Government Office for Science

Foresight

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

DR 20: The Future Challenges of Identity 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

The Future Challenges of Identity Crime in the UK

The purpose of this paper is to explore the challenges, context and future of identity related crime in the UK. It will contribute to the Government Office for Science Foresight project that is investigating how changes in technology, geo-politics, demographics and economics over the next ten years might affect notions of identity and subsequently impact on behaviour. This paper accompanies DR19 ‘Identity Related Crime in the UK’ (Wall, 2013) of this same Foresight series which explores the regulative challenges that various identity crimes are individually posing for the public, policymakers and also law enforcement.

1. Introduction

The first part of this paper[1] introduces the main challenges that identity crimes give rise to. The second part explores the role played by technology in identity crime by looking at how it is used to create and manipulate identities and also maintain multiple identities for criminal purposes. The third part looks at how the same technologies can be used to police identity crime. The fourth part discusses the different views of governmental, corporate and personal responsibility for identity crime and the fifth part considers whether identity crime is a driver for radicalisation and protest action. The conclusion draws together the earlier findings to ascertain whether or not identity fraud will become more or less possible over the next decade.

Identity Crime is a generic term used to describe a range of crimes from full life-identity construction, to credit card theft and then the subsequent frauds. Between each point on the spectrum lies an array of activities that each display different behaviours. Perhaps the most important distinction to be made here is to distinguish between *identity or information theft* and the *illegal use of identity information to* commit crime*. Identity theft*[2] is the acquisition of personal identifiers and identity related data, usually through the act of 'phishing' and its social and technical derivatives, but also accidental loss, data breach/ theft, and deception. The *illegal use of identity information,* in contrast to identity theft, can take a number of different forms. It can be used to manipulate existing or create new identities, commit identity fraud[3]*,* and, in the case of new social network media, commit extortion (blackmail) or cyber-bullying (internet trolling) (discussed in detail in (Wall, 2013). The latter indicating how identity crimes are going to develop in the future.

A broad reading of the literature on identity crime (as indicated in Wall, 2013) suggests that fraudsters (both individuals and businesses) will continue to use new technologies to develop instruments of fraud (identifiers) in order to exploit current and new security paradigms. It is anticipated that this trend will continue as western economies undertake austerity measures, which is already an explanation for recent rising low end fraud rates (see CIFAS, 2012). Whilst we can be certain that identity crime is having a negative economic impact, it is also somewhat of an enigma because that negative impact is purely assessed in monetary terms. Little account is taken into hand for the emotional harms experienced by victims, or the negative impacts that the fear of identity crime has upon participation in online facilities. Of great concern is the probability that victimisation will deter economically disadvantaged groups from participating in the Digital Economy. It is the poorest part of the population which can least afford to take risks and so are likely to be generally dis-incentivised from using financial online services and also government services which are becoming an important component of citizenship in the information age.

[1] Many thanks to the two anonymous reviewers who made useful and constructive comments upon an earlier draft of this paper.

[2] Which is not technically a theft under s.1 of the Theft Act 1968: 'A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it'. The implication is that the identity theft will eventually result in the theft of money through fraud.

[3] The identity theft, creating false identity and identity fraud mainly reflects a Home Office Steering Committee definition published on the 'What is Identity Theft?' page of the Identity Theft Website (www.identitytheft.org.uk) which is sponsored by a selection of public and private sector bodies (see list at http://www.identitytheft.org.uk/about-us.asp). It also reflects distinctions found in Solove (2004), Koops and Leenes (2006). I have added the new social media identity crimes.

Before moving on to the next section we first need to identify the main challenges to our understanding of identity crimes. In a crime field where the topics are so contentious, to be forewarned is to be forearmed. 'Identity crime' is particularly contentious in terms of its lack of linguistic ability to accurately describe the acts and also in the way that it is used as a pawn in the debates over the politics of financial crime. It is often misused and not always reported in a coherent manner. Problems with definition and other challenges have contributed to its over-sensationalization and a contrast between perceptions and realities. A useful illustration of this contrast can be found in the Scottish Crime and Justice Survey 2012 which found that 58 per cent of adults were most worried about someone using their personal financial information to obtain money, goods or services and 48 per cent were worried about having their identity stolen (National Statistics, 2012: 6). These figures contrasted starkly with 4.5 per cent of Scottish adults having fallen victim to card fraud in the past 12 months and 0.5 per cent of adults reporting being a victim of identity theft during the same period, including impersonation or using personal information (National Statistics, 2012: 34; also see Levi and Williams, 2012 for further comment). The main challenges to understanding identity crime are seven-fold.

- The terminology is problematic. The colloquial use of the terms is not only inconsistent in so far as identity theft is often confused with identity fraud, but it does not match the law. So, on the one hand the media find it hard to report accurately and on the other hand criminal justice agencies find the term problematic to apply (see discussion in Wall, 2013). Schneier has argued that the current emphasis upon identity theft "… is a misnomer which is hurting the fight against fraud", stating that identity theft would be better conceptualised as "fraud due to impersonation" (Schneier cited by Leyden, 2005). Almost a decade on, 'identity crime' as a descriptor is here to stay, but understanding it is made easier by identifying some of the factors that negatively shape our understanding of it. This is particularly important if the problem of over-sensationalization is to be resolved.

- Because of the problems with definition, any statistics will be haphazard and misuse of the term might obscure and divert resources from key forms of identity crime. For example, currently there is arguably a disproportionate focus upon fraud and relatively little knowledge about the creation of false identity. Harm from identity crime, as identified earlier also tends to be measured in monetary terms.

- Identity crimes are media sensitive, especially when linked with cybercrime. They combine an event or possible event, with cultural experiences (e.g. developed through fiction and film), with the outrage of personal invasion to make very good news stories. In the worst case scenario, single reported events (signal events) can generate a ripple effect that leads to sensationalization and over-sensitivity towards identity crime (see the discussion in Wall, 2007: 166). As a consequence, the public's anticipation of victimisation becomes exaggerated, which is contrasted with very low levels of reporting by victims. The National Fraud Authority found 9.4 per cent who responded to their survey had been a victim of identity fraud in the UK (NFA, 2012), still a high percentage, but less than some surveys would have us believe. This percentage is roughly comparable with other surveys both domestically and internationally.

- Identity crimes are almost invisible to criminal justice agencies and the private security sector, because firstly, they are *de minimis* crimes, too small to investigate in the public interest (see Wall, 2007; 2010). Identity related cybercrimes, tend to be fairly small individually, but significant in their aggregate, particularly, where the crime involves information theft (identifiers) rather than the fraud. They are usually individually small and whilst felt by victims, they are hard to prove and their impacts are also very hard to assess, a quality that victim surveys tend not to pick up. Secondly, identity crimes mainly take place in private transactions that are often invisible to the victim (LoPucki, 2003) and law enforcement. Thirdly, identity crimes (like cybercrimes) fall outside the normal police routine business, which means that unless they are substantial (over £500-£1000, sometimes even more) they are often not investigated even when reported, and most importantly not recorded (Wall, 2007/11). The creation of the National Fraud Reporting Centre (Action Fraud) and a national policing unit, the Police Central e-Crime Unit (PCeU) in the Metropolitan police, in recent years has helped remedy this problem. Not only is the unit achieving much success with cybercrime that impacts nationally and internationally, but important police experience is also being built up in the area. There does still remain, however, a general police-wide problem with intelligence gathering however and the trickle down of experience to local police forces is slow.

- Identity crimes are often confused with conventional crimes (such as frauds) that use technological systems to help organise them. This is in contrast to true cybercrimes which are spawned by networked technologies and often not yet written in law. In between these two positions are a range of hybrid cybercrimes that are conventional crimes, such as frauds and scams, for which the internet gives new globalised crime opportunities (see Wall, 2007 for the distinction). The process of stealing information falls into the hybrid cybercrime category, whereas the bulk sales of the information would fall in the true cybercrimes category. The fraud that occurs subsequently, on the other hand, usually falls into the conventional crime category.

- Identity crimes contain different *modus operandi* that are frequently confused when they are reported by the media. The acquisition of identifiers, via hacking, is a ‘crime against the machine’ and the resulting fraud is a ‘crime that uses the machine’ whereas cyber-bullying, internet trolling etc., are ‘crimes in the machine’. These three distinct forms of cybercrime are represented by three distinct bodies of law (see Wall, 2007:49-51).

- Identity crimes have different impacts upon different victim groups: individuals, corporations and nation states. Whereas victims surveys tend to show a relatively small incidence of victimisation (that the victim felt serious enough to report), often in percentage lower than 10 per cent (see NFA, 2012; National Statistics, 2012), corresponding surveys conducted with businesses and organisations show a much higher percentage of victimisation, often as much as 100 per cent (Wall, 2007: 19). It is hard to assess incidents against the national (usually financial) infrastructure because they often start out as attacks (multiple victimisations) on individuals and/or organisations with the intention of weakening the infrastructure.

Many of the above mentioned challenges to understanding identity crime also provide reasons why so few identity crimes have appeared on the radar of the criminal justice agencies and what this section has indicated is that the many perceptions and realities of identity crime can be quite different. As stated earlier, there are reasons why identity crimes are over-sensationalized, but also possibly under-reported because victims may not know, or even feel, that they are victims, especially with identity theft. Further indication of the confusion between perceptions and realities, especially, the involvement of the internet, is evidenced by research findings that identify only a small percentage of identity crimes as resulting from networked technology. Javelin (2009: 7) found that “(d)espite the hefty blame largely perpetuated by the media placed on the Internet and cyber-crime, online identity theft methods (phishing, hacking and malware) only accounted for 11% of fraud cases in 2008”. Javelin says, friends, not strangers, may in fact, be the main source of identity theft. Only a small percentage of reported losses through identity frauds results from online activities. Most known cases of fraud occur through offline methods much closer to home, through lost wallets (43%), whilst conducting a transaction (19%), friendly theft (13%), data breach (11%), stolen paper in mail (3%) and other (1%).

One of the more reliable indicators of identity fraud is the UK Annual Fraud Indicator compiled by the National Fraud Authority. In January the NFA surveyed a sample of 4000 adults using and online survey and found that 9.4 per cent had been a victim of identity fraud during the past year. Just less than half of victims (44.7%) had been able to recover their losses whereas over half (53.3 per cent) did not. Their average loss was £481. The total UK loss to individuals through identity fraud is £1.3 billion annually (NFA, 2012:26). The total UK losses when business is (seemingly) included is much higher and VeriSign estimate this to be about £3.5b (Ashford, 2010).

In summary, there are a number of conceptual issues that can hinder our understanding of, and responses to identity related crime and challenge law enforcement. Whilst there has been much effort made to overcome them, they still remain a challenge. Moreover, although the incidence of identity crime may not be as prevalent as sometimes claimed (Anderson *et al*., 2012); the final estimate of losses still remains relatively high. The next section explores the role of technology in identity crime.

2. The Role of Technology in Identity Crime

Identity crime is not a new phenomenon, because criminals have long impersonated victims to embezzle their money or commit espionage. Many of ways that technology currently facilitates identity crime are described in (Wall, 2013) however the question asked here is whether or not technology will continue to enable criminals to manipulate and control multiple identities for criminal purposes. Will the technology (in the form of digital footprints; the ability to cross-reference large data sources etc.) make the fabrication of identities and the ability to steal others more difficult? Similarly, will the same technologies an enablers or preventers to making it more possible or less possible for criminals to create and maintain multiple personas for criminal purposes and other purposes both online and offline?

What has changed in recent decades has been the expansion in the technological infrastructures of financial and information services. In more recent years we have also witnessed a massive expansion in the availability and use of social network media technologies, including Facebook, Twitter, YouTube and associated applications. Financial, information and network services need to become more technology dependent in order to increase their level of service and provide what clients want, whilst keeping their service delivery efficient to maintain an edge over their competitors. Therefore, as the need for identifier access systems has increased, then so has the need to possess simultaneous identities (identifiers) that perform different access functions. So, information technology is an enabler and force multiplier that allows service delivery to take place asymmetrically (one-to-many) as opposed to the symmetry (one-to-one) of the previous systems. Many transactions can take place simultaneously and asymmetrically via automated systems whereas previous transactions took place symmetrically one at a time. This multiplier effect works both ways and we know from experience that each technological advance in service delivery also creates new criminal opportunities for identity related crime (see Wall, 2007/11). A further point of discussion here is the possibility of using the same technology as a crime disabler either by designing out crime in the system (see chapters in Ekblom, 2010 and Stajano and Wilson, 2011), by correcting existing design faults (by software updates) or by including monitoring of use (say through transaction logs) so that intelligence can be gathered and wrong doing can be investigated. Technology not only creates criminal opportunities, but the same technology also provides the potential for regulation. In this section the role of technology as enabler of criminal opportunity will next be explored, firstly with regard to the manipulation of identity and the creation and maintenance of multiple identities. In the following section (p12) the role of technology as preventer and regulator of criminal behaviour will be examined.

2.1 The manipulation of identity

As long as there remains value in manipulating or controlling identities then criminals will seek to better their skills in this area and there is evidence that they are becoming more sophisticated, almost professional, in their skills acquisition. The ‘value’ may be financial or status, as is often the case in social network media crimes. The issue here is not so much about the manipulation of identity *per se*, but about identifiers (trusted symbols) that give access to resources. Identifiers which contribute to identity, in the case of individuals to ideas of personhood; in the case of corporations to business identity; in the case of nation states to statehood (state identity). The debates over identity crime can therefore vary in their intensity and depth according to victim groups. Generally speaking, however, identity as we know it is largely a product of post modernity and has become a function of policing the risk society

(Ericson and Haggerty, 1997). It is the product of the techno-social need to develop data doubles in order to enable information systems to 'trust' service users and it contrasts with the prior acceptance of anonymity (see Whitson and Haggerty, 2008). Once verified, identity provides access to resources and therefore becomes a 'thing' in and of itself. This process of objectification gives identity a value that can be either traded or sold for profit. It is, therefore, most useful to distinguish between identifiers (identity assets) and personhood signifiers (full identity)[4]. The former are identity related identity snapshots of the individual that are required by information systems for access to resources. Personhood, by comparison is the bigger picture, a combination of the 'presentation of the self in everyday life' (see Goffman, 1959) and the process of actually living out that self. So, if pin numbers and system access identifiers are about identity then social network media are more about the self and personhood and citizenship. Whilst this distinction appears clear on paper, in practice it is being increasingly muddied in the late information age as our identifiers can become mistaken for our actual identity. Poole argues that online identity is becoming our real identity through social network media access data (reported in Carmody, 2011). For the purposes of this paper it will be argued that there has actually developed a tipping point where the different individual identifiers cumulatively become the identity - stealing enough identifiers enables the criminal to take over the victims' person, not just their identity. Consequently, those wishing to commit identity frauds will manipulate identifiers whereas those wishing to create false identities, bully or troll victims online will manipulate actual identity data. Thus, opportunities for identity crime using identifiers are often created by the way that organisations misuse identifiers because they have failed to plan for proper identity provision and processes for verification. Victims are effectively forced by organisations to provide identifiers that are non-secret and in some cases in the public domain (such as mother's maiden name, first school, social security number in the USA).

A careful reading of the news literature on identity crime, which broadly informs public opinion and drives the politics of the crime agenda, finds many assumptions from a previous age where identity was regarded as unproblematic and which becomes contrasted with the onset of a digital age which has, for various reasons made identity more problematic. Yet, identity is still much the same as it always has been in that it still identifies individuals; however, the requirements for such identification and the environment in which it takes place have changed. Not only have financial systems become dependent upon identifiers, technological identity factors (pin number, personal information), but there are now many more informational and financial facilities available - facilities that increasingly encompass aspects of everyday life, including buying essential goods and services but also accessing government. So, we now have more need for identifier access systems and one of the main transformations in the digital age has been the possession (and need to possess) simultaneous identities that perform different functions in a digital networked world.

Looking to the future, identity can be characterised in many different ways: philosophically, psychologically, politically, economically and socially. For the purposes of this study, we need to look at how crime and identity interact. Identity holds various value characteristics and so far the evidence (or lack of evidence to the contrary) suggests that it will continue to be a key future driver for criminal activity. This value relates to the access to informational sources that the identifier provides and which can be obtained by selling or trading it. Some criminal acts involving identifiers and whole identity are *preparatory*, committed to give access to information in order to organise a criminal act. Others are *implementary*, in that the information gives access to (financial) systems in order to steal resources. Value in identity can also be in the

[4] Drawing on Finch (2002)

form of an intellectual property, for example, at an individual level in an artist's creations, or at a business level if the business is a creator, manufacturer or trader, or combinations of all three). The intellectual property value is both described and protected by copyright, designs; patents and trademark law [please note that intellectual property value is not discussed here].

The ability of criminals to use identity information, despite widespread assumptions to the contrary, is becoming harder as banks, organisations and other agencies ask for combinations of information and discrete forms of identification to enable users to have access to their services. The fabrication of new false identities is also becoming harder for similar reasons. In terms of prevention, as mentioned earlier, four technological methods that rely upon the algorithms that we individually produce are available to assist: facial, textual, behaviour online and behaviour offline. In the future, systems will continue to use some forms of identifiers, simply because the public are now used to them, and the layering of current identifiers seems to be favoured over the introduction of new unique identifiers. The problem here is, as outlined in the conclusion of Wall (2013) whether users would use technically secure systems. So, yes, whilst technology will continue to enable criminals to manipulate and control multiple identities for criminal purposes, technological and social counter-measures will increasingly be used to make the manipulation and creation of those identities for criminal purposes more difficult. The problem with using such technologies is that they are often applied to solve what is in effect a social or business problem, raising privacy concerns about total surveillance and questioning whether such practices would also inhibit creativity and freedom of movement or expression by restricting legitimate forms of behaviour that fall outside the algorithm.

2.2 Creating and maintaining multiple identities

The ability to create and maintaining multiple identities is becoming harder and harder as banks and other agencies rely upon more discrete forms of identification to give users access to their services. The days of 'identity farming' described by crime authors such as Frederick Forsyth, John le Carré, Ernest Hemingway, John Grisham, Victor Ludlum and many others, where the birth certificates of dead child born at approximately the same time as the offender are obtained[5] and new identities carefully constructed over time are largely over. As le Carré himself once enigmatically said, "[t]he more identities a man has, the more they express the person they conceal" (le Carré, 1974: 207). The different identifiers eventually construct the individual and betray him or her. Whilst identity farming creates a good story line, 25 years is usually too long to wait for a pay off, argues Schneier (2008), plus most contemporary cases of false identity have been exposed by a combination of social and technical factors.

In contrast to financial and governmental information systems, it is far easier to create false and multiple identities by using new social network media. As the example in the next section illustrates (also see Wall, 2013), Facebook and the new professional media require real-person identity information for registration, however, many users find it easier to participate with false or alternate identities. Often for legitimate reasons, such as hiding an aspect of their social, sexual or spiritual identity that they may not want employers or others to know about or for political reasons. So the alternate (false) identities may be regarded as false to social media network providers but real to the individuals involved and also their friends!

[5] A number of books and articles are available online that purport how to instruct the reader on creating a false identity. A google search reveals the following books available through Amazon.com and elsewhere. See Charrett (1997); Pinola (2011) and Ahearn and Horan (2010). Also see Schneier (2008) for discussion of this issue.

In principle, intelligent procedures could be developed that connect the various databases together in order to identify criminals and also correct their wrongdoing against victims. In practice, it is very unlikely that interoperability between databases will be fully possible in the near future because of different standards of data collection, different (legal) circumstances of collection, different ethical frameworks, and the fact that databases may be held in both the public and private sectors.

3. The Role of Technology in Policing Identity Crime

The role of technology in the policing of Identity Crime (policing used here generally) is at the heart of many questions frequently asked about identity crime, but which are rarely answered. The more simple questions such as, will identity fraud become more or less possible over the next decade, are easier to answer. Yes, at the time of writing, chip and pin technology has successfully and drastically reduced some forms of identity related crime (FFAUK, 2010). The problem with such answers is that they are never so simplistic. Whilst, chip and pin has reduced frauds, they are not invulnerable, see Leyden (2012b). As long as identity has a tradable value, it is unlikely that identity crime will disappear over the next decade. What is certain is that as one form of identity crime disappears, another opportunity will emerge alongside new convergences of technology. New forms of mobile payments schemes, for example, such as Barclaycard's contactless payment scheme[6] are being introduced and will inevitably bring with them new ways of committing fraud.

The point being made here is the identity crime will never be eradicated. It can only be managed and a key part of the discussion about identity security management is about its substance. How would we know if it had been eradicated because the impact of identity crimes and therefore solutions is evaluated almost solely in terms of monetary loss, which with a few exceptions tends to increase annually (NFA, 2012; also Javelin, 2012). However, the impact of identity crimes is much broader than money because not only are there identity crimes that cause other forms of harm, but when they do, they also have negative impacts upon the victims' financial reputation (inc. credit rating) and psychological impacts upon the victim's personhood and wellbeing.

The impacts of identity crime and their resolution are never completely resolved (Solove, 2004) because of knock-on effects, such as the problem of sleeper fraud (the continued use of information to defraud long after the event). Whilst illegally taken, organisationally generated identifiers (passwords, etc.) can quickly lose their validity, but personal information does not, and can potentially be used to commit frauds long after the information has been acquired. Not surprising then, that identity crimes remain a great worry for victims as the Scottish Crime and Justice Survey found, the fear of identity crime is often 10 or more times the actual incidence (National Statistics, 2012: 6).

But will new technologies, for example, make the fabrication of identities and the ability to steal others more difficult, will it prevent criminals from creating new multiple identities and could it be used for intelligence-gathering and policing responses? Using technology to police identity crime has a number of complexities. The banks, financial houses and other information organisations have used computer technology to provide more convenient services to their customers. Not only does this improve convenience for the customer, but it also increases profits for the organisations involved. The true 'cost' to the individual of this arrangement is that it changes the relationship between the organisation and the customer because the customer-oriented service distanciates (Giddens, 1990) them from the provider. It disembeds customers from the 'social' structure around the organisation that they were once part of – e.g. local banks no longer know their own customers - so that they no longer identify as strongly with it and the

[6] Barclay's contactless payment scheme, http://www.barclaycard.co.uk/simplepayment/index.html

similarly the organisation does not identify with the customer as strongly. The responsibility for information security shifts from the organisation to the individual so, the 'security' problem is re-presented as the feckless individual freely giving away their personal information, rather than business sector not creating robust systems with good quality security (Whitson and Haggerty, 2008). The shift from information security to identity security places a great emphasis on identity and also the use of technology to secure it. The simple use of technological means to prevent identity theft, whilst theoretically strong, also creates a series of tensions. On the one hand is the need to protect the individual's privacy rights and protect them from unnecessary and unlawful intrusion either by others, the police or the organisation. On the other hand, there is the view that we have experienced a fundamental change, in fact, the death of privacy because of the 'disappearance of disappearance' (Haggerty and Ericson, 2000). In lay terms, networked technologies keep searchable logs of almost every transaction that we make and can therefore data mine it to identify users and their online behaviours.

In theory, technological processes can be used to govern the use of identity, to make the individual use their identities and identifiers responsibly and to identify abuses and the abusers of identity. The big question, however, is whether good security can also uphold the principles of privacy as there is a perpetual tension between the two. This tension is found in many of the debates about preventing identity crimes, especially, where technological processes are employed (see Solove, 2004)[7].

Recent thinking about identity crime prevention has begun to a shift from using more traditional informational identifiers such as biometrics, to thinking about new forms of behaviourmetric identification (Harry, 2009; Erdem, 2011). Using technologies that were originally developed for marketing purposes, behaviourmetrics is a variation of biometrics that uses behavioural algorithms instead of biological characteristics in order to develop a digital fingerprint and it is gaining popularity. Behaviourmetrics typically uses typing rhythm, gait, and voice to build its algorithms and it can be expanded to almost any form of behaviour, including networked behaviours. *Digital* footprints created by of our regular usage of networked technologies create patterns of behaviour that not only identify individuals, but can also observe *irregularities in behaviour* online and offline that indicate potential criminal behaviour or even potential victimisation. Similarly, the text written by individuals also indicates regularities and *irregularities in writing style* that may indicate that the individual is either committing a crime or is being victimised. Add these to behavioural recognition and facial recognition and other biometric information and technological processes can be used to regulate criminal behaviour and also protect users against victimisation. Each activity creates an algorithm of an aspect of our social action, a grand digital footprint that can identify us and even be used in access control. In theory, future technologies will (in theory) not require identifiers as they will be able to identify our complete identity by our actions (Harry, 2009; Erdem, 2011). This possibility raises concerns for values, such privacy, but also generates a set of six counter arguments:

- *False positives* and tolerance levels for failure. The problem of false positives can arise when tolerance levels for matching data are inappropriately set. This can mean, for example, that individuals looking alike or acting in a similar manner to others may confuse the behaviour algorithm. See for example, the case of US citizen, John Gass whose driving licence was checked by software designed to identify fakes and revoked because the software thought he

[7] N.B. US the debates about security and privacy revolve around the US Constitutional Amendments where as the debate in the UK and EU revolve around the European Convention on Human Rights as articulated in the Human Rights Act 1998.

looked like another driver (see Boyle, 2011). False positives reduce trust in behaviourmetric systems.

- *False negatives* and 'dirty data' arising from the human problem of badly inputted and maintained data, colloquially known as GIGO (Garbage in, Garbage Out). Once data has been inputted wrongly or not maintained it becomes very problematic, as a data double, to which incoming data is compared against for verification. Although an exaggerated example, the loss of a limb may render an individual invisible to an intelligent surveillance the machine if its loss was not reported and data sets not amended accordingly. The machine would be looking for two arms or legs and only finding one. Poor data management becomes even more problematic in a world where governments are moving towards 'big data', data sets that are so large and complex that it becomes difficult to process using conventional database management tools.

- *Learned or faked behaviour to create false positives or negatives*. A question arises as to whether algorithmic behaviour could be electronically faked or even learned by fraudsters either to convince a system that the fraudster is someone else or not.

- *Unnecessary identifiers*. There is a strong critique of the need for so many unnecessary unique identifiers driven by particular organisational needs. Some are personal and others system generated. There are few common standards or core common principles and their establishment is prevented because of the practice of constantly modifying individual legacy systems to keep them going.

- *Legal problems*. The use of behaviourmetrics creates legal problems over privacy legislation and more generally reverses the burden of proof so that the individuals have to prove that they are innocent. As opposed to being innocent until proven guilty.

- *Ungovernability*. Finally the contemporary debate regarding surveillant technologies has raised the important general question as to whether or not "[t]he technology has overtaken our ability to regulate it" (see further Hastings, 2012).

At the heart of the behaviourmetrics problem is a fundamental tension between the needs of the organisation as expressed in its informational requirements and the needs of the individual to use the system in the way that they want to. See, for example, the recent tensions between the Facebook organisation needing real name identities in order to develop their business model and many Facebook users wanting precisely the opposite. Jeffries (2012) cites Mason, a sometimes, political activist who has modified his name so that he can exercise freedom of expression and is so doing has learned to live with his pseudonym along with his family and friends;

> "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. "I can't imagine putting my real last name on Facebook. I've gotten very used to my 'fake' name." His girlfriend Rachel, 24, uses her grandmother's maiden name as a surname. Like Mason, she finds her pseudonym doesn't interfere with using Facebook at all Jeffries (2012).

Yet, despite this user trend, Facebook has even experimented with schemes that encourage friends to uncover friends who use false names (Protalinski, 2012). There is an ironic twist here because the behaviourmetric test would theoretically identify Mason from his textual behaviour without any identifying factors real or fake. Perhaps the most convincing argument for not using biometrics/ behaviourmetrics as sole identifiers, however, is their unreliability because of their propensity to show false positives, not just in terms of facial recognition, but also in terms of writing given the ‘cut and paste’ world of the internet blogosphere.

The same technological opportunities to develop criminal networks will be present in the foreseeable future as currently exist, though through new media, for example, more located in mobile technologies than at the present. Consequently, there will likely be more opportunities will exist for intelligence gathering and policing. The same technologies that create the opportunities for crime also create possibilities for policing (Wall, 2007 ch 8). The main challenge for police, however, will be to maximise those opportunities, whilst also dealing with any ethical issues that arise, for example, if gatekeepers to closed networks have to be deceived into allowing access in order to covertly surveille them. This issue has been brought to the fore in the recent discussion about police use of Facebook (Burns, 2012). New York Police are actively engaging with Facebook by creating fake accounts in order to entrap offenders (Tickle, 2012). In so doing, the police will increasingly experience legal tensions, as they often do when conducting covert operations, between the collection of intelligence about criminality and the compilation of conclusive evidence of wrongdoing. The courts in the US seem to be more ready to accept such evidence than in the UK.

Since its inception two decades ago the internet has been used by criminals to create distributed networks that enable them to discuss their activities and even learn their trade, for an example of this see, Wall (2007: 66-68). As stated earlier, the internet gives criminals a global reach and acts as a force multiplier. It also connects criminals to form new forms of organisation. Criminals today may conduct criminal operations without ever meeting, communicating via online peer to peer (p2p) networks. These networks can also enlist others who are broadly interested in the technical aspects of the criminal activity, but not be part of it. In other words, criminals people source solutions to their technical problems. But the networks are not invisible, even when cloaked, and can often be identified. A number of scholars have, with mixed results, begun to use Social Network Analysis software, such as UCINET, to analyse network data in order to analyse criminal networks (see for example, Morselli, 2009; Holt *et al*., 2012; Décary-Hétu and Dupont, 2012; Medina, 2012).

4. Conflicting Views on Responsibility for Identity Crime

There is clearly a disparity between governmental, corporate and individual views as to where risk and responsibility lies for identity crime. This disparity begs the question as to how will conflict be resolved between the Governmental (and corporate) view of where risk and responsibility lies and the citizens' own views of risk and responsibility for dealing with it?

Solove (2004: 118) has argued that identity thieves are only one of the culprits in identity theft and that both Government and business should also bear some responsibility. He goes on to conclude that (intentionally or unintentionally) identity theft is created by an architecture that has been legally constructed. Furthermore, he goes on to argue that it also contributes to the harm experienced by victims. This is because law not only fails to regulate the bureaucracies, but is also indifferent, or has little regard for the welfare of identity crime victims (Solove, 2004: 118). One of the responses by the corporate sector has been to shift responsibility from the bank to the individual. Rather than being the responsibility of the bank, the redefinition of fraud as identity theft suggests that it has become the individual's fault for allowing their identity to be stolen (Solove, 2004, Whitson and Haggerty, 2008). The result of the shift in responsibility to the victim (from the bank) has received a varied response and Whitson and Haggerty have argued that the corporate sector has promoted methods for protection against identity theft that are beyond what is reasonably practicable for most citizens and arguably mask the role played by major institutions in fostering the preconditions for identity theft (Whitson and Haggerty, 2008: 591).

As a consequence, a critical eye would view much of identity theft policing policy (where it exists) as bridging the reassurance gap in policing cybercrimes. The public fear of identity crime creates demands for security that government and police cannot deliver (paraphrasing Wall 2012) and this is exacerbated by the fact that, as Anderson has observed, fraud has been in policy terms an orphan caught between Home Office, BIS, the FSA, the OFT and others which has led to fraud being redefined it as 'identity theft' (Ross Anderson, response to Hawkes, 2011). In many ways the problem was historically more complex that this, because the Fraud Act was only introduced in 2006 to give fraud comprehensive coverage by law. It had previously been dealt with indirectly by a range of legislation. Furthermore, fraud policy was caught for many years between the Attorney General's Office, the Cabinet Office and the Home Office. Similarly, policing fraud was caught between the Serious Fraud Office, SOCA (Serious and Organised Crime Agency), the City of London Police and regional police forces.

Today, the UK fraud policy making process is more coherent than in the past. It is located around the National Fraud Strategy (Attorney General's Office) (NFSA 2009) and national fraud policing is led by the City of London Police, though more serious and organised identity frauds are dealt with by the Police Central e-Crime Unit (PeCU) or possibly the Serious Fraud Office. In the future it will be also covered by the economic crime command of new National Crime Agency when it comes into force (Home Office, 2011). Currently, the public report fraud victimisation to Action Fraud, the national fraud reporting centre. The reports are triaged by a National Fraud Intelligence Bureau, based in the City of London Police, which decides upon the appropriate response. Strategic intelligence is sent to the National Fraud Authority for inclusion in the National Fraud Indicator (NFA, 2012) and provides an evidence base for developing fraud policy, notably the National Fraud Strategy. Tactical intelligence is sent to relevant policing agencies.

The *elephant in the room* in debates over identity crimes is the problem of helping victims to restore their damaged (identity) reputations online. It takes approximately six to seven months to readjust one's credit record following identity fraud victimisation. There are a number of private agencies that provide services to protect reputation and also privacy, but these are mostly preventative. See Reputation services http://www.reputation.com also Privacy Defender, http://privacy-defender.com/. The process of repairing financial reputation is more complex and service quality varies.

An increased clarity of division about responsibilities for fraud on the part of public and private sectors, combined with education (e.g. public service broadcasts), plus a trusted system for repairing damaged reputation and lost identities would help to untangle the current confusion between the citizen view of identity theft and that of government.

5. Identity Crime as a Future Driver of Radicalisation and Protest

As social networked medias become more popular and prominent in mass social and political process, see for example, the Arab Spring but also the US elections (for different reasons), then the question arises as to what extent will notions of identity become drivers of crimes of order and even terror, particularly in relation to radicalisation, extremism, protest and resistance. Can expected changes in identity be used as a predictor of changes in crime?

The expected changes in identity are not so much predictors of change in crime, but of broader political activities. The more conventional types of identity crime are unlikely to be drivers of identity crime, however, the newer forms of identity crime related to social networking media may be drivers of radicalisation. One can imagine that successful appeals to individuals on social network sites to identify with particular identity groups could radicalise them if they identify with, and become absorbed into, an identity group. The threat of ejection or rejection might increase the hold of the group on its members. Thus radical information could be drip fed. But radicalisation must be measured in terms of resulting social action in the form of protest, resistance and intervention. Research seems to indicate that only those who are ready to be radicalised will become so, suggesting that radicalisation might take place because of circumstances in addition to membership of a social network.

Whilst the jury is still out on the issue of social networks, identity group radicalisation and extremism, events such as the Arab spring have clearly demonstrated that a combination of (national) identity, feelings of injustice and social network media can lead to information and mis-information flowing virally across the networks. What is clear is that radicalisation and extremism are different issues to protest and resistance. The former are more likely to be found in criminal codes, whereas the latter more likely upheld by law and international political values as a check against abuses of authority. Clearly, social network media has had a significant impact on levels of protest and resistance in that truthful and reliable information that counters un-truths can quickly be circulated. Also, the same new media enables the circulation of key information about the organisation of protest meetings, plus information about the forms of resistance to take. Evidence of this is found in the organisation of protest in Tunisia (Ryan, 2011), Egypt (Alexander, 2011) and Iran (Twitter Revolution, Leyne, 2010) and Syria (Othman, 2012). Othman argues that in these countries it is not just a case of technology driving revolutions but the revolutions are now driving the technology;

> Since last year thousands of (Syrian) activists have been educated because their lives depend upon it. The internet has been so central to the revolution in Syria, it has brought us together and it has given us freedom. Because a free and open internet is the most powerful tool in combating human rights abuses (Othman, 2012).

There are also examples elsewhere, for example, the G20 protests in Canada, Italy and the UK. The protests and resistance exploit the crowd or people sourcing potential of the internet (see Tapscott and Williams, 2007)[8]. The problem with such behaviours is working out whether they are identity driven or just involve the use of identity.

[8] N.B. Tapscott and Williams describe the basic principles, though they are primarily describing its use for business.

6. Conclusions

This paper has explored the challenges, context and future of identity related crime in the UK. It has distinguished between the acquisition of personal or corporate information (identity theft) and its subsequent use to defraud, extort, bully or defame victims. At the root of the identity crime debate are a number of terminological and conceptual issues that have led to identity crime becoming over-sensationalised and inevitably mis-reported – the theft of information becomes confused with the crimes that use the information. This has contributed to the public's fear of identity crime being up to ten times greater than their actual victimisation. The statistics therefore do not present the realities of identity crimes. Realities, which it is suggested, are that the impacts tend to be individually smaller and different than anticipated, and possess characteristics that keep them off the radar of the criminal justice system. Until recent years, frauds and identity crimes have not been regarded as police territory, though recent developments in policing, e.g. Action Fraud, are addressing this matter.

The role of technology has changed over the past decades with the expansion of networked technological infrastructures for delivering financial and information services. But, whilst popular with business and their customers, the new customer focused services have had the knock-on effect of shifting responsibility for security to the user. This shift becomes even more problematic with developments in social network media technology which changes the identity crime profile to include extortion and bullying (trolling). The distinction is made in the paper between identity and identifiers that are necessary for systems to work. The problem is that identifiers have become mixed up with identity and the continued modification of legacy systems is likely to hinder any attempts to introduce standards of identifier. Despite this resistance, security systems that use combinations of identifiers are clearly reducing the manipulation of identity and also the creation and maintenance of multiple identities for criminal purposes. However, this reduction would seem to be limited to existing systems and technology. The new social media network technology creates a whole new ball park and introduces new forms of identity crime that creates new forms of financial and especially non-financial harms.

Of course, the very technologies that create criminal opportunities can be also harnessed to police new crimes (in the broader sense). This has certainly been the case with chip and pin identity and frauds. There is a different problem, however, with social network media which insists upon real life identity information, information that often undermines the freedoms that social network media provide, but also expose individuals to possible extortion and bullying. A possible solution to issues of identity has been suggested in the form of biometrics and particularly behaviourmetrics, however, for each advantage there are more disadvantages. The big question asked here is whether good security can also uphold the principles of privacy as there is a perpetual tension between the two. To resolve this tension, however, will require clarity of division about responsibilities for fraud on the part of public and private sectors, combined with education (e.g. public service broadcasts), plus a trusted system for repairing damaged reputation and lost identities.

Finally, it was considered whether changes in identity crime could become drivers for crime in relation to radicalisation, extremism, protest and resistance. It was concluded that radicalisation and extremism are different issues to protest and resistance. Not only are radicalisation and extremism more likely to be regarded as crimes, but they also require other circumstances to be present. Protest and resistance are quite different as they are often upheld by value systems, if not by laws of freedom of expression. Plus, there is more potential for protest and resistance through new social network media. As stated earlier, the technology no longer drives revolutions, but the revolutions are now also driving the technology. Whilst we can make observations about the future of identity crime, the reality is that we do not really know because the convergence of technologies can quickly shape our lives. Remember that a decade ago we did not anticipate the impact that Facebook, Twitter and also botnets would have on our lives and in shaping the cyberthreat landscape.

References

Ahearn F. and Horan, E. (2010) *How to Disappear: Erase Your Digital Footprint, Leave False Trails, and Vanish without a Trace*, Guildford Ct.: Lyons Press

Alexander, A. (2011) 'Internet role in Egypt's protests', *BBC News Online*, 9 February, http://www.bbc.co.uk/news/world-middle-east-12400319

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

Ashford, W. (2010) 'UK internet users need to be more vigilant as online fraud hits £3.5bn, says VeriSign', *ComputerWeekly.com*, 1 June, http://www.computerweekly.com/news/1280092905/UK-internet-users-need-to-be-more-vigilant-as-online-fraud-hits-35bn-says-VeriSign

Boyle, R. (2011) 'Anti-Fraud Facial Recognition System Revokes the Wrong Person's License', *POPSCI*, 18 July, http://www.popsci.com/gadgets/article/2011-07/anti-fraud-facial-recognition-system-generates-false-positives-revoking-wrong-persons-license

Burns, K. (2012) 'NYPD releases statement about social media use in investigations', *Washington Square News*, 21 September, http://nyunews.com/index.php/2012/09/21/nypd-2/

Carmody, T. (2011) 'You Are Not Your Name and Photo: A Call to Re-Imagine Identity', *WIRED*, 20 November, http://www.wired.com/business/2011/10/you-are-not-your-name-and-photo-a-call-to-re-imagine-identity/

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

CIFAS (2012) *2011 Fraud Trends: 2011 fraud trends: fraud levels surge upwards*, Press release, 26 Jan, http://www.cifas.org.uk/annualfraudtrends-jantwelve

Décary-Hétu, D. and Dupont, B. (2012) 'The Social Network of Hackers', *Global Crime*, 13(3):160-175.

Ekblom, P. (2010) (ed) *From Research to Realization: Designing Out Crime from Products*, New York: Criminal Justice Press

Erdem, S. (2011) 'Maintaining The Security In Internet Marketing: Moving From Biometrics To Behaviometrics', *Review of Business Information Systems*, 15(3): 43-48

Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*, Oxford: Oxford University Press

FFAUK (2012) *Fraud the facts 2012*, Financial Fraud Action UK, http://www.financialfraudaction.org.uk/Publications/#/1/

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

Giddens, A. (1990) *The Consequences of Modernity*, Cambridge: Polity

Goffman, E. (1959) *The Presentation of Self in Everyday Life*, New York: Anchor Books

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

Harry, D. (2009) 'Putting Behavioural Metrics In Perspective', *WebProNews*, 15 January, http://www.webpronews.com/putting-behavioural-metrics-in-perspective-2009-01

Hastings, R. (2012) 'New HD CCTV puts human rights at risk: Watchdog warns: Big Brother Britain has arrived unnoticed', *The Independent*, 3 October, http://www.independent.co.uk/news/uk/crime/new-hd-cctv-puts-human-rights-at-risk-8194844.html

Hawkes, N. (2011) 'How not to measure identity fraud', *Straight Statistics Blog*, http://www.straightstatistics.org/article/how-not-measure-identity-fraud

Holt, T., Strumsky, D., Smirnova, O. and Kilger, M. (2012) 'Examining the Social Networks of Malware Writers and Hackers', *International Journal of Cyber Criminology*, 6(1): 891-903

Home Office (2011) The National Crime Agency: A plan for the creation of a national crime-fighting capability, Home Office, http://www.homeoffice.gov.uk/publications/crime/nca-creation-plan?view=Binary

Javelin (2009) *2009 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

Koops, B-J., and Leenes, R. (2006) ID Theft, ID Fraud and/or ID-Related Crime - Definitions Matter, *Datenschutz und Datensicherheit*, 30(9): 553-556. Available at SSRN http://ssrn.com/abstract=982076

Le Carré, J. (1974) *Tinker, Tailor, Soldier, Spy*, London: Hodder and Staughton

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

Leyden, J. (2005) ‘Fight fraud not ID theft’, *The Register*, 28 April, at www.theregister.co.uk/2005/04/28/id_fraud/

Leyden, J. (2012b) ‘Chip and PIN keypads 'easily fooled' with counterfeit cards’, The Register, 27 July, http://www.theregister.co.uk/2012/07/27/chip_and_pin_keypad_insecurity/

Leyne, J. (2010) ‘How Iran's political battle is fought in cyberspace’, *BBC News Online*, 11 February, http://news.bbc.co.uk/1/hi/world/middle_east/8505645.stm

LoPucki, L. (2003) ‘Did Privacy Cause Identity Theft?,’ *Hastings Law Journal*, 54(4): 1277-1297.

Medina, R. (2012) ‘Social Network Analysis: A case study of the Islamist terrorist network’, *Security Journal*, Advance Online Publication, May 28

Morselli, C. (2009) *Inside Criminal Networks*, New York: Springer

National Statistics (2012) *2010/11 Scottish Crime and Justice Survey: Main Findings*, National Statistics/ Scottish Government, http://www.scotland.gov.uk/Resource/Doc/361684/0122316.pdf

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

Othman, D. (2012) ‘Syria: 'The internet has been central to the revolution'’, The Guardian, http://www.guardian.co.uk/world/video/2012/nov/04/syria-internet-video

Pinola, M. (2011) *How to Create a Fake Identity and Stay Anonymous Online*, (publisher unknown – available online)

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

Ryan, Y. (2011) ‘How Tunisia's revolution began’, *Aljazeera*, 26 January, http://www.aljazeera.com/indepth/features/2011/01/2011126121815985483.html

Schneier, B. (2008) ‘How to Create the Perfect Fake Identity’, *WIRED*, 4 September

Solove, D. (2004) *The Digital Person: Technology and Privacy in the Information Age*, New York: NYU Press

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)

Tapscott, D. and Williams, A. (2007) *Wikinomics: How mass collaboration changes everything*, London: Atlantic Books

Tickle, L. (2012) ‘How police investigators are catching paedophiles online’, *The Guardian*, 22 August, http://www.guardian.co.uk/social-care-network/2012/aug/22/police-investigators-catching-paedophiles-online

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. (2010) ‘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. (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) *Identity Crime in the UK*, Paper DR19 Future of Identity Series, London: Government Office for Science Foresight initiative project

Whitson, J. and Haggerty, K. (2008) ‘Identity theft and the care of the virtual self’, *Economy and Society*, 37(4): 572-594

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

Foresight
1 Victoria Street
London SW1H 0ET
www.foresight.gov.uk
URN 13/522