Responding to Identity Crime on the Internet

Eric Holm
The Business School. University of Ballarat
PhD Candidate at Bond University
P.O. Box 663, Ballarat VIC 3353
e.holm@ballarat.edu.au

ABSTRACT

This paper discusses the unique challenges of responding to identity crime. Identity crime involves the use of personal identification information to perpetrate crimes. As such, identity crime involves using personal and private information to for illegal purposes. In this article, the two significant issues that obstruct responses to this crime are considered. These are first, the reporting of crime, and second the issue of jurisdiction. The paper also presents an exploration of some responses to identity crime.

KEYWORDS

Identity crime, regulation, online fraud, jurisdiction, personal information.

1 INTRODUCTION

Certain information is worth money whereas other information is worthless when it comes to crimes involving identity [1]. The information that is valuable to the identity criminal is that which can be converted into gain, typically by way of fraudulent activity [2]. Certain information, particularly personal identification provides opportunities for identity criminals to either obtain credit under false pretenses or to impersonate another for like purposes [2]. Personal identification particulars include social security details, driver's license details, passport details as well as other information [2]. The theft of identity particulars may be the catalyst for a number of crimes that follow. The offenses that may follow can include fraud, money laundering, organized crime and even acts of terrorism [2].

There are two variations to identity crime committed by an identity criminal. The first is through the assumption of parts of another's identity to perpetrate the crime [3]. This involves the criminal using parts of the victim's identity to obtain goods or service, for instance [3]. The second is through the assumption of identity wholly which involves the criminal basically becoming the victim [4]. This involves, establishing lines of credit while impersonating the victim. Each type of identity crime has costly implications for an individual [5].

Identity crime is reliant upon information [6]. Much of the information used for identity crimes is obtained through various means on the Internet. A study conducted in the United States on identity crime found that the most common method used for obtaining information was to purchase the information on the Internet [7]. However, information is also obtained by other means such as through committing computer crimes including spam, scams and phishing [8] as well as other crimes. Importantly it is the availability of personal information that is the enabler for identity crime [2]. Sometimes this information can simply be acquired through the interpersonal exchanges that take place on the Internet, such as, through social networking [9].

The misuse of information for identity crime occurs typically when information is used for gain [4]. However, not all identity crime leads directly to a financial gain and there may be other motivations for committing such crime, like avoiding criminal sanctions [10]. Therefore, the impetus for such crime is dependent upon the motivation of the offender [10].

There is debate as to whether identity crime is more prominent on the Internet [11] or elsewhere. Interestingly, sometimes components of this crime may take place both online and offline [12]. However, an important reason why so much identity crime takes place on the Internet is that a significant amount of personal identification information is stored on the Internet as well as there being ample targets [13].

The exposure to risk of an individual online is dependent on many things. Information is exchanged on the Internet not only by individuals, but by governments and corporations [14]. While it is argued that the decision to interact on the Internet is associated with exposing oneself to greater risk, [15] ultimately a latent risk subsists for all information on the Internet [16]. Indeed, it seems that the greater the amount of personal information on the Internet, the greater the risk a person has of becoming a victim of identity crime.

Information is used in a variety of ways to perpetrate identity crime. According to the Social Security website, a common example is the misuse of social security numbers in the United States [17]. This personal identifier is a key identification detail that can be used in conjunction with a person's name to establish identity. This information is used by the identity criminal to use or establish an identity for crime [17]. Other notable personal identification information includes passports, birth dates and bank details, but is not limited to these [18].

2 THE ISSUE OF RELIABLE DATA

The losses attributable to identity crime can be measured by monetary losses [19] but a number of additional offenses can be committed once personal information is stolen. In Australia it has been suggested that identity crime is one of the more prominent emerging types of fraud [20]. However, one of the challenges of recording this crime in is that identity crimes are at times subsumed into the recorded incidence of other crime such as fraud [21]. The misreporting of this crime tends to distort the reliability of data that pertain to the measurement of identity crime [22]. Importantly, different ways of reporting the crime result in different responses to such crimes [2].

In 2012, the Australian Bureau of Statistics (ABS) estimated that approximately three per cent of the Australian population had become victims of identity crime [23]. The most significant implication of this crime was financial [24]. In 2006, the losses arising from identity crime in the United Kingdom economy was $1.7 billion [25]. The United Kingdom figure took into account the cost of preventative measures as well as the costs associated with the prosecution of cases. In many statistics relating to identity crime, the wider losses attributable to identity crime are not considered despite being significant.

Conservatively there are significant costs associated with identity crime that have been estimated at tens of billions of dollars worldwide [26]. However, it is difficult to gather an accurate view of the total cost attributable to this crime because instances of identity crime are not always reported. For instance, the ABS suggests that only 43 per cent of victims of crimes involving credit and bank cards in 2007 were prepared to report this crime to police [27]. This suggests a significant proportion of identity crime relating to credit and debit cards is not reported [28]. This distorts the statistics on the true incidence of identity crime.

The direct monetary losses arising from identity crime are more easily quantifiable but the indirect losses remain more difficult to measure. A cost rarely considered is the indirect cost related to a victim psychologically [29]. Likewise, there are losses attributable to lost trust that can also be difficult to measure [30]. In addition, there is a hidden cost associated with reputational damage that is similarly difficult to reflect in monetary terms partly due to the intangible nature of this loss [31]. These indirect costs are also rarely considered in the statistics that pertain to identity crime.

There are costs with the preventative measures [32] taken to reduce identity crime which are not contemplated when measuring the impact of this crime. Indeed, there are numerous preventative steps that can be taken to overcome the threats of cyber-crime. For instance there may be preventative measures taken through technological means [33] as well as physical security measures [34]. These have a cost associated with them and this cost is seldom incorporated into the overall costs associated with crime [35].

There are broader implications of identity crime on national economies that have scarcely been researched [36]. What remains difficult to ascertain is how extensive the impact of this crime is globally [2]. Where losses are sustained, these are not recorded on any global register of losses but rather are recorded domestically [37]. Further, there is no central repository of data pertaining to identity crime; the data gathered are both varied and dispersed [38]. This makes the reporting of accurate global statistics on this crime problematic. A central repository of information that pertains to victimization arising from identity crime would be most useful for law enforcement efforts [39].

3 THE ISSUE OF JURISDICTION

There is no central body that controls information dissemination on the Internet. The Internet itself is dispersed and thereby transcends all jurisdictional boundaries. This presents difficulties in responding to identity crime in terms of the coordination of investigation and enforcement efforts [40]. Furthermore, the regulatory responses to identity crime also vary depending on the particular emphasis that is placed upon the regulatory responses to these domestically [41]. There are variations in the way in which identity crime is dealt with. As most responses to identity crime are dealt with through domestic criminal sanctions, these differences identify the domestic priorities placed on the responses to this crime.

Contrasts can be made in the regulatory responses to this crime. For example, in the United States, the penalties applicable under federal law are fifteen years' imprisonment and a fine [42]. Comparatively, Australian offenses under Commonwealth Law have penalties with a maximum of five years' imprisonment [43]. Likewise, differences also exist in regard to the restorative functions of these laws. The variations in penalties as well as other functions point out the different importance placed on this crime.

Similar variations in regulatory responses exist within the states and territories of Australia. While one state may react to the crime of dealing with and possession of identification material with imprisonment for five years [44] another may prescribe a penalty of seven years [45]. Furthermore, other jurisdictions, such as the Northern Territory, do not have offenses that recognize identity crime as the core offense and instead they deal with this through other offenses [46]. There are also varied responses to restorative justice.

The issue of jurisdiction stems from the ability of the state to bring an action against the identity criminal. Historically, the effects doctrine has been adopted as a way to justify a state taking action against the individual [47]. This doctrine applies where the harm is linked to the state [47]. This approach has been utilized as a justification for which an action to apply criminal sanctions may be taken [48]. This doctrine provides for a state to exercise jurisdiction outside its physical location [49]. For identity crime, this could enable a state to bring an action against an offender in another state, provided it could be ascertained that an effect of the actions of such an offender caused a crime to be committed within the domestic territory [50].

Another challenge in regulating identity crime is that, the responses to this crime are dealt with by domestic laws and therefore the responsibility for investigation and enforcement belong to the state concerned [51]. This brings into question the domestic authority's capacity to deal with such crime which may be influenced by the scarcity of resources that exist for law enforcement [52]. A consequence of this is that, important technical, social and legal information pertaining to that crime are often not shared [53]. However, regulatory responses are not the only way in which this crime can be dealt with and these will be further explored in the outline of responses to identity crime that follow.

4 THE RESPONSES TO IDENTITY CRIME

4.1 Regulatory responses

A number of developments internationally will positively influence the regulatory response to identity crime. An important recent development is the Council of Europe Convention on Cybercrime which is an international agreement supporting and enhancing the investigation and enforcement of domestic law relating to cyber-crime internationally [54]. The importance of this convention for identity crime resides in the enhancements that can be made in the facilitation and cooperation of law enforcement efforts toward cyber-crimes on the Internet [54]. Signatories to such Conventions typically improve their interrelations with other countries specifically in terms of investigation and cooperation efforts [55]. While this Convention does not specifically mention identity crime it nonetheless will impact on this crime through the enhancements in cooperation of law enforcement efforts around cyber-crimes [55].

Jurisdictions are boundaries that are problematical when applied to the Internet [56]. However, the Convention on Cybercrime has received attention because it prompts cooperation and reliance on domestic laws in dealing with jurisdictional issues around cybercrime [57]. This has a positive influence on the way cyber-crimes are dealt with domestically [58]. Australia is working toward accepting this convention [59].

4.2 Technological responses

This paper has not sought to provide an exhaustive coverage of any specific responses to identity crime but rather it traverses the key responses that have been identified in the literature. In relation to technological responses, authentication provides an important way of identifying an individual [33] with whom one conducts transactions with on the Internet [60]. Another technological response that is helpful in preventing the unauthorized interception of data is encryption [61]. However these technological responses remain susceptible to the more sophisticated forms of attack [61]. Another weakness of such responses is the human beings involved with dealing with such measures [62].

Authentication is an important response to identity crime because this crime involves the assumption of another identity and authentication aims to prevent such actions [63]. Therefore, this technological response facilitates the security around the ascertainment of identity [33]. This is an important response in dealing with identity crime because it has a focus on preventing the assumption of identity which is a key aspect of this crime.

Encryption is a technological solution that protects data transfer when information is exchanged on the Internet [61] Encryption provides a protective measure in relation to data that are transferred between computers connected together [64]. Therefore this response plays an important role in the prevention of identity crime through enhancing data security [65].

4.3 Education as a response

There seems to be a lack of appreciation of the vulnerabilities arising from identity crime. Individuals have become the focus of this crime because they are the easier target [66]. Furthermore, individuals are becoming the more common target due to their lack of knowledge regarding identity crime [67]. It has been suggested that a key weakness in cyber security is the human and computer interface [68]. Indeed, there are behavioral factors that influence the way in which individuals exchange information across the Internet [69]. Therefore it is important to understand this relationship and to work on enhancing knowledge with respect to the vulnerabilities arising from this crime [67]. However, the educative process cannot be focused at the organisation or institution and rather needs to be focus also on the individual [70].

The computer and human interface is important in understanding cyber-crimes. While the computer can have robust methods of security, the human has become the weak link in the overall security in place to prevent cybercrime [71]. The human aspect of this interface means that humans are now the target due to their vulnerabilities [68]. It is for this reason that educative responses to identity crime need to be expansive.

The discussion of responses to identity crime aims to identify the more prominent responses to this crime and is far from exhaustive. There are additional responses such as governmental and organizational responses that have not been discussed in this paper [72]. However, this presents opportunities for further research.

5 CONCLUSION

In reflecting back on the title of this paper, it is clear that there are challenges in responding to identity crime. The responses listed cannot work in isolation to be effective. All responses to this crime rely on data relating to it. Then there are the issues pertaining to jurisdiction. Interestingly, the issues of data and jurisdiction remain closely intertwined. The lack of data relating to identity crime has a stifling effect on the response to this crime. The catalyst for change in relation to responding to this crime will need to come from improvements in the reporting of the crime, which will then prompt more work in resolving the jurisdictional issues. In the absence of this, the true incidence of identity crime will remain concealed and jurisdictional boundaries will continue to present barriers in responding to this crime.

6 REFERENCES

1. Forester, T., Morrison, P.: *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press, Boston MA (1994).
2. Saunders, K., Zucker, B.: Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act., *Cornell Journal of Law and Public Policy* 8, 661-666 (1999).
3. Office of the Australian Information Commissioner, http://www.oaic.gov.au/publications/reports/audits/document_verification_service_audit_report.html.
4. Australian Federal Police, http://www.afp.gov.au/policing/fraud/identity-crime.aspx.
5. Public Interest Advocacy Centre, http://www.travel-net.com/~piacca/IDTHEFT.pdf.
6. Department of Justice, http://www.cops.usdoj.gov/files/ric/Publications/e05042360.txt.
7. Anderson, K.: Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy and Marketing* 25, 160-171 (2006).
8. Australian Competition and Consumer Commission, http://www.accc.gov.au/content/item.phtml?itemId=816453&nodeId=ef518e04976145ffed4b13dd0ecda1a6&fn=Little%20Black%20Book%20of%20Scams.pdf.
9. Wei, R.: Lifestyles and New Media: Adoption and Use of Wireless Communication Technologies in China. *New Media & Society* 8, 991-1008 (2006).
10. State of New Jersey Commission of Investigation and Attorney-General of New Jersey, http://csrc.nist.gov/publications/secpubs/computer.pdf.
11. Public Interest Advocacy Centre, http://www.travel-net.com/~piacca/IDTHEFT.pdf.
12. Organisation for Economic Development, http://www.oecd.org/dataoecd/35/24/4064.
13. Quirk, P., Forder, J: *Electronic Commerce and the Law*. John Wiley & Sons Australia, Ltd, Milton, Qld (2003).

14. Australian Office of the Australian Information Commissioner, http://www.privacy.gov.au/faq/smallbusiness/q2.
15. Bossler, A., Holt, T.: The effect of self-control on victimization in the Cyberworld. *Journal of Criminal Justice* 38, 227–236 (2010).
16. PCWorld, http://www.docstoc.com/docs/51221743/PC-World-September-2010.
17. Social Security Administration, http://www.ssa.gov/pubs/10064.html/.
18. Australian Government, http://www.cybersmart.gov.au/Schools/Common%20cybersafety%20issues/Protecting%20personal%20information.aspx.
19. State of New Jersey Commission of Investigation and the Attorney General of New Jersey, http://csrc.nist.gov/publications/secpubs/computer.pdf.
20. Queensland Police Fraud Investigative Group, http://www.police.qld.gov.au/Resources/Internet/services/reportsPublications/documents/page27.pdf.
21. Australian Institute of criminology, http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi382.aspx.
22. Grabosky, P., Smith, R., Dempsey, G.: *Electronic theft: unlawful acquisition in cyberspace*. Cambridge: Cambridge University Press, United Kingdom (2001).
23. Australian Bureau of Statistics, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/65767D57E11FC149CA2579E40012057F?opendocument.
24. Lynch, J.: Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal* 20, 266-67 (2005).
25. Home Office Identity Fraud Steering Committee, http://www.identitytheft.org.uk/faqs.asp.
26. Willox, N., Regan, T.: Identity fraud: Providing a solution. *Journal of Economic Crime Management* 1, 1-15 (2002).
27. Australian Bureau of Statistics, http://www.ausstats.abs.gov.au/Ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf.
28. National Consumer Council, http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.
29. Black, P.:Phish to fry: responding to the phishing problem. *Journal of Law and Information Science* 73, 73-91 (2005).
30. Jarvenpaa, S., Tractinsky, N., Vitale, M.: Consumer Trust in an Internet Store: Across-Cultural Validation. *Journal of Computer Mediated Communication* 5. 45-71 (1999).
31. Parliamentary Joint Committee on the Australian Crime Commission, http://www.parliament.wa.gov.au/intranet/libpages.nsf/WebFiles/Hot+topics+-+organised+crime+cttee+rept/$FILE/hot+topics+-+Aust+Crime+Commiss+cttee+rept.pdf.
32. Sullivan, R.: Payments Fraud and Identity Theft? *Economic Review* 3, 36-37 (2008).
33. Morrison, R.: Commentary: Multi-Factor Identification and Authentication. *Information Systems Management* 24, 331-332 (2007).
34. Baker, R.: An Analysis of Fraud on the Internet. *Internet Research: Electronic Networking Applications and Policy* 9, 348-360 (1999).
35. Felson, M.: *Crime and Everyday Life, Insight and Implications for Society*. Sage, Thousand Oaks, CA (1994).
36. Organisation for Economic Co-operation and Development, http://www.oecd.org/dataoecd/49/39/40879136.pdf.
37. Australian Institute of Criminology, http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi382.aspx.
38. United States Department of Justice, http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.
39. Organisation for Economic Cooperation and Development, http://www.oecd.org/dataoecd/49/39/40879136.pdf.
40. Smith, R.: Examining Legislative and Regulatory Controls on Identity Fraud in Australia. In: *Proc. 2002 Marcus Evans Conferences*, pp.7-12, Sydney (2002).
41. Towell, E., Westphal, H.: *Investigating the future of Internet regulation* 8, 26-31 (1998).
42. 18 U.S.C. 1028A (2004).
43. *Commonwealth Criminal Code 1995* (Cth) Div 372 (1)(b).
44. *Queensland Criminal Code 1899* (Qld) s 408D(7).
45. *Criminal Code Compilation Act* 1913 (WA) s 490(1)(a).
46. *Criminal Code Act 2009* (NT) s 276(1)(a).

47. Coppel, J.: A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law. *Leiden Journal of International Law* 6, 73-90 (1993).
48. *United States v. Aluminum Co. of America*, 148 F.2d 416, 444 (2d Cir. 1945).
49. *Hartford Fire Insurance Co. v. California*, 113 S. Ct. 2891 (1993)
50. *Gencor Ltd v. Commission* [1999] ECR II-753 at paras. 89-92.
51. Svantesson, S.: Jurisdictional Issues in Cyberspace: At the Crossroads — The Proposed Hague Convention and the Future of Internet Defamation. *Computer Law & Security Report* 18, 191 - 196 (2002).
52. Bolton, R., Hand, D.: Statistical Fraud Detection: A Review. *Statistical Science* 17, 235-255 (2002).
53. United Nations Office on Drugs and Crime, http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.
54. European Convention on Cyber Crime, opened for Signature 23 November 2001, CETS No. 185, art 185 (Entered into force 1 July 2004).
55. Attorney-General for Australia, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
56. Fitzgerald, B.: Fitzgerald, A.: Beale, T.: Lim, Y.: Middleton, G.: *Internet and E-Commerce Law – Technology Law and Policy*. Law Book Co, Pyrmont, NSW (2007).
57. Parliament of Australia, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4575.
58. Australian Government Information Management Office, http://www.finance.gov.au/publications/future-challenges-for-egovernment/docs/AGIMO-FC-no14.pdf>.
59. Australian Government, http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/(8AB0BDE05570AAD0EF9C283AA8F533E3)~TSLB+-+LSD+-+FINAL+APPROVED+public+consultation+paper+-+cybercrime+convention+-+15+February+2011.pdf/$file/TSLB+-+LSD+-+FINAL+APPROVED+public+consultation+paper+-+cybercrime+convention+-+15+February+2011.pdf.
60. O'Farrell, N., Outllet, E., Outllet, E.: *Hack Proofing your wireless network*. Syngress Publishing, Rockland, MA (2002).
61. Broadhurst, R., Grabosky, P.: Computer-related Crime in Asia: Emergent Issues. In: Broadhurst, R., Grabosky, P. (eds) *Cyber-Crime: The Challenge in Asia*, Hong Kong University Press, pp.1-26. (2005).
62. Sullivan, R,: Can Smart Cards Reduce Payments Fraud and Identity Fraud. *Economic Review* 3 (2008).
63. Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, http://www.scag.gov.au/lawlink/SCAG/ll_scag.nsf/vwFiles/MCLOC_MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf/$file/MCLOC_MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf.
64. Broadhurst, R.: Grabosky, P.: Computer-related Crime in Asia: Emergent Issues. In: Broadhurst, R., Grabosky, P. (eds.) Cyber-Crime: The Challenge in Asia, pp 15-17. Hong Kong University Press (2005).
65. Ferguson, N.: Schneier, B.: *Practical Cryptography* (Wiley, New York, NY (2003).
66. Australian Institute of Criminology, http://www.aic.gov.au/documents/9/3/6/%7B936C8901-37B3-4175-B3EE-97EF27103D69%7Drpp78.pdf.
67. Community for Information Technology Leaders, http://www.cioupdate.com/technology-trends/cios-cybercrime-and-wetware.html.
68. Symantec, http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.
69. Stajano, F.: Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM* 44, 70 (2011).
70. Bard Prison Initiative, http://www.stcloudstate.edu/continuingstudies/distance/documents/EducationasCrimePreventionTheCaseForReinstatingthePellGrantforOffendersKarpowitzandKenner.pdf.
71. Federal Reserve Bank of Kansas City, http://www.kansascityfed.org/PUBLICAT/econrev/pdf/3q08sullivan.pdf.
72. Benson, M.: Offenders or Opportunities: Approaches to Controlling Identity Theft. *Criminology & Public Policy* 8, 231–236 (2009).