Social Networking and Identity Theft in the Digital Society

Eric Holm
Federation University Australia
PhD student, Bond University,
Mount Helen, Australia
e.holm@federation.edu.au

***Abstract* - This paper explores the vulnerability of social network users to identity theft facilitated by the information they share on social networking sites. While social networking presents new possibilities for friendships and the sharing of interests, at the same time it brings vulnerability through the outflow of personal information online. Identity criminals can exploit the weaknesses of social network users and social networking sites, effectively enabling the identity criminal to construct an identity from the information they obtain. The information gathered by an identity criminal can be used to establish identity, a powerful precursor to committing identity fraud. While there are preventative mechanisms that can reduce the incidence of this crime, information sharing on social networks is common and voluntary, which makes it difficult to control. While this paper presents an evaluation of existing work, further empirical research work is needed to understand the vulnerability of personal information on social networking sites. Social networking sites have a vested interest in promoting rather than preventing the sharing of information. In addition, identity crime is pervasive, which makes the amelioration of the risks difficult. In concluding this paper, efforts are made to point toward starting points that will assist in resolving this crime.**

Keywords- social networking; identity theft; identity fraud.

I. INTRODUCTION

Social networking has inspired computer users to share information online. Social networking sites bring together people with common interests and enable mass social interaction to take place. This overcomes geographical constraints and can bring together disparate groups [1]. Social networking is attractive due to its social inclusiveness [2] as well as its interactive nature [3]. For example, 500 million people have used Facebook to create profiles to express themselves across this social networking platform [4]. The social linkages created by such sites bring together new social associations as well as new ways to interact online including instant communication and gaming [4]. In this regard, there have been many narratives about both the positive and negative social implications and influences of this social interaction [5]. Criminal activity has been a negative implication of such interaction and this one seemingly harmless type of human interaction has lent itself to another that is far more sinister: identity crime.

This paper will first consider why the identity crime is serious in the context of the strong uptake of social networking which has been mentioned. The paper will then discuss the responses to dealing with identity crime and social networking that include deliberating the suitability of criminal law and privacy responses to this crime. Thereafter, the paper will discuss the challenges in dealing with identity crime and social networking. Finally, the paper will provide some recommendations arising from this paper and foreshadow future work.

II. THE EMERGING ROLE OF SOCIAL NETWORKING IN INFORMATION SHARING

The extent to which individuals share information on a social networking site is determined by the decisions they make which are influenced by many drivers. The control mechanism used on a social networking site is typically the user privacy settings, which allow an individual to determine the visibility of their social networking profile to others. A social networking profile is the mode in which social networking users represent themselves online and facilitates their existence on the social networking site. The dissemination of information is at the heart of social networking [6]. The opportunity to share information is attractive to users who aspire in particular, to share their emotions, expressions and experiences online [7]. A key driver for social networking sites is the reciprocal nature of such information sharing [8]. Social networking sites finely balance the security needs of user with the ease of use and much of the research around changing the architecture of the interface has been previously explored [9]. Such sharing of information provides the foundation under which many relationships are formed [10] as well as the basis for rekindling relationships with old friends [11]. In addition, many social networking sites also contain incentives for such information sharing to take place whether by promoting the creation of these friendships, sharing general interests or religious beliefs, and numerous other motivators [8]. Many positive outcomes can be derived from social networking.

Social networks have become an alternative to communication in many traditional social contexts [12]. Increasingly communication takes place online and social networking has become a platform that functions in place of (or in conjunction with) existing social contexts. However, social networking is a relatively new phenomenon and many of the social conventions around it are still developing [13]. It may be for this reason that many users are complacent about the potential risks associated with the sharing of personal information on this platform. Studies related to information sharing suggest that gender also influences the preparedness of users to share information, with boys and men being prepared to share information online more freely than girls and women [14]. Furthermore, younger men are seemingly more prepared to share information than older men [15] and it may be that factors like peer pressure play a role in this. Nonetheless, there seems to be complacency in relation to the risks associated with information sharing on social networking sites. Many users share information about themselves that includes their full names, their location, date of birth and also photographs [10]. This can be the information required by identity criminals to form an identity that can be used to perpetrate crime.

When information is acquired by an identity criminal, in most instances it is taken without the knowledge or consent of the victim [16]. In this sense, the victim might not be aware that their information has been stolen until they find themselves exposed to crime-related financial liability. Hence, the motivation for the identity criminal is typically monetary gain [17]. Such crime involves the collection of the information required to replicate the identity of the victim [18]. Once stolen, the identity criminal will typically use the name of the victim to commit fraud: identity fraud [19]. Information taken from a social networking site can be used to establish a false identity. The documents needed to establish identity vary, but most governments accept a range of identification documents to establish it [20]. By world standards, name, gender, nationality and date of birth are considered unique personal identifiers that collectively satisfy identity requirements [21]. Indeed, many of these details are commonly shared on social networking sites. When this information is used, many victims will not know that they have become victims until some considerable time has passed [22]. The time between when an identity crime occurs and an investigation takes place makes it difficult to gather evidence of the crime and to both locate and prosecute the offender [22]. During this time, the victim withstands the frustration of financial losses caused by such crime and research has shown that this frustration worsens the longer it takes for the situation to be resolved [23]. The subversive nature of this this crime ultimately adds to a victim's frustration.

III. WHY IS THIS CRIME SERIOUS?

Identity crime has the potential to reach anyone. Research conducted at Carnegie Melon University suggests that children 15-18 years of age (43%) are the age group most likely to be victimized by identity criminals. Of the other age groups, children aged 11-14 years (28%), 6-10 years (19%) and five years and under make up the balance of victims [24]. However, at the same time, it is evident that children of working age are at risk due to their levels of income as well as their relevant engagement with technology [25]. Overall, these victims present fruitful targets to identity criminals. While it is not clear what the reasons for this might be, it is probable that the risk of victimisation is linked to increased levels of engagement with technology [26]. Inadequate levels of supervision of children's Internet usage, particularly with respect to social networking may also contribute to this [27]. Children have a particular vulnerability to identity theft crime as they usually possess an unblemished personal history and remain relatively undefended as targets of this crime [24]. This increases their status as prime targets of identity criminals. In addition, children often unknowingly share information about themselves that can place them at risk [28]. From these indicators of victimisation, it becomes clear that identity fraudsters are opportunistic when it comes to the perpetration of this crime and anyone can become a victim.

In the United States in 2009, an estimated 11 million Americans had been the victims of identity crime [20]. In 2010, 7% of households in the United States experienced identity theft victimization, [29] amounting to about 8.6 million households [29]. Similarly, in 2010-2011 the estimated cost of personal fraud to Australians was $1.4 billion [30] with approximately 44,700 Australians becoming victims of identity crime [31]. Statistics from the United Kingdom similarly suggest that identity crime is increasing prodigiously with the reported number of cases almost doubling between 2007 and 2012 from 77,500 to 123,600 [32]. These statistics suggest that identity crime is global and significant in terms of both its impact and cost.

The cost of identity crime is often regarded as being comprised of both direct and indirect costs. The most significant cost of identity crime is the financial cost [33]. However, the true cost of identity crime extends beyond financial loss [34]. These have been referred to as the difference between direct and indirect costs or hard and soft costs [34]. The financial costs (the hard costs) are easily quantified whereas the non-financial costs (soft costs) are more difficult to quantify as they relate to the cost of preventative measures as well as damage to reputation [34]. The cumulative losses reflect both the hard and soft costs of identity fraud crime. Obtaining accurate measures of the true cost is also influenced by the lack of data available on this crime [34]. The banking sector suffers significant losses in relation to identity crime [35] but its spokespersons remain reluctant to disclose the losses arising from this crime. Interestingly, bank losses in the United States have been estimated to amount to over $2 billion per year [36]. However, the banking sector prefers not to report these losses due to the commercial sensitivities they perceive them [37]. This contributes towards the difficulty in establishing measures on the true cost of identity crime. The key issue this raises relates to the strength of responses which remain linked to the commensurate strength of that response [38].

Ultimately, there are costs related to identity crime, which are more easily identified, and those that are not, many of which are not considered in connection with one another.

IV. DEALING WITH IDENTITY CRIME AND SOCIAL NETWORKING

There are many practical difficulties in convicting identity criminals [39]. In the first place, in an international context, no central body is responsible for overseeing crime committed via the Internet or where on the Internet this crime might occur. Identifying and controlling crime perpetrated through social networking sites is fraught with difficulties [40]. The Internet is a dispersed communication entity that permeates country boundaries thereby making regulatory responses to crime difficult [40]. Further, different values influence the way in which crimes are viewed. Interpol increasingly plays a role in dealing with cybercrimes like identity crime by having a programme to deal with the emerging threats in this realm [41]. The Council of Europe Cybercrime Convention aims to harmonise the regulation of cyber-crimes [41]. It provides domestic criminal law authorities with the necessary cooperative mechanisms to investigate and prosecute computer crimes [41]. However, like most international instruments, crimes require attention through domestic laws [42]. Success will therefore be dependent on the stance maintained by each country in question.

The term ‘cybercrime’ has been used to describe crimes in which the computer or computer network is typically the target. This crime is distinguishable from other traditional crimes as it is limited to where the computer is used in the crime [43]. This thereby includes frauds in which the computer is used as a tool to commit the crime [43]. Likewise, if identity crime takes place through the use of a computer it is arguably included within the scope of the convention. However, the European Convention fails to deal directly with identity crime [44]. It captures computer-related forgery (article 7) as well as computer-related fraud (article 8) and thereby by association it would apply to related offences [45]. The significance of this is that the abovementioned convention would assist in the investigation and enforcement of identity crime despite not making reference to it [46]. In a global sense, unfortunately, there is nothing simple about applying criminal sanctions to international crimes like identity crime, particularly when they fall outside globally acknowledged atrocities such as genocide. Even so, the effectiveness of such responses is reliant on the preparedness of countries to agree and cooperate on responses to crime.

V. PRIVACY PERSPECTIVE

International responses to privacy share some of the challenges with the international regulation of crime. There is a lack of supremacy and centrality when it comes to the regulation of privacy internationally [46]. Akin to crime, domestic laws which are often based on international agreements are similarly relied upon to regulate privacy [47]. International principles of privacy protection are provided for in international agreements like the Universal Declaration of Human Rights [48]. These international agreements recognise the protection of the inalienable rights of all humans to privacy [48], highlighting the need for them to enjoy freedom of speech and belief [48]. Further, Article 12 suggests that no one should be subjected to interference with respect to their privacy [48]. Such international agreements have provided the foundation for the development of domestic laws [47]. Australia has been a member of the United Nations since 1945 [48] and has thereby developed such laws domestically. This can be seen in the Commonwealth Privacy Act, which provides for how information is collected, used and disclosed within Australia [49]. However, a limitation of the domestic privacy response in Australia is that it is not prescriptive and rather offers guidelines on the use of personal information. Further, it is constrained by the same jurisdictional boundaries that limit the extraterritorial reach of criminal sanctions explained above [50]. These are barriers to resolving the privacy-related issues of identity crime arising through the use of social networking.

VI. CHALLENGES IN DEALING WITH THE SOCIAL NETWORKING NEXUS WITH IDENTITY CRIME

A major challenge in responding to identity crime is the ability of law enforcement agencies to obtain evidence for the prosecution of this crime. The gathering of evidence on this crime involves obtaining digital evidence both on and off line [49]. It is essential for such investigative efforts across geographic borders to be effective as so much of crime such as identity crime takes place using the Internet, particularly due to the way in data are disseminated on social networking sites. The speed with which data transference takes place on the Internet makes the investigation of identity crimes difficult as the data possessed or used by a criminal can be destroyed or manipulated just as quickly [51]. Furthermore, as identity crime is cross jurisdictional then cooperation between law enforcement authorities is essential [52]. Any successful effort to investigate and enforce identity crime is reliant on the cooperation of countries [52] and the success of such efforts will also be dependent on the speed of such a response. In relation to civil responses to identity crime, there are similarly many barriers on the ability of the individual to successfully take civil action against the criminal as individuals have a greater scarcity of resources to successfully pursue such action. Similar issues around detecting and locating the offender exist for these actions also.

A key weakness in the integrity of data is the way in which individual users manage their own information. Users need to accept the need for greater accountability for the information shared on social networking sites. Each activity we engage in results in users leaving traces of themselves like digital footprints. Therefore, a commonsense response to dealing with the exploitation of social networking by identity criminals is for social networking users to improve their level of education about the relevant issues [49]. An educational program is necessary to ensure social networking users are both aware of the risks and of the need to exercise caution with respect to their personal information [53]. Moreover, in relation to the second point, this should take into account the ways in which, information might potentially be misused by identity criminals [54]. While education could have a direct impact on crime reduction [55] there will always typically be a proportion of the population not responsive to such efforts. The role of education is therefore not exhaustive but still should be regarded as another way of dealing with this crime. Social networking sites themselves should accept some responsibility in the protection of the user by encouraging the tacit sharing of personal information in some instances. This should be broader than the general technological security measures in place and needs to include the architecture underpinning the sites use [56]. This should involve reconsidering the ways in which, information sharing takes place on such sites and consideration of the architecture that facilitates this. Identity crime can be reduced through better understanding of and mitigation of these risks [57].

A number of additional and general technical responses can be applied to prevent identity crimes. The responses include improved measures of authentication and encryption, but are not limited to these [58]. The aim of such technological responses is to ensure data integrity is maintained while correspondingly preventing unwanted misuse of information or intrusion [59]. However, as with most responses, such efforts have vulnerabilities by way of the advancements criminals make to overcome them [59]. The strength of the responses to identity crime often needs to be balanced against the perceived costs of such preventative action [60]. Nevertheless, these responses provide additional ways of dealing with information security and thereby provide another way in which, identity crime can be responded to.

VII. Discussion

Ultimately, policymakers should consider a multi-faceted approach for dealing with identity crimes [61]. A mixture of techniques is necessary for counteracting the threats of this crime as the crime is ubiquitous response [62]. There are limitations with any approach to dealing with this crime, some of which have been discussed in this paper. The relationship of social networking and identity crime is unique and thereby requires creative responses. A major obstacle to responding to social networking and identity crime is the availability of accurate data relating to this relationship. While not all conceivable approaches to dealing with this phenomenon have been canvassed in this paper, the ones that have provide some insight into the many issues presented by this crime as well as some view of the plausible ways forward.

The information that is disseminated through the use of social networking is the key catalyst to identity crime which is largely based on the actions of individual users. The motivation for this research has been to explore the relationship between identity crime and social networking which has scarcely been explored in existing literature and to establish a basis upon which further research might take place. Further empirical research is needed to further probe the parameters of this relationship. It is hoped that through raising awareness of this relationship that further research interest is generated and that through further research, that social networking users will can take greater precautions to prevent themselves from becoming victims of this crime.

VIII. Evaluation

The material discussed in this paper, largely from secondary sources, identifies a relationship between social networking and identity crime. To further develop the contention, empirical research is needed to explore the scope of this relationship. In terms of the responses to this phenomenon, this paper has explored a number of technological and non-technological responses which are by no means exhaustive. Further research into the relationship between social networking and identity crime is likely to provide insights into the mechanisms that might better deal with this crime.

IX. Recommendations

Information is the vehicle to identity theft and considerable information is stored on social networking sites. Law and technological responses have limitations in relation to the extent they can mitigate this crime and particularly given the voluntary nature of information dissemination and the issues around jurisdiction and cooperation discussed. The individual vulnerability to this crime is through personal identification information which ultimately means that the behavioural factors are important to understanding the crime and indeed mitigating risk. Therefore, it is hoped that through the dissemination of research and information that individuals may become better informed of the risks inherent in the activities they engage with on the Internet: particularly social networking. Individual users of social networking need to take greater responsibility for the personal identification information shared on social networking sites to avoid victimisation. In this respect, if behavioural norms can be changed on social networking sites then the risk inherent with identity crime can be reduced.

X. Conclusion and future work

Social networking has encouraged many users to share personal information online, and social network users frequently engage in the sharing of information about themselves [9]. This article has considered the way in which social networking can potentially nourish the transference of personal information on the Internet, which in turn can provide identity criminals with the information needed to commit identity crime. While there are many ways to respond to this crime, a blend of techniques is likely to work best, given the pervasive nature of this crime and barriers presented by multiple jurisdictions. Future work is needed to explore these responses. An important starting point for dealing with this crime is to increase awareness of the risks associated with information sharing around social networking. If you have read this far, then this paper has achieved some of its educational aim: perhaps you will be more careful with your social networking profiles in the future. More research is needed to develop further knowledge about this crime and similarly more research is needed to understand the data surrounding identity crime and the nexus of this to the responses to it.

ACKNOWLEDGMENT

I would like to thank the support of The Business School at Federation University Australia (formerly University of Ballarat) which provided the assistance needed to prepare this article and Dr Ian Dobson for editorial support. I would also like to acknowledge the support of the institution I have studied in Australia and my research supervisors at Bond University.

REFERENCES

[1] J. B. Walther and S. Boyd, “Attraction to computer-mediated social support,” in Communication Technology and Society: Audience Adoption and Uses, C. A. Lin and D. Atkin, Eds. Cresskill: Hampton Press, 2002, pp. 153-88.

[2] J. Bargh and K. McKenna. “The Internet and Social Life,” Annual Review of Psychology, vol. 55, Feb. 2004, pp. 573-590, doi:10.1089/cpb.2005.8.423.

[3] I. Berson, M. Berson, and J. Ferron, “Emerging risks of violence in the digital age: Lessons for educators from an online study of adolescent girls in the United States,” Journal of School Violence, vol. 1, Jan. 2002, pp. 51-71.

[4] P. Valkenburg and J. Peter, “Internet communication and its relation to well-being: Identifying some underlying mechanisms,” Media Psychology, vol. 9, Dec. 2007, pp.23-58, doi:10.1080/15213260709336802.

[5] M.Green and T. Brock, “Antecedents and civic consequences of choosing real versus ersatz social activities,” Media Psychology, vol. 11, Dec. 2008, pp. 566–592, doi:10.1080/15213260802491994.

[6] J. Fogel and E. Nehmad, “Internet social network communities: Risk taking, trust, and privacy concerns,”Computers in Human Behavior, vol. 25, Jan. 2009, pp. 153–160, doi>10.1016/j.chb.2008.08.006.

[7] F. Stajano and P. Wilson, “Understanding Scam Victims: Seven Principles for Systems Security,” Communications of the ACM, vol. 54, Mar. 2011, pp. 70, doi :10.1145/1897852.1897872.

[8] A. Ledbetter, J. Mazer, J. DeGroot, K. Meyer, Y. Mao, and B. Swafford, “Attitudes toward online social connection and self-disclosure as predictors of Facebook communication and relational closeness,” Communication Research, vol. 38, Feb. 2011, pp. 27–53, doi: 10.1177/0093650210365537.

[9] M. Lucas and N. Borrisov, “flyByNight: Mitigating the Privacy Risks of Social Netowrking,” Proc. of the 7th ACM workshop on Privacy in the electronic society (WPES ’08), ACM, Oct. 2008, pp. 1-8, doi>10.1145/1456403.1456405

[10] S. Hindujaa and J. Patchin, “Personal information of adolescents on the Internet: A quantitative content analysis of MySpace,” Journal of Adolescence, vol. 31, Jan. 2008, pp. 125-146, doi:10.1016/j.adolescence.2007.05.004.

[11] N. Ellison, C. Steinfield, C, and Lampe. C, “Benefits of Facebook “friends:” Social capital and college students’ use of online social network sites,” Journal of Computer-Mediated Communication, vol. 12, Aug. 2007, pp.1143-1168, doi: 10.1111/j.1083-6101.2007.00367.x.

[12] Y. Yum and K. Hara, “Computer-mediated relationship development: A cross-cultural comparison,” Journal of Computer-Mediated Communication, vol. 11, Aug. 2006, pp. 133–152, doi: 10.1111/j.1083-6101.2006.tb00307.x.

[13] P. Van Eecke and M. Truyens, “Privacy and social networks,” Computer Law & Security Review, vol. 26, Sept. 2010, pp. 535-546, doi: http://dx.doi.org/10.1016/j.clsr.2010.07.006.

[14] H. Jelicic, D. Bobek, E. Phelps, and R. Lerner, “Using positive youth development to predict contribution and risk behaviors in early adolescence: Findings from the first two waves of the 4-H Study of Positive Youth Development,” International Journal of Behavioral Development, vol. 31, May. 2007, pp. 263–273, doi: 10.1177/0165025407076439.

[15] J. Huang, D. Jacobs, D. Derevensky, J. Gupta, R, and T. Paskus, “Gambling and health risk behaviors among US college student-athletes: Findings from a national study,” Journal of Adolescent Health, vol .40, May. 2007, pp. 390-397, doi:10.1016/j.jadohealth.2006.11.146.

[16] K. Saunders and B. Zucker, “Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act,” Cornell Journal of Law and Public Policy, vol. 8, Spring. 1999, pp.661.

[17] T. Hemphill, “Identity Theft: A Cost of Business?,” Business and Society Review, vol. 106, Dec. 2001, pp.51-63, doi:10.1111/0045-3609.00101.

[18] N. Archer, S. Sproule, Y. Yuan, K. Guo, and J. Xiang, Identity Theft and Fraud Evaluating and Managing Risk. Ottawa, Canada: University of Ottawa Press, 2012.

[19] Australian Crime Commission. (2009, November, 28). Organised Crime in Australia 2011. [Online]. Available: http://www.crimecommission.gov.au/sites/default/files/files/OCA/2011/oca2011.pdf [retrieved: January, 2011].

[20] United Kingdom Cabinet Office. (2002, February 15). Identity Fraud: A Study. [Online]. Available: http://www.statewatch.org/news/2004/may/id-fraud-report.pdf [retrieved: November, 2013].

[21] International Civil Aviation Organization. (2009, November, 9). Towards Better Practice in National Identity Management. [Online]. Available: http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-19/TagMrtd19-wp03.pdf [retrieved: October, 2013].

[22] Government of South Australian (2005, May.). Australian E-Commerce Safety Guide 2005. [Online]. Available: http://www.cbs.sa.gov.au/assets/files/EcommGuide_2005.pdf [retrieved: September, 2013].

[23] L. Langton, M. Planty, and US Department of Justice (2008, Dec.). Victims of Identity Theft, 2008 [Online]. Available: http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf [retrieved: December, 2010].

[24] Carnegie Mellon. (2011, Mar.). Child Identity Theft. 2011 [Online]. Available: http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf [retrieved: March, 2011].

[25] S. Willis and B. Tranter, "Beyond the "Digital Divide": Internet Diffusion and Inequality in Australia," Journal of Sociology, vol. 42, Mar. 2006, pp. 43-59, doi:10.1177/1440783306061352.

[26] L. Plowman, O. Stevenson, C. Stephen, and J. McPake, "Preschool children's learning with technology at home," Computers & Education, vol. 59, Aug. 2012, pp. 30-37, doi:http://dx.doi.org/10.1016/j.compedu.2011.11.014.

[27] S. Livingstone and E. Helsper, "Parental mediation and children's Internet use," Journal of Broadcasting and Electronic Media, vol. 52, Dec. 2008, pp. 581–599, DOI: 10.1080/08838150802437396.

[28] Australian Government. (2013, Feb.). Identity Theft. [Online]. Available: http://www.scamwatch.gov.au/content/index.phtml/tag/identitytheft [retrieved: March 2011].

[29] National Crime Justice Reference Service. (2013, Jan.). Identity Theft – Facts and Figures. [Online]. Available: https://www.ncjrs.gov/spotlight/identity_theft/facts.html [retrieved: October, 2013].

[30] Australian Bureau of Statistics. (2012, Apr.). Personal fraud costs Australians $1.4 billion. [Online]. Available: http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument [retrieved: April, 2012].

[31] Australian Bureau of Statistics. (2012, Apr.). Personal Fraud 2010-2011. [Online]. Available: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/65767D57E11FC149CA2579E40012057F?opendocument [retrieved: November, 2013].

[32] CIFAS. (2012, Jun.). Is Identity Fraud Serious? [Online]. Available: http://www.cifas.org.uk/is_identity_fraud_serious [retrieved: October, 2013].

[33] R. Smith. (2003, Sep.). Addressing Identity-Related Fraud. Presented at Cards Australasia. [Online]. Available: http://www.aic.gov.au/about_aic/research_programs/staff/~/media/conferences/other/smith_russell/2003-09-identity.ashx [retrieved: December, 2012].

[34] M. Perl, "It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft," Journal of Criminal Law and Criminology, vol. 94, Fall. 2003, pp.169-208.

[35] D. Lacey and S. Cuganesan, "The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic," The Journal of Consumer Affairs, vol. 38, Jul. 2004, pp 244-261, doi:10.1111/j.1745-6606.2004.tb00867.x.

[36] Kroll Advisory Solutions (2011, May.). Global Fraud Report: The Strategic Impact of Fraud, Regulation, and Compliance [Online]. Available: http://www.krollconsulting.com/media/pdfs/KRL_FraudReport2011.pdf [retrieved: December, 2013].

[37] Federal Trade Commission (2003, Sep.). Identity Theft Survey Report Federal Trade Commission [Online]. Available: http://www.ftc.gov/os/2003/09/synovatereport.pdf [retrieved: December, 2013].

[38] Pat Mayhew and Australian Institute of Criminology (2003, Apr.). Counting the Costs of Crime in Australia [Online]. Available: http://www.aic.gov.au/documents/A/A/3/%7BAA329573-5D62-46FB-9E6F-4D86A6DDD9BC%7Dti247.pdf [retrieved: November, 2013].

[39] R. Smith. (2002, Jul.). Examining the Legislative and Regulatory Controls on Identity Fraud in Australia [Online]. Available: http://www.aic.gov.au/media_library/conferences/other/smith_russell/2002-07-fraud.pdf [retrieved: November, 2012].

[40] B. Fitzgerald, A. Fitzgerald, T. Beale, Y. Lim, and G. Middleton, Internet and C-Commerce Law: Technology, Law and Policy. Pyrmont: Lawbook Co, 2007.

[41] Interpol (2014, Jan.). Interpold [Online]. Available: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [retrieved: Jan, 2014].

[42] S. Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," Murdoch University Electronic Journal of Law, vol. 8, Jun. 2001, pp. 1.

[43] J. Clough, "The Council of Europe Convention on Cybercrime: Defining 'Crime' in a digital world," Criminal Law Forum, vol. 23, Dec. 2012, pp. 363-391, doi:10.1007/s10609-012-9183-3.

[44] M. Gercke and Council of Europe. (2007, Nov.). Internet-Related Identity Theft Discussion Paper. [Online]. Available: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf [retrieved: January, 2014].

[45] Council of Europe. (2011, Jul.). Convention on Cybercrime: Member States of the Council of Europe – Article 12 [Online]. Available: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [retrieved: January, 2014].

[46] K. Grewlich, Governance in 'Cyberspace' Access and Public Interest in Global Communications, Boston, USA: Klewer Law International, 1999.

[47] International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

[48] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948).

[49] Australian Government: Office of the Australian Information Commissioner. (2007, Aug.). Scanning "Proof of Identity" Documents [Online]. Available: http://www.privacy.gov.au/materials/types/infosheets/view/6553 [retrieved: December, 2013].

[50] P. Argy, "Internet Content Regulation: an Australian Computer Society Perspective," University of New South Wales Law Journal, vol. 23, Jul. 2000, pp. 265-267.

[51] C. Blakesley, "United States Jurisdiction over Extraterritorial Crime," The Journal of Criminal Law and Criminology, vol. 73, Jan. 1982, pp.1109.

[52] A. Cassese, International Law. Kansas, USA: Oxford University Press, 2001.

[53] Organisation for Economic Co-operation and Development. (2008, Jun.). OECD Policy Guidance on Online Identity Theft [Online]. Available: http://www.oecd.org/dataoecd/49/39/40879136.pdf [retrieved: October, 2013].

[54] M. Harer and Federal Bureau of Prisons. (1994, Aug.). Recidivism among Federal Prisoners Released in 1987 [Online]. Available: http://149.101.37.70/news/research_projects/published_reports/recidivism/oreprrecid87.pdf [retrieved: October, 2013].

[55] Parliament of Australia - House of Representatives Standing Committee on Communication (2010, Jun.). Chapter 6: Criminal and Law Enforcement Framework [Online]. Available: http://parlinfo.aph.gov.au/parlInfo/search/summary/summary.w3p;adv=yes;orderBy=customrank;page=0;resCount=Default;query=Criminal+and+Law+Enforcement+Framework [retrieved: April, 2013].

[56] B. Schneier, Secrets and Lies: Digital Security in a Networked World. New York, USA: John Wiley, 2000.

[57] L. Lessig, Code and Other Laws of Cyberspace. Virginia, USA: Basic Books, 1999.

[58] J. Lynch, “Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks,” Berkeley Technology Law Journal, vol. 20, Jan. 2005, pp. 266-67.

[59] R. Sullivan, “Can Smart Cards Reduce Payments Fraud and Identity Fraud,” Economic Review, vol. 93, 2008, pp. 36-62.

[60] N. Phair, Cybercrime: the Reality of the Threat. Kambah, ACT: E-Security Publishing, 2007.

[61] G. Newman, “Policy Thoughts on “Bounded Rationality of Identity Thieves,”’ Criminology & Public Policy, vol. 271, Jun. 2009, pp.271-278, doi: 10.1111/j.1745-9133.2009.00562.x.

[62] R. G. Broadhurst and P. N. Grabosky, “Computer-Related Crime in Asia: Emergent Issues,” in Cyber-Crime: The Challenge in Asia, R. G. Broadhurst and P. N. Grabosky. Eds. Hong Kong: Hong Kong University Press, 2005, p 1.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7