). CloudEyeZ.Com's Underground Activity Index[7], set up in July 2012, monitors the illegal sale of credit card details (sets of identifiers) and at the time of writing in September 2012 average prices for the sale of stolen Visa, Mastercard and American Express card details ranged from $2-$3 each (Kirk, 2012). See Glenny (2012) for a detailed description of this 'dark market'. To end this section, there is also a grey market in sale of legitimately obtained personal information by legitimate businesses which is subsequently sold on to third parties unfairly without the donor's knowledge (see Poulter, 2011).

The evolution of identity theft through psychological means (social engineering), and through technological means (trashing, phishing, pharming, smishing, vishing, man in the middle attacks), and the intervention of botnets and surveillance software, combined with the growth of a business model around the sale of the information indicates that identity theft is robust and is unlikely to diminish in the future.

[6] See description at IT LawWiki <http://itlaw.wikia.com/wiki/Carderplanet>
[7] CloudeyeZ.com, Underground Activity Index, https://www.cloudeyez.com/intel

3. Creating a false identity

False identity is the creation of an entirely new false identity in order to evade capture for another crime, conduct industrial espionage, or to conduct fraud and/or prevent detection, or (ironically) to help victims of identity-crime to recover their reputation after victimisation. There is a difference between using a fake ID card (Insley, 2010) and creating and living behind a new false identity (Shaikh, 2003; Banerji, 2012) and much help can be obtained online to develop new identities or change them, see for example, Charrett (1997). Having said that, the sources are not entirely new and many predate new networked technologies, plus the ideas may now be untenable due to modern levels of security and its dynamics.

- A 'traditional' method of obtaining an identity was by 'identity farming' (Schneier, 2008). The fraudster would obtain the birth certificate of a dead child who was born as approximately the same time as themselves and carefully construct a new identity over time.

> "[y]ou invent a handful of infants. You apply for Social Security numbers for them. Eventually, you open bank accounts for them, file tax returns for them, register them to vote, and apply for credit cards in their name. And now, 25 years later, you have a handful of identities ready and waiting for some real people to step into them" (Schneier, 2008).

- The problem with 'identity farming', states Schneier, is that 25 years is too long to wait for a payoff, especially for a terrorist organisation or organised crime. Plus, he observes individuals do have to show up somewhere for part of their lives. Every individual has a 'data shadow' (Schneier 2008) or 'data double' (Haggerty and Ericson, 2000) that literally follows us around and interacts with organisations, institutions and agencies instead of with us as individuals. Furthermore, the numbers of data points that our data doubles have to digitally interact with has massively increased in line with the expansion of IT based services; weakening the identity farming hypothesis. Evidence of a counter-thesis can be seen in a number of recent cases, for example, that of David Hemler, a US Air force deserter who sought refuge in Sweden in the 1980s. Hemler assumed a made up identity along with a carefully constructed story. He later applied for and received residency rights from the Swedish government under his false identity (Banerji, 2012) only to be later exposed after he contacted relatives. In Helmer's case, it is unlikely that such permission would be granted today because of current requirements for supplemental biometric information. This example also illustrates how identity has changed from a negotiated state to a technical state.

- In another case, Brian Hackett from the UK wanted to hide his past and under the guise of a former friend who had committed suicide some years previously he claimed that he, Hackett, was one of the people who died in the 1999 Paddington Rail Crash. Hackett's body was, of course, never found and he was later exposed by curious relatives (See Finch, 2002; Cowley, 2000). In Hackett's case, the technical requirements of autopsy combined with relative's curiosity thwarted what would in days-gone-by have been a possible fraud.

- In more recent years, Facebook has not only become an important aspect of one's identity but a threat to the biometric data double. Andrea Sirlo[8] recently created a fake identity as a pilot on Facebook and added to it by creating fake identity cards. He also strengthened the plausibility of his identity by sending "himself imaginary comments from dozens of fake cabin crew friends who expressed their 'delight' at being rostered with him on flights" (Pisa, 2012). Using his fake ID and its fake history, Sirlo joined cabin crew on a flight from Munich to Turin. The Italian Civil Aviation Authority became suspicious at how Sirlo could claim to be a captain when he appeared to be so young (Pisa, 2012). The lack of synchronisation between Sirlo's assumed identity and his 'data double' caused the alarm to be raised.

- Another way of obtaining false identities is through travel agents and brokers who can provide real passports for fake identities through corrupt links with governmental officials (Straits Times, 2012). Since the documents are real it becomes hard to detect false identity (see for example Home Office, 2012). However, whilst documents may be good for proving identity and even travelling across borders in weak enforcement regimes, the combination of different forms of ID required will likely eventually expose most fraudsters.

- As a footnote, Facebook requires its users to declare their real identity (One India, 2012) and have even tested a scheme that asks friends to reveal other friends who state untruths about their identity (Protalinski, 2012). Yet, there is a tension present in Facebook's business model. On the one hand, the business model requires real names as a good way of keeping its users safe, but also providing revenue from advertising. On the other hand, "many Facebook users opt to use pseudonyms to hide from stalkers, abusive exes, and even governments that don't condone free speech" (Protalinski, 2012). Facebook themselves have estimated that 83 million registered users are actually duplicated accounts, spammers, or non-people, "like that profile you made for your puppy" (Jeffries, 2012). What is interesting here is that many of these fake accounts are actually inhabited by real individuals who simply obscure their legal names. One of Jefferies' interviewees, Mason, said that he used his middle name as a surname and he and his friends (and family) have grown quite used to it.

> "At this point, I can't imagine putting my real last name on Facebook. I've gotten very used to my 'fake' name and it would creep me out to see my full real name up there." Mason estimates that 10 to 20 percent of his friends use modified-but-plausible names on Facebook (Jefferies, 2012).

- Changing one's name in this way is also a frequent practice adopted by identity crime victims as a way of avoiding future victimisation by their impersonator.

- The main focus of this section has been on individuals creating identities for their own purposes. New professional social media, for example, Linked In and others provides fraudsters with a ready source of information about the individuals who work within businesses, agencies and organisations. Information that can be, and has been, used to impersonate individuals in order to gain access to businesses and organisations. Sometimes this has involved individuals defrauding businesses, but it increasingly offers new

[8] The surname Sirlo, is the name for the air corridor over Turin. The scam bore a resemblance to the 2002 Leonardo Di Caprio film *Catch Me If You Can* directed by Steven Speilberg.

opportunities for business to commit fraud on other businesses, for example to defraud them or commit espionage so as to steal their commercial secrets (see Nasheri, 2005).

As social networking media closes the gap between online and offline identities, and identifiers, then criminals will begin to exploit the many new forms of identity that are becoming more and more relevant and which are acquiring exchangeable value, or leverage value in blackmail.

What the above examples show is that identifiers differ from identity, and that identity itself is felt rather than real by not only the owner but also by his or her friends. But more importantly, where individuals have deliberately sought to hide behind false identities they were mainly uncovered by social rather than technological means, or a combination of both. The examples also suggest that no system is perfect because as long as one of the identification authorisers, where ever that may be remains corruptible then biometric systems are imperfect.

4. Committing Identity Fraud

Identity fraud is conceptually different from identity theft discussed earlier because identity fraud relates to the application of the 'stolen' information to fraud. Identity fraudsters have long exploited the social capital invested in the trusted identities of individuals or groups in order to deceive victims, typically pretending to be someone else in order to perpetrate a scam – e.g., cold calling online and offline scams such as distraction burglary (see further Lister and Wall, 2006). It is not only cheap to effect, but also easy to mimic the trust signals, ranging from brands to uniforms, found in the physical world (see further the arguments in Kirlappos, *et al*., 2012).

In virtual environments, the process of mimicry is made all the easier and more convincing by new digital technologies which enable fraudsters to reproduce the trusted signs and symbols in order to carry out their cons. Networked technologies have, as stated earlier, become a force multiplier and have changed the dynamics of fraud. Identity frauds use personal or organisational identifiers in order to gain direct access to victim's personal and private financial resources by either directly accessing their accounts via stolen card information and withdrawing money, or taking over their accounts completely. Alternatively, the victim could be a business and its systems be accessed for industrial espionage as well as stealing goods or money. Whereas identity theft - described earlier - is asymmetric, identity fraud is symmetric because an individual has to use the information, whether at a cash machine, buying goods and services online, or impersonating someone. These individuals who ferry money between the bank and the criminal are referred to as 'money mules'. Often students or the less well off, they are usually paid a fee 'per visit' to the ATM machine.

Online, there are four main permutations of frauds that help illustrate the dynamics of the identity fraud and demonstrate how it is evolving. The titles are self-explanatory:

- ***Individual to individual fraud*** – the use of personal identity information to commit frauds against individual victims. They include bank account fraud that ranges from illegal withdrawal of money to account take over (but not credit cards - see below). Networked technologies have also enabled local frauds to become global, see for example, the explosion in advanced fee scams (also known as Nigerian 401 scams), lottery scams, dating scams, pyramid selling scams, entrapment marketing scams, auction frauds, loan scams, credit repair scams, short-firm frauds (see further Wall, 2010a).

- ***Individual to business fraud*** – the use of personal identity information to commit frauds against businesses. Examples include creating fake bank accounts through application fraud (fake identity)**,** card fraud, buying fake or cloned credit cards, Benefit fraud, and Insurance fraud. Networked technologies have enabled new forms of individual-to-business frauds to take place see for example; click frauds which exploit online advertising systems (Wall, 2010a).

- ***Business to individual fraud*** – the use of personal identity information by businesses to defraud individuals. Examples include the sale of personal protection insurance, contract entrapment scams.

- ***Business to business fraud*** - the use of identity information by businesses to defraud businesses. Examples include espionage and/or exploiting commercially sensitive information or trust symbols, such as brands, that have been built up over time.

5. New forms of identity crime

As social networking media closes the gap between online and offline identities and identifiers, then criminals will begin to exploit the many new forms of identity that previously existed but are becoming more relevant today and are acquiring exchangeable value. Examples of valuation are beginning to occur. The new relevant forms of identity are:

- *Social Friendship identity*, exploiting friendship links that give access to social groupings;
- *Citizenship identity*, exploiting characteristics that imply citizenship to various groupings;
- *Financial identity*, exploiting characteristics that give access to financial resources;
- *Professional identity*, exploiting access to a professional community and its clients;
- *Organisational identity*, exploiting an employee's access to organisational resources;
- *Sexual Identity*, exploiting characteristics that display sexual orientation; and
- *Geographic identity*, exploiting location information to see, for example, whether someone is not at home in order to steal from them (Blumberg and Eckersley, 2009).

A key driver in creating exchangeable value (that attracts criminals) is reputation within a network. As more and more different identity group characteristics develop, then reputation becomes all the more important as a way of ordering the hierarchy. It is therefore highly likely that the value of reputation will increase and instances of extortion (blackmail), cyber-bullying (trolling) and even defamation (libel) will continue to rise as individuals work through their life course.

Examples of Facebook extortion/ blackmail already exist. In 2010 a Wisconsin male teenager pretended to be a young girl and got young men to send naked photos of them to him. He then tried to blackmail them (Musil, 2010). In a similar case in the Philippines, a fifteen year old boy was arrested, also for pretending to be a young girl and getting his classmates to send him naked photos of themselves (Andrade, 2012). In another case, also in the Philippines, a 24 year old man was arrested for blackmailing a 16 year old girl after enticing her to send him semi-nude photographs of herself so that he could allegedly help her with her modelling career (Inquirer News, 2012).

Cyber-bullying or 'Trolling' describes the increasing practice of intentionally provoking online users with inflammatory messages in order to elicit an emotional response that will disrupt online activities and upset those offline. Some cases of trolling have even resulted in suicide. See, for example, the suicide of Tyler Clementi after his roommate used his webcam to video Clementi kissing another man in order to 'out' him online (Pilkington, 2010). Or, the suicide of Amanda Todd after she was bullied online by an 'internet troll' (Wolf, 2012) and there are many more. The Todd case so incensed the internet vigilante group Anonymous that they subsequently revealed online the identity of her tormentor (Swash, 2012). On the subject of death, the UK Data Protection Act 1998 only applies to living people, so the memorial pages of deceased individuals are particularly prone to the posting of upsetting messages or even defacement. The callousness of such acts leaves most readers dumbfounded, though in her

analysis of trolling Phillips argues that that trolls are "... directly reflective of the culture out of which they emerge, immediately complicating knee-jerk condemnations of the entire behavioral category (sic)". She argues that "[u]ntil the conversation is directed towards the institutional incubators out of which trolling emerges -- as opposed to just the trolls themselves -- no ground will be gained, and no solutions reached" (see discussion in Phillips, 2012).

Whilst extortion and bullying hit the headlines and raised public concerns, it is equally likely that instances of identity data manipulation will also increase in the future when individuals seek to correct past infelicities. One driver is career prospects, with the value at stake being their employability. A recent CareerBuilder survey found that 37 per cent of employers are using social media to investigate their prospective employees before they make a final decision over whether or not to employ them (Messieh, 2012). There are also reports that employers are also asking candidates for Facebook passwords (Horn, 2012). If Facebook has 83 million fake accounts (BBC, 2012c) then it is arguable that a lot of people may have a lot to hide and the price of that privacy may be high for some. The twist with Facebook is that not to have a Facebook page is becoming out of the ordinary. Facebook has only been touched upon here and there are so many other examples of social network media, which may become new sources of identity crimes in the future.

Informational value in identity as a driver for criminal activity is developing in new, and often unanticipated, ways. It raises questions about how to police new identity crimes as well as fundamental questions about who owns personal data and who is authorised to use it, especially when stored in 'the cloud' across judicial boundaries (currently the subject of much debate). There is also the problem of where the line exists between a troll's right to express him or herself and it being a criminal act. To get deeper into identity crime it is now important to look at the law relating to identity crimes.

6. The law and identity crime

Three distinct acts of law cover identity crime in the UK; The Fraud Act 2006; The Identity Documents Act 2010; and The Forgery and Counterfeiting Act 1981. Within these Acts are five key offences to cover the three types of identity crime mentioned previously (other legislation listed later covers other aspects of identity crime). Although the legislation covers a broad range of identity related crime, the prosecutions made under these acts, as listed in Annex H of Home Office (2012)[9], usefully give an idea of proportionality and change over time. In 2008 there were 11,687 cautions and proceedings under the five pieces of legislation. In 2009 this increased to 14,579 and in 2010 (the latest available statistics) there was a slight increase to 14,727.

- The Fraud Act 2006 has two relevant pieces of legislation relating to identity crime. First, there is *Dishonestly making a false representation to make a gain for oneself or another or to cause loss to another or to expose another to a risk of loss* (Fraud Act 2006 sections 1(2a), (3) & (4) & 2.)). This is the most numerous all the five identity related offences and represents 91 per cent of identity related crime in 2010 (12,982 of 14,727). Cautions and prosecutions have increased steadily over the three years, whilst conviction rates remained much the same at 79, 77 and 78 per cent in 2008, 2009 and 2010 respectively. Prosecutions under the different sections of this offence include identity related offences such as possessing phishing kits, using stolen credit card information, but also road accident fraud, benefit fraud, false information about houses (false claims), mortgage fraud and other identity related crimes.

  Second, there is *Possession etc. of articles for use in frauds* (Fraud Act 2006, section 6). This represents about 6 per cent of identity crimes in 2010 (849 of 14,727) and has declined in numbers over the three years. Prosecutions rates have increased a little (83%, 90%, 91% - convictions as a percentage of prosecutions) and include possession of articles for use in fraud such as (amongst other items), cloned credit cards.

- The Identity Documents Act 2010 (formerly the Identity Cards Act 2006, section 25(5) & (7)) has an offence for *Possessing or controlling a false or improperly obtained ID card or which relates to another, or apparatus etc for making false ID cards*. The different types of identification documents are described in Home Office (2012). These comprise about 4 per cent of the identity related crime prosecutions in 2010 (471 of 14,727) and the number of prosecutions decreased over the three years studied from 701 to 536 to 471. This may be because organisational gatekeepers, ranging from human resources to door staff in clubs have been made more aware of how to detect fake documents and also of what their responsibilities are. As a consequence individuals are less likely to now use more spurious forms of identity documents (including fakes) than they may have previously done so. Interestingly, public debates about identity in the late 2000s led to the rejection of plans for national identity cards and the Identity Cards Act 2006 was supplanted by the Identity Documents Act 2010.

- The Forgery and Counterfeiting Act 1981 also has two pieces of legislation relating to identity crime. The first offence is *Using a false instrument etc. in respect of scheduled drug*

[9] Based upon information from the Justice Statistics Analytical Services in the Ministry of Justice [Ref: OS 570-10]

(Forgery and Counterfeiting Act 1981, Sections 3&4). This is a less frequently prosecuted offence comprising of less than 1% of all identity crime offences related to the procurement of drugs in 2010 (26 of 14,727). Numbers have declined over the three year period (587, 578, 389), although prosecutions remain at around 100 per cent. Offences relate mainly to forged identity documentation for NHS and Pharmacies.

- The second is *Using a false instrument or a copy of a false instrument* (Forgery and Counterfeiting Act 1981, Sections 3&4). This is also a less frequently prosecuted offence comprising of 2 per cent of identity related offences in 2010 (389 of 14,727).

Cautions and prosecutions under the Fraud Act, Identity Documents Acts and Forgery and Counterfeiting Act are presented in the following table adapted from Annex H in Home Office (2012).

Table 1: Number of offenders cautioned and defendants proceeded against at magistrates' courts and found guilty at all courts for selected offences, England and Wales, 2008 to 2010

	2008			2009			2010		
	Cautioned	Proceeded	Guilty	Cautioned	Proceeded	Guilty	Cautioned	Proceeded	Guilty
Fraud Act 2006 sections 1(2a), (3) & (4) & 2. (% of annual total)	3746 (83%)	5718 (80%)	4526 (76%)	3942 (87%)	8530 (85%)	6610 (84%)	3587 (88%)	9395 (88%)	7319 (87%)
Fraud Act 2006, section 6. (% of annual total)	341 (8%)	529 (7%)	438 (7%)	279 (6%)	671 (7%)	602 (8%)	250 (6%)	599 (6%)	544 (6%)
Identity Cards Act 2006, section 25(5) & (7). (% of annual total)	225 (5%)	476 (7%)	550 (9%)	179 (4%)	357 (4%)	418 (5%)	160 (4%)	311 (3%)	359 (4%)
Forgery and Counterfeiting Act 1981, Sections 3&4. (% of annual total)	27 (1%)	38 (1%)	40 (1%)	20 (0%)	23 (0%)	21 (0%)	10 (0%)	16 (0%)	16 (0%)
Forgery and Counterfeiting Act 1981, Sections 3&4. (% of annual total)	175 (4%)	412 (6%)	377 (6%)	95 (2%)	483 (5%)	238 (3%)	52 (1%)	337 (3%)	174 (2%)
Total	4514	7173	5931	4515	10064	7889	4069	10658	8412
Total Cautioned & Proceeded against	11687			14579			14727		

N.B. Adapted from *Justice Statistics Analytical Services in the Ministry of Justice* [Ref: OS 570-10]) [reproduced in Annex H, Home Office (2012)][10,11,12,13,14,15.]

In addition to the three acts mentioned above are other legislation that can assist in the prosecution of identity crimes. The Computer Misuse Act 1990 provides for the manner in which identity crimes take place. It covers unauthorised access, unauthorised access with intent to commit a crime and unauthorised access to change data and includes distributed denial of service attacks, is not discussed here in detail. The provisions only partly cover identity crime, mainly the use of viruses to acquire personal information and using it to obtain unauthorised access to systems. Available information on cautions and prosecutions suggests that the prosecution rate is very low, approximately 300 cases since its introduction in 1990 (Wall, 2007/11).[16]

Cases of cyber-extortion or blackmail (using social network media or not) fall under section 21(1) of the Theft Act 1968 and possibly 29(1)(i) and 30 of the Larceny Act 1916 if the blackmail also involves 'menaces'. Cyber-Bullying or trolling mentioned in section 5 is not the subject of specific laws, though the words by which trolls use to elicit a response are subject to the UK law on hate and harassment. Part 4A of The Public Order Act 1986 (as amended by The Criminal Justice and Public Order Act 1994) prohibits anyone from causing alarm or distress:

> (1) A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, he— (a) uses threatening, abusive or insulting words or behaviour, or disorderly behaviour, or (b) displays any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

The Public Order Act 1986 also contains provisions for dealing with hatred on grounds of racial, religious and hatred sexual orientation. Similar acts exist in other jurisdictions, but the challenge lies in determining jurisdiction. Cyber-bullying is also covered by the provisions of the

---

[10] The following six footnotes are taken from Home Office (2012).
The cautions statistics relate to persons for whom these offences were the principal offences for which they were dealt with. When an offender has been cautioned for two or more offences at the same time the principal offence is the more serious offence.
[11] The cautions statistics relate to persons for whom these offences were the principal offences for which they were dealt with. When an offender has been cautioned for two or more offences at the same time the principal offence is the more serious offence.
[12] The figures given in the table for court proceedings relate to persons for whom these offences were the principal offences for which they were dealt with. When a defendant has been found guilty of two or more offences it is the offence for which the heaviest penalty is imposed. Where the same disposal is imposed for two or more offences, the offence selected is the offence for which the statutory maximum penalty is the most severe.
[13] Every effort is made to ensure that the figures presented are accurate and complete. However, it is important to note that these data have been extracted from large administrative data systems generated by the courts and police forces. As a consequence, care should be taken to ensure data collection processes and their inevitable limitations are taken into account when those data are used.
[14] Excludes data for Cardiff magistrates' court for April, July, and August 2008.
[15] The number of defendants found guilty in a particular year may exceed the number proceeded against as the proceedings in the magistrates' court took place in an earlier year and the defendants were found guilty at the Crown Court in the following year; or the defendants were found guilty of a different offence to that for which they were originally proceeded against.
[16] The limited information about cautions and prosecutions under the Computer Misuse Act 1990 are compiled from the answer to various questions in Parliament (see Wall 2007 and 2010).

Communications Act 2003, the Malicious Communications Act 1988 and in some circumstances the Contempt of Court Act 1981.

One of the problems with the current laws relating to identity crime is that, at first glance, the legal provisions do not appear to tally with the colloquial definitions. Neither the terms ‘identity crime’, nor ‘identity theft’ appear in the legislation. As Smith (2010: 273) observes, identity theft is a ‘social rather than legal concept’. But the law nevertheless provides measures to deal with most types of identity crime. So, new law in this respect is not required, which is an observation supported by Levi and Williams who found in their 2012 survey of key cybercrime stakeholders that less than 10 per cent wanted more UK legislation and less than 5 per cent wanted more effective reporting mechanisms outside the police (Levi and Williams, 2012: 63). What is required is a better management of public expectations through more public knowledge, better training for criminal justice agencies (police, prosecution, courts, legal profession) and clearer procedures. Where there is demand for new law is to assist victims of identity crime (see later).

On the subject of reporting, victims of fraud can report their victimisation to the Action Fraud national fraud reporting centre which has received reports from fraud victims since 2010. These reports are triaged by a National Fraud Intelligence Bureau, based in the City of London Police, who decides upon appropriate responses (Wall, 2010a). Tactical information is sent to the relevant police forces and strategic intelligence informs the National Fraud Strategy (NFSA, 2009, see discussion in Trueman, 2011). The central collation of intelligence helps to overcome the longstanding problem of locality which contributes towards developing a national and international picture of a ‘distributed’ fraud problem.

7. Conclusions

This paper has explored the regulative challenges that identity crimes are individually posing for the public, policymakers and law enforcement. Identity crimes erode public trust in networked systems and reduce their impact by discincentivising users, especially the poorer sections of society. There is some confusion in public debates between the different types of identity crimes. In this paper identity theft, itself a problematic term because the information is ot actually stolen, is distinguished from creating false identities (impersonation). Both categories are also separated from identity fraud which is the use of identity information to commit fraud and other crimes. There are four permutations of identity fraud; individual to individual; individual to business; business to individual; business to business. In the future new types and twists of identity crime are likely to emerge out of the new forms identity (and identifiers) that are becoming the drivers of new social media. Yet, the law relating to individual identity crimes whilst quite recent is quite robust, but does not reflect the terminology of identity crime, which is confusing for regulators. This does not assist new UK national fraud reporting systems. Furthermore, the law does not assist victims of identity fraud as well as it could.

In many ways, some of these observations are not all new, see for example, the Trustguide report (Lacohée *et al*., 2006), but almost a decade on they do demonstrate the resilience of identity crimes and illustrate their likely continued evolution. There is much public concern that if identity crimes are not responded to more effectively then victims will quickly lose trust in networked systems and stay away from virtual environments. But any response is going to be an uphill struggle because of the increasing psychological and technological sophistication of information thieves and fraudsters. Echoing the immortal words of 1930s bank robber, Slick Willie Sutton “criminals will go to wherever the money [or advantage for them] is” and this is why it will continue to take place. The fraudsters and criminals will seek out the weaknesses in systems and exploit them. But as it becomes harder in practice to deceive security checks, then offenders will constantly weigh up the risks associated with the opportunities for crime. The problem for security policy makers is that when systems becomes secure enough to prevent fraudsters, will the users still be interested in using those systems?

References

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T. and Savage, S. (2012) 'Measuring the Cost of Cybercrime', paper to the *11th Annual Workshop on the Economics of Information Security*, Berlin, 25-26th June, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Andrade, J. (2012) 'Teen blackmail via Facebook', *Philippine Daily Inquirer*, http://newsinfo.inquirer.net/205505/teen-blackmail-via-facebook

Banerji, R. (2012) 'David Hemler: 28 years on the run', *BBC News Online*, 3 September, http://www.bbc.co.uk/news/magazine-193312090

BBC (2009) 'T-Mobile staff sold personal data', *BBC News Online*, 17 November, http://news.bbc.co.uk/1/hi/uk/8364421.stm

BBC (2010) 'Laptop with personal data of 24,000 people is stolen', *BBC News Online*, 29 June, http://www.bbc.co.uk/news/10453067

BBC (2012a) 'Watchdog finds undeleted data on second-hand disk drives', *BBC News Online*, 25 April, http://www.bbc.co.uk/news/technology-17827562

BBC (2012b) 'Credit card 'info for sale' websites closed in global raids', *BBC News Online*, 26 April, http://www.bbc.co.uk/news/uk-17851257

BBC (2012c) 'Facebook has more than 83 million illegitimate accounts', *BBC News Online*, 2 August, http://www.bbc.co.uk/news/technology-19093078

BBC (2012d) 'US jails hacker who sold access to hijacked PCs', *BBC News Online*, 7 September, http://www.bbc.co.uk/news/technology-19517316

Blumberg, A. and Eckersley, P. (2009) 'On Locational Privacy, and How to Avoid Losing it Forever', *Electronic Frontier Foundation Report*, August, https://www.eff.org/files/eff-locational-privacy.pdf

Branton, J. (2010) 'Your identity for sale online: Thieves sell credit numbers, more on members-only sites', *The Columbian*, 25 November, http://www.columbian.com/news/2010/nov/25/your-identity-for-sale-online/

Casciani, D. (2008) 'UK identities sold for £80 online', *BBC News Online*, 17 November, http://news.bbc.co.uk/1/hi/uk/7732569.stm

Charrett, S. (1997) *The Modern Identity Changer: How to Create a New Identity for Privacy and Personal Freedom*, Boulder, Colorado: Paladin Press

Cowley, J. (2000) 'Where are they now?', *The Observer*, 18 June, http://www.guardian.co.uk/theobserver/2000/jun/18/features.review17

Finch, E. (2002) 'What a tangled web we weave: identify theft and the internet', in Y. Jewkes (ed.), *dot.cons: Crime, Deviance and Identity on the Internet*, Cullompton: Willan, 86–104

FireEye (2012) Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data. *FireEye Report*, September, http://www.fireeye.com/resources/pdfs/fireeye-top-spear-phishing-words.pdf

Glenny, M. (2012) *DarkMarket: How Hackers Became the New Mafia*, New York: Vintage

Haggerty, K. and Ericson, R. (2000) 'The surveillant assemblage', *British Journal of Sociology*, 51 (4): 605–22

Home Office (2012) *False ID Guidance*, http://www.homeoffice.gov.uk/publications/alcohol-drugs/alcohol/alcohol-supporting-guidance/false-id-guidance?view=Binary

Horn, L. (2012) 'Trend Watch: Employers Asking Candidates For Facebook Passwords', *PCMAG.COM*, 22 March, http://www.pcmag.com/article2/0,2817,2401999,00.asp

Inquirer News (2012) 'Man in Facebook blackmail case pleads 'not guilty'', *Inquirer News*, 28 March, http://newsinfo.inquirer.net/168409/man-in-facebook-blackmail-case-pleads-%E2%80%98not-guilty%E2%80%99

Insley, J. (2010) 'Need a false identity? It'll cost a couple of quid, *The Observer*, 16 May, http://www.guardian.co.uk/money/2010/may/16/false-identity-cost

Javelin (2009) *2009 Identity Fraud Survey Report: Consumer Version*, Pleasanton, CA: Javelin Strategy and Research.

Javelin (2010) 2010 *Identity Fraud Survey Report: Consumer Version*, Pleasanton, CA: Javelin Strategy and Research.

Javelin (2011) 2011 *Identity Fraud Survey Report: Consumer Version*, Pleasanton, CA: Javelin Strategy and Research.

Javelin (2012) 2012 *Identity Fraud Survey Report: Consumer Version*, Pleasanton, CA: Javelin Strategy and Research.

Jeffries, A. (2012) 'Facebook's fake-name fight grows as users skirt the rules', *The Verge*, 17 September, http://www.theverge.com/2012/9/17/3322436/facebook-fake-name-pseudonym-middle-name

Keane, B. (2012) 'Cybercrime: rarer and less costly than we're told', *Crikey*, 31 October, http://www.crikey.com.au/2012/10/31/cybercrime-rarer-and-less-costly-than-were-told/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+CrikeyDaily+%28Crikey+Daily%29

Kirk, J. (2012) 'Project Monitors Price of Stolen Credit Card Data in Real Time', *PCWorld*, 1 August, http://www.pcworld.com/article/260245/project_monitors_price_of_stolen_credit_card_data_in_real_time.html

Kirlappos, I., Sasse, A. and Harvey, N. (2012) 'Why Trust Seals Don't Work: A Study of User Perceptions and Behavior', *Lecture Notes in Computer Science*, 7344: 308-324, http://www.springerlink.com/content/wj3v741872461gl7

Lacohée, H. Crane, S. and Phippen, A. (2006) *Trustguide: Final Report*, Trustguide, http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf

Levi, M. and Williams, M. (2012) *eCrime Reduction Partnership Mapping Study*, Cardiff: NOMINET/ Cardiff University.

Leyden, J. (2012a) 'If you see 'URGENT tax rebate download' in an inbox, kill it with fire', *The Register*, 26 September, http://www.theregister.co.uk/2012/09/26/spear_phishing_hooks/

Leyden, J. (2012b) 'Pushdo botnet's smokescreen traffic hits legitimate websites', *The Register*, 19 September, http://www.theregister.co.uk/2012/09/19/pushdo_spews_fake_traffic/

Leyden, J. (2012c) 'UK data-blurt cockups soared 1,000 PER CENT over last five years', *The Register*, 30 August, http://www.theregister.co.uk/2012/08/30/data_breach_increase/

Lister, S. and Wall, D. (2006) 'Deconstructing Distraction Burglary: An Ageist Offence?', *Ageing, Crime and Society*, pp. 107-123, in A. Wahidin and M. Cain, (eds.) Cullompton: Willan Publishing, 2006. Available at SSRN: http://ssrn.com/abstract=1085050

Menn, J. (2010) *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet*, New York: PublicAffairs

Messieh, N. (2012) 'Survey: 37% of your prospective employers are looking you up on Facebook', *The Next Web*, 18 April, http://www.thenational.ae/news/world/europe/jailed-italian-mafia-bosses-find-friends-on-facebook

Milmo, P., Rogers, W., Parkes, R., Busuttil, G., Walker, C., and Speker, A. (2010) (eds) *Gatley on Libel and Slander*, 11th Edition, London: Sweet and Maxwell.

Musil, S. (2010) 'Report: Teen gets 15 years for Facebook blackmail', *cnet News*, 24, http://news.cnet.com/8301-1023_3-10459536-93.html

Nasheri, H. (2005) *Economic Espionage and Industrial Spying*, New York: Cambridge University Press

NFA (2012) *Annual Fraud Indicator*, National Fraud Authority, March, http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2012?view=Binary

NFSA (2009) *The National Fraud Strategy A new approach to combating fraud*, The National Fraud Strategic Authority, at http://www.attorneygeneral.gov.uk/NewsCentre/News/Documents/NFSA_STRATEGY_AW_Web%5B1%5D.pdf

One India (2012) 'You may get call from Facebook if profile identity is fake: Beware fake Facebook profile holders', *OneIndia*, 9 September, http://news.oneindia.in/2012/09/09/youmay-get-call-from-facebook-if-profile-identity-issuspec-1067709.html

Phillips, W. (2012) 'What an Academic Who Wrote Her Dissertation on Trolls Thinks of Violentacrez', *The Atlantic*, 15 October, http://www.theatlantic.com/technology/archive/2012/10/what-an-academic-who-wrote-her-dissertation-on-trolls-thinks-of-violentacrez/263631/

Pilkington, E. (2010) 'Tyler Clementi, student outed as gay on internet, jumps to his death', *The Guardian*, 30 September, http://www.guardian.co.uk/world/2010/sep/30/tyler-clementi-gay-student-suicide

Pisa, N. (2012) ''Fake pilot who joined cabin crew in cockpit' is arrested in plot mirroring Spielberg's hit film Catch Me If You Can', *Daily Mail*, 23 September, http://www.dailymail.co.uk/news/article-2207422/Italian-police-arrest-man-posed-pilot-joined-cabin-crew-budget-airline-cockpit.html?ITO=1490

Poulsen, K. (2011) *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground,* New York: Crown Publishers

Poulter, S. (2011) 'Thinking of checking out a bargain? Beware the company websites that are selling on your personal details', *Daily Mail*, 8 April, http://www.dailymail.co.uk/news/article-1375066/Beware-company-websites-selling-personal-details.html#ixzz260WNCodO

Protalinski, E. (2012) 'Facebook tests prompt asking you to snitch on your friends who aren't using their real name', *Next Web*, 21 September, http://thenextweb.com/facebook/2012/09/21/facebook-now-wants-snitch-friends-arent-using-real-name/

RSA (2011) *The Psychology of Social Engineering*, RSA, July, http://www.rsa.com/solutions/consumer_authentication/intelreport/11477_Online_Fraud_report_0711.pdf

Schneier, B. (2008) 'How to Create the Perfect Fake Identity', *WIRED*, 4 September, http://www.wired.com/politics/security/commentary/securitymatters/2008/09/securitymatters_0904

Shaikh, T. (2003) '£1,400 buys a new identity, a new passport and entry to the UK', *The Telegraph*, 12 January, http://www.telegraph.co.uk/news/uknews/1418636/1400-buys-a-new-identity-a-new-passport-and-entry-to-the-UK.html

Smith, R. (2010) 'Identity theft and fraud', pp. 273-301 in Y. Jewkes and M. Yar (eds) *Handbook of Internet Crime*, Cullompton: Willan

Stajano, F. and Wilson, P. (2011) 'Understanding scam victims: Seven principles for systems security', *Communications of the ACM*, 54(3):70-75 (early version available at http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf)

Straits Times (2012) 'Real passports with fake identities issued in Indonesia', *The Straits Times*, 17 July, http://www.asianewsnet.net/home/news.php?id=33554&sec=1

Swash, R. (2012) 'A new internet age? Web users turn on 'trolls'', *The Guardian*, 19 October, http://www.guardian.co.uk/technology/2012/oct/19/new-internet-age-trolls

Trueman, B. (2011) 'Is the UK's anti-fraud strategy achieving its aims?', *AccountancyAge*, 14 November, http://www.accountancyage.com/aa/opinion/2124714/uks-anti-fraud-strategy-scratch

Wall, D.S. (2007) *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity.

Wall, D.S. (2007/11) 'Policing Cybercrime: Situating the public police in networks of security in cyberspace', *Police Practice and Research: An International Journal*, 8(2): 183-205 (Revised Feb. 2011) Available at SSRN: http://ssrn.com/abstract=853225

Wall, D.S. (2008/11) 'Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime', *Information, Communication & Society*, 11(6): 861-884 (Revised Feb. 2011). Available at SSRN: http://ssrn.com/abstract=1155155

Wall, D.S. (2010a) 'Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age', pp. 68-85 in T. Holt, T., and B. Schell (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, Hershey, PA (USA): IGI Global

Wall, D.S. (2010b) 'The Organization of Cybercrime and Organized Cybercrime', pp, 53-68 in M. Bellini, P. Brunst, and J. Jaenke (2010) (eds) *Current issues in IT security*, Freiburg: Max-Planck-Instituts für ausländisches und internationales Strafrecht

Wall, D.S. (2012) 'Enemies within: Redefining the insider threat in organizational security policy', *Security Journal*, advance online publication, March 19, pp.1-18

Wall, D.S. (2013) *The Future Challenge of Identity Crime in the UK*, Paper DR20, Future of Identity Series, London: Government Office for Science Foresight initiative project

Wolf, N. (2012) 'Amanda Todd's suicide and social media's sexualisation of youth culture', *The Guardian*, 26 October, http://www.guardian.co.uk/commentisfree/2012/oct/26/amanda-todd-suicide-social-media-sexualisation

(All www addresses correct on 12th November 2012).

Foresight
1 Victoria Street
London SW1H 0ET
www.foresight.gov.uk
URN 13/521