1-1-2014

Social networking and identity theft in the digital society

Eric Holm
Bond University, eric.holm@student.bond.edu.au

Social Networking, the Catalyst for Identity Thefts in the Digital Society

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

***Abstract* - This paper explores the vulnerability of social network users to identity theft when they share personal identification information online. The sharing of details like age, sex, address and other personal information like photographs can assist in establishing an identity. Identity criminals exploit social network users and the weaknesses of social networking sites to gather the information needed to commit identity theft and identity fraud using this identification information. While there are mechanisms that can reduce the incidence of this crime, information sharing on social networks is voluntary, which, makes its control difficult. This paper presents an exploration of existing literature from Australia, the United States and United Kingdom and highlights the importance of the relationship between social networking and identity crime. The drivers to sharing information on these platforms are considered. The paper provides opportunities to improve the understanding of the relationship between personal information and the crime. A difficulty in having preventative mechanisms in place is that social networking sites have a vested interest in promoting rather than preventing the sharing of information. Further, identity crime is pervasive which, makes the amelioration of risks difficult. In conclusion, efforts have been made in this paper to outline arguments that will assist in resolving the crime given vulnerability of social network users to identity theft.**

Keywords- social networking, privacy, 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 they enable mass social interaction [1]. This mechanism of communication overcomes geographical constraints and can bring together disparate groups [2]. Social networking is attractive due to its social inclusiveness [3] as well as its interactive nature [4]. For example, over 500 million people have used Facebook to create profiles to express themselves across this social networking platform [5]. Facebook is the most popular social networking site, followed by Myspace according to college students in the United States [6]. The social linkages these platforms create are particularly attractive to these users [7]. Many of the new innovative forms of communication are accompanied by new ways of accepting and exploiting this interaction. Acceptance of these new ways of interaction expands social connections between people, but this communication can be exploited, leading to something far more sinister: identity crimes.

This paper considers why identity crime is serious in the context of the strong uptake of social networking. The basis of the discussion is around literature obtained from the United States, United Kingdom and Australia. The paper then discusses the responses to identity crime in social networking including the suitability of criminal law and privacy responses to this crime. Thereafter the paper discusses the international dimensions to dealing with identity crime in social networking and provides some recommendations and foreshadows future work.

II. RELATED WORK

The extent that individuals share information on a social networking site is determined by the decisions they make and are influenced by many behavioral drivers. The control mechanism used on social networking sites is typically the user privacy settings, which, allows an individual to determine the visibility of their profile to others. Most users tend to leave these at the default setting established by the social networking provider, which, may be less than optimal to the end user of these services in respect of privacy [8]. A social networking profile is how the social networking users represent themselves online and it facilitates their presence and disseminates information about them and this is at the heart of social networking [9]. The opportunity to share information is attractive to users who aspire in particular to share their emotions, expressions and experiences online [10]. One of the attractions of social networking sites is the reciprocal nature of such information sharing [11], but social networking sites seek to balance the security needs of user with their ease of use [12]. While the sharing of information provides the foundation under which, many relationships are formed [13] it also provides the basis for rekindling relationships with old friends [14]. In addition, many social networking sites provide incentives for promoting the creation of these friendships, sharing general interests or religious beliefs, and numerous other activities [11]. In this regard there is a vested interest for social networking site providers to encourage the sharing of information and there are many positive outcomes that can be derived from social networking [15].

Social networks have become an alternative to communication in many traditional social contexts [15]. 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 [8] and it may be for this reason that many users are complacent about the potential risks associated with sharing personal information online. For instance, accepting 'friend' requests may occur far more readily through a social networking site than it might off it [16]. Friend requests on a social networking site may appear innocuous but later become harmful particularly if granted to an identity criminal. Gender influences the preparedness of users to share information, with men being prepared to share information online more freely than women [16]. Furthermore, younger men are seemingly more prepared to share information than older men [17] and factors like peer pressure may play a role in this. Nonetheless, there seems to be complacency in relation to the risks associated with information sharing on social networking sites with many users sharing information about themselves including their full name, their location, date of birth and also photographs [13]. This information can be used by identity criminals to form an identity that they subsequently use to perpetrate crime.

The interest in social networking is profound, with the social networking site Facebook having an estimated 1.15 billion users. Platforms such as Twitter, Google plus, Myspace and LinkedIn have all attracted masses of members [18]. While user uptake in social networking sites is staggering, user engagement is equally astounding with 20 per cent of Facebook users checking their accounts numerous times per day [18], this is evidence suggesting that many users are also using different platforms to log into their chosen social networking site whether through a computer, mobile phone, tablet or an assortment of these [19]. Indeed, new technologies are facilitating an even more committed user base for social networking activity. This may contribute toward the complacency around the sharing of information.

In addition to individual users, many businesses interact on social networking sites to increase their business exposure to customers and clients [20]. They utilize the services of social networking providers to share information, advertise, promote and position themselves in the wider market and this makes them susceptible to identity crime on social networking sites in the same way as it does for individuals [20]. For corporations, the victimization from identity crime may be arising from corporate disclosure rules as this adds to the volume of information that is readily available to identity criminals [20].

In most instances, information acquired by an identity criminal is taken without the knowledge or consent of the victim [21]. The victim might not be aware that their information has been stolen until they find themselves exposed to financial liability. The usual motivation for the identity criminal is monetary gain but there may be other motivations for this crime [22]. The distinction between identity theft and fraud is important as identity theft is based on the theft of information, and identity fraud results from that theft [23]. In Australia, these crime types are distinguished through offenses that relate to the possession of identification information and offenses related to the dealing with it [24]. While both are crimes, offenses that result in financial loss are the more detrimental to the victim. Although in absence of financial loss it is still possible to suffer detriment from this crime.

Personal identification information is information that identifies a person, such as a passport, a driver's license or a bank statement [25]. However, there are other identifiers that could be regarded as personal identifying information and include demographic details including name, address or date of birth [26]. Past research has suggested that sensitive information also includes personal photographs, names and gender which, are prone to leakage on social networking sites [27]. Past research has also shown that Facebook users in particular are more prepared to reveal personal information (including their real name) on this site as well as including email addresses in their profiles [27]. While the documents needed to establish identity vary, most governments accept a range of identification documents [21] and by world standards, name, gender, date of birth and nationality are unique personal identifiers that are considered collectively to satisfy identity requirements [28]. The information stolen may be used by the identity criminal to achieve their desired outcomes of establishing identity. Once established they may use it for identity fraud or other to commit other crimes [21]. In the United States, for instance, identities have been stolen and used for perpetrating a range of criminal offences where the victims becomes wrongfully accused [21].

What is interesting in relation to the existing literature is that there is a body of literature exploring social networking as well as identity crime with little confluence between these topics. There is a real risk of identity crime through the disclosures of personal identification information on the on social networking sites. This paper aims to explore through relevant literature how social networking plays an important role as an enabler for identity crime. Identity crime is pervasive and will exploit emerging social interactions online, it is important to understand this vulnerability to better mitigate the crime.

III. METHODOLOGY

This paper is a selective literature review largely from countries including Australia, United Kingdom and the United States on issues of social networking disclosures and identity crime. The literature review is discussed from cognate areas with the view to exploring the confluence of social networking disclosure and identity crime and informing future research into this. As an emerging area of research little data presently exists on this topic and the

outlook of this paper is to bring together existing work to point toward future opportunities for research work.

IV. How the crime is committed?

An estimated 16.6 million Americans were the victims of identity crime in the United States in 2012 [29]. Around 7% of households in the United States experienced identity theft victimization in 2010 [30] totaling about 8.6 million households [30]. The most quantifiable data relating to loss pertains to financial losses and this is expressed in the selected literature as follows. In 2010-2011 the estimated cost of personal fraud to Australians was $1.4 billion [31] with about 44,700 Australians being victims of identity crime [31]. Statistics from the United Kingdom suggest that identity crime is increasing prodigiously with the reported number of cases almost doubling from 77,500 to 123,600 between 2007 and 2012 [32]. These statistics suggest that identity crime is global and significant in terms of its impact and financial cost.

It is likely that the uptake of social networking has contributed to the volume of information exchanged and subsequently identity crime. Further, among the methods used by an identity criminal to obtain information is to utilize social engineering to gather information from other users [33]. A criminal may purport to be someone else like a friend or relative to gather the information they need to commit identity crime [34]. Hence caution should be exercised with friend requests in addition to the promulgation of information. In the context of corporate crime, a criminal might affiliate themselves with an organization or someone known to the organization [23]. A common rationale for this activity is that it is easier to obtain information through manipulation than by exploiting system security [35]. This approach seeks to exploit social interaction by playing on emotions [36].

While computer crime occurs through many highly technological means and is a highly sophisticated crime, paradoxically a basic understanding of computers is all that is needed to commit identity crime on the Internet [37]. Unlike other computer crime, this crime is pervasive as it is not restricted to those with specialist skills. A rudimentary understanding of information is what is needed along with an understanding of the crime and Internet access. In addition, identity crime is easy to commit and there is a low cost to committing it [37]. This crime is more readily accessible to criminals than many other Internet-related crimes because it is an instantaneous crime that is open to many prospective criminals [38]. In many respects the Internet has opened up numerous online communication mechanisms, as well many new ways of committing crime. Many of these aspects of identity crime make it attractive to criminals.

The dissemination of information has increased the risk of identity crime as well as establishing a separate industry based on the trade of personal identification information. Past research has suggested that purchasing information is the most common way of obtaining the information needed to perpetrate identity crime [39]. Beyond that, there are other techniques that can be used to obtain information [40]. However, the increased availability of information online has created an underground market for that information [41]. This presents numerous commercial imperatives for sharing that can also feed into identity crime and may devolve from social networking. The availability of personal identification information is the enabler for this crime and increasingly has a measurable monetary value [20]. Further, social networking feeds into the mass of information that has such a value and in many respects supports the current research around the cloud computers and the ways the Internet is emerging [42].

V. 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 are those most likely to be victimized by identity criminals [35]. However, people of working age are at also at risk due to their levels of income as well as their relevant engagement with emerging technologies on the Internet [35]. Working age victims present ready-made targets to identity criminals and it is also probable that the risk of victimisation is linked to increased levels of engagement with technology [39]. Having said that, children have become victims of this crime for reasons that include the inadequate supervision of children's Internet usage [43]. Children have a vulnerability to identity theft crime as they usually possess unblemished personal histories and remain relatively undefended as targets of this crime [35]. In addition, children often unknowingly share information about themselves that can place them at risk particularly if left unmonitored [35]. However, anyone using social networking can become a target of this crime and social networking: it seems reasonable to suggest that the more one reveals about oneself online, the more that can be used to perpetrate this crime.

Identity crime is serious because of the financial and emotional cost of the crime. The cost of identity crime comprises both direct and indirect costs. The most significant cost of identity crime is the financial cost [44], but the cost of identity crime extends beyond financial loss and incorporates additional costs referred to as soft costs [44]. The financial costs (the hard costs) are easily quantified whereas the non-financial costs (soft costs), such as those that relate to the cost of damage to reputation and the emotional cost of the crime, are more difficult to quantify and to prevent [44]. However, the cumulative losses can only be determined by considering both the hard and soft costs of this crime [44]. The banking sector for instance, is exposed to significant losses in relation to identity crime [44] but its spokespersons remain reluctant to disclose the losses arising from this crime [45]. Nonetheless, bank losses in the United States have been estimated to amount to over $2 billion per year [46]. However, due to the commercial sensitivities many banks are reluctant to share data [45]. This reluctance contributes towards the difficulty of establishing an accurate measurement of the true cost of identity crime [47]. Furthermore, there are issues with victims not reporting victimisation that also contributes toward the lack of accurate data [48]. The crime has a

profound impact on an individual in terms of damaging their reputation and confidence as well as being financially reprehensible.

VI. RESPONDING TO THE CRIME

There are many practical difficulties in convicting identity criminals [47]. In the first place, in an international context, no central body is responsible for overseeing crime committed via the Internet. For this reason, controlling crime perpetrated through social networking sites is fraught with difficulties in the investigation and enforcement [48]. The Internet is a dispersed communication entity that permeates country boundaries, making regulatory responses difficult [48]. Further, different values influence the ways in which, crimes are viewed domestically and most international instruments continue to require attention through domestic laws. Success of responsive efforts will be dependent on the stance maintained by each country in question [49].

The European Cybercrime Convention has worked to harmonize the regulation of cyber-crimes internationally [50] and it provides domestic criminal law authorities with cooperative mechanisms to investigate and prosecute computer crimes [50]. The term 'cybercrime' is a phrase the European Convention uses to describe crimes where the computer or computer network is the target. Computer crime is distinguishable from traditional crimes because a computer is used to commit the crime [51]. This therefore subsumes frauds where the computer is used as a tool to commit the crime [50]. Likewise, when identity crime takes place through the computer it is arguably captured within the scope of the European Convention. However, the European Convention fails to deal directly with identity crime [50]. Rather, it captures computer-related forgery (article 7) as well as computer-related fraud (article 8) and it would apply to related offenses including identity crime but this is not made explicit [50]. The significance of this convention is that it assists in the investigation and enforcement of identity crime despite not making reference to it [50]. Given its scope for computer crimes, it would arguably encompass identity crime. Unfortunately, there is nothing simple about applying criminal sanctions to international identity crime particularly when they fall outside globally acknowledged crimes and 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.

VII. PRIVACY PERSPECTIVE

International responses to privacy share comparable challenges with the international regulation of crimes on the Internet. There is a lack of centrality when it comes to the regulation of privacy internationally [52]. Domestic laws are often based on international agreements that are relied upon to regulate privacy [48]. International principles of privacy protection are provided for in international agreements like the Universal Declaration of Human Rights [53]. This international agreement recognizes the protection of the inalienable rights of all humans to privacy, highlighting the need for them to enjoy freedom of speech and belief [53]. Further, Article 12 suggests that no one should be subjected to interference with respect to their privacy [53]. This international agreement provides the foundation for the development of domestic laws in the same way as the European Convention does for cybercrimes [48]. However, despite the operation of this agreement, a limitation of the Australian privacy responses, for instance, is that they are not prescriptive. Further, privacy is constrained by the same jurisdictional boundaries that limit the extraterritorial reach of criminal sanctions explained above [54]. This means that there are challenges of dealing with identity crime and privacy in an international context.

VIII. FOCUS ON THE VICTIMS

The perpetrators of identity crime are illusive and many victims will often not know that they have become victims until considerable time has passed [55]. The time between when an identity crime occurs and an investigation takes place makes it difficult to gather evidence about the crime and to locate and prosecute the offender [55]. During this time, the victim must withstand the frustration and emotional distress and the financial losses caused by the crime. The impact of this is worsened the longer it takes for the situation to be resolved [56]. The subversive nature of this crime adds to a victim's frustration as well as facilitating the criminal's opportunity to evade capture. The crime also places an emotional burden on the victim and once an identity crime is discovered it can also take considerable time to resolve [56]. This delay influences the ability of law enforcement to investigate the crime effectively and provides the criminal with a greater likelihood of avoiding capture. This crime is pervasive and the criminal's illusive natures makes it difficult to capture them. Identity criminals may also harvest personal information over a period of time [39]. Further, the victim of the crime will find it difficult to determine when and where the information was obtained and what corrective action they should take to avoid future victimisation.

IX. DIFFICULTIES OF RESPONDING TO THE CRIME

A major challenge in responding to identity crime is the ability of law enforcement agencies to obtain evidence for the prosecution of perpetrators of this crime. The gathering of evidence involves obtaining digital evidence both on- and off-line [57]. As there are many new ways of using information, it is essential for investigative efforts to deal with the speed data transference takes place on the Internet, making the investigation of identity crimes difficult [58]. Furthermore, as

identity crime is cross jurisdictional, cooperation between law enforcement authorities is essential [59]. This also makes the civil responses to identity crime difficult given the scarcity of resources the individual has to prosecute criminals. Similar issues around detecting and locating the offender also exist for these actions.

A key weakness in the integrity of data is the way individual users manage their own information. Social networking users need to be more accountable for the information they willfully share on social networking sites. Each activity we engage in on the Internet leaves traces and a commonsense response to dealing with the exploitation of social networking by identity criminals is for social networking users to improve their behavioral practises on the Internet [57]. An educational program is necessary to ensure that social networking users are aware of the risks and of the need to exercise caution with respect to the sharing of personal information [60]. Moreover, this should take into account the ways information might potentially be misused by criminals [59]. While education could have a direct impact on crime reduction there will typically be a proportion of the population not responsive to such efforts [59]. The role of education is not going to resolve the crime entirely but irrespective it should be regarded as a way of dealing with this crime. However, social networking sites also should accept some responsibility for the protection of the users as they are responsible for attracting and retaining them. This should be broader than the general technological security measures and needs to include the architecture underpinning the sites to give users better understanding [61]. This might involve reconsidering the architecture that facilitates information exchange. Ultimately, identity crime can be reduced through better understanding of and mitigation of these risks [62].

Social networking providers put forward mechanisms to assist in the protection of information [15]. However, many of the tools used by social networking sites are underutilized, which, may be due to their complexity or lack of integration with the interface [15]. Alternatively, it may be due to the lack of engagement with the technology. Many users tend to utilize default functions within their profile that could mitigate many of the benefits of these tools [63]. More could be done by social networking providers to apply enhanced measures through related tools to protect users.

A number of additional and general technical responses can be applied to prevent identity crimes. The responses include improved authentication and encryption measures and might also involve elementary information security measures [62]. The purpose of technological responses is to ensure data integrity is maintained while correspondingly preventing unwanted misuse of information or intrusion [64]. However, as with most responses, these efforts aim to improve information integrity [62], but the strength of the responses to identity crime are often balanced against the perceived costs of such preventative action. In this respect, the threat of identity crime and the need for technological protection is understated. Nonetheless, these important technological measures provide additional ways to deal with information security and identity crime.

X. THE PROFILE OF THE SOCIAL NETWORKING USER AT RISK

Research conducted by Fogel and Nehmad indicated that certain social networking users are more prepared to engage in risk taking behaviors than others. Further, Facebook users have a greater sense of trust in the service they use than Myspace users [9]. In this regard, it has been found that men are more prepared to accept requests for friendship on social networking sites than are women. Men are also more prepared to share details like phone numbers and addresses than women [9]. This is where there appears to be a dichotomy between those that share information on the Internet and victims. But interestingly and somewhat conversely, it is women that are more often victimized in identity crime than men [9]. However, anyone using social networking sites is at risk and it seems that the more information that is shared equates to greater risk.

As mentioned, the development of protocols for communication on social networking sites is still developing and this influences the ways that information is shared. An interesting example of this is how people accept friends on social networking sites. The likely behaviors online are expected to be quite different to those undertaken in person outside the Internet [17]. Permitting a friend to have access to a profile is viewed far differently than the parameters of friendship that exist beyond the Internet. However, in many respects there are some elements of these relationships that are likely to be similar and shared. Walther and Boyd refer to friendship as a relationship of support based around emotional support [2]. However, the characteristics of friendship on this basis offline are difficult to transpose to a social networking 'friend' online [65]. What is interesting about this interaction is that the characteristic behaviors offline are not transposed online, this is interesting to observe as the protocols continue to develop, and this changes the profile of the victim.

The issue of consent on social networking raises questions about the right to share information belonging to another. Given the lack of prevalence of privacy principles on social networking sites, it is difficult to assume that consent is freely given for the use of personal information on social networking sites [66]. The issue of consent extends to the timeframes that information is retained on social networking sites. On these sites, data are typically subject to retention periods but these are often not adhered to, as interesting information is used in profile histories to attract new users [67]. Much of the information on social networking sites is also used to derive commercial benefits, this may be contrary and likely to be different from users' expectations about how this information will be used [15]. It is important to note that the business model of social networking providers is based on the dissemination of information and these providers arguably

challenge the legal boundaries of privacy through the way they exchange data [15]. Once information has been passed on, particularly to third parties, it is unclear as to what obligations will be adhered to and the responsibilities of these parties are not defined [15]. Despite this being beyond the scope of this paper, users need to understand the risks attached to third party applications and understand the specific consent they are providing to the use of their sensitive information [8]. There are also significant privacy-related issues with these providers and the providers of third party applications to social networking sites, but this falls beyond the scope of this discussion.

There is an obvious dichotomy between the stakeholders involved with the protection of personal identification information and end users. Despite the many attempts to warn of the risks of information disclosure, information is still shared. The motivations of social networking providers are at odds with that of users [15]. There is a need to find the middle ground to ensure that a shared understanding is formed around the sensitivity of information online [68]. An educative effort is needed to deal with crimes [69], like identity crime that should include the social networking providers but should not be administered by them, given their divergent interests. There are few motivations for social networking sites to change their approach as there would be commercial ramifications in doing so [69]. However, they are in the best position to understand the architecture behind the interface and to deal with the problem.

Some researchers suggest that the improvement to privacy must come from improvements in the technology that underpins the architecture used by social networking services [62]. It is the technology that encourages information sharing in the first place, so the same technology can mitigate the incidence of crime in the future. The commercial interests may need to put aside interest for the greater good to reduce identity crime [27]. While many ways of exploiting individuals still exist, social networking has brought about new ways to exploit individuals and the service itself can play a role in reducing it [65]. The accessibility of social networking is an enabler for identity crime and the low cost of identity crime plays a role perpetuating the crime [66]. This crime brings new ways of committing old offenses [66]. In short, it would seem right that the mechanism itself should play a role in the solution.

XI. DISCUSSION

Ultimately, policymakers should consider a multi-faceted approach for dealing with identity crime [70]. A mixture of techniques is necessary to counteract the threats of identity crime as it requires a ubiquitous response [71]. The relationship between social networking and identity crime is unique and therefore requires unique and creative responses. A major obstacle to responding to social networking and identity crime is the availability of accurate data relating to the relationship between the two concepts. While not all approaches to dealing with this phenomenon have been canvassed in this paper, the ones that have provide insight into the many issues evident. In particular, there is a need for a greater understanding of the behavioral factors of individuals in interacting with technology [72]. In addition, steps need to be taken to deal with the dissemination of information to avoid victimisation as well as better mechanisms to deal with this crime after it occurs [73].

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 for further research to take place. More empirical research is needed to probe the parameters of this relationship. It is hoped that more interest in this research will be generated by raising awareness of this relationship.

XII. EVALUATION

The material discussed in this paper has largely been drawn from secondary sources to identify a relationship between social networking and identity crime. To develop the contention further, empirical research is needed to discover the scope of this relationship. This paper has explored a number of responses to this phenomenon but these are by no means exhaustive and further research into the relationship between social networking and identity crime would be likely to provide greater insights into the mechanisms that might better deal with this crime.

XIII. RECOMMENDATIONS

Information is a vehicle for identity crime and considerable information is stored on social networking sites. Legal and technological responses have limitations in relation to the extent they can mitigate this crime particularly given the voluntary nature of information dissemination and the issues around jurisdiction and cooperation discussed [74]. The individual vulnerability arises because of personal identification information that eventually means that behavioral factors are important in 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 in on the Internet involving information sharing, 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 behavioral norms can be changed on social networking sites then the risk inherent with identity crime can be reduced.

At the same time, individuals remain ambivalent to the risks that come from information sharing. A difficulty with information on social networking sites is that once it is shared with another person, it becomes harder to control [68].

Likewise the privacy mechanisms to prevent this are not strong. Social networking makes the protection of information far more difficult than traditional means, as information can be transferred instantaneously. With social networking, a tension exists between the technical designers of social networking sites and users concerning the disclosure of information, as one requires it for survival and the other for the joy of sharing experiences [75]. For social network providers this involves striking a balance, as far as they are compelled to, between the interests of members sharing information and their self-interest in promoting information sharing and risk [12].

More regulatory development is needed around privacy in an international context to develop principles to reflect the changing ways that information sharing takes place on the Internet. The regulatory environment needs to be progressive in the way that it deals with the changing risks present on the Internet [71]. In this, there are behavioral factors that need to be the focus as these relate to the decisions made by users in sharing information. Similarly, a better understanding of the crime and the new ways it can be committed through using social networking need to be developed [76].

XIV. IDENTITY CRIME REGULATION GLOBALLY

A number of barriers exist to dealing with this and related internet crime from a regulatory standpoint [77]. Criminal law has limitations in particular in supporting the victims of the crime. There are multiple issues that need to be resolved for regulation to be effective such as the need for cooperation to deal with the jurisdictional barriers to facilitate the investigation and prosecution of identity crimes [78]. The barriers to criminal sanctions also have an impact on actions in privacy as well as civil causes of action for the victims of this crime. In the absence of clear legal pathways, victims are left with few options for obtaining reparation. The issues of state sovereignty also present obstacles for actions against criminals [71]. The varied responses to identity crime complicate this. These present limitations on the ability of states and individuals to bring the offenders to justice and for victims to obtain support [80]. Internationally, there is a need for mechanisms to be developed in this realm to deal with the unique characteristics of this crime [71]. This will then translate to better domestic responses to this crime and related crime in Australia, as well as elsewhere [81].

XV. 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 [12]. The sharing of personal identification information is prominent on social networking sites in ways that promote profiles which, might include details such demographic details and others. This article has considered the many ways that social networking can potentially nourish the transference of personal information on the Internet, in turn providing 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. These issues pertain not only to the difficulty of applying criminal sanctions but also to those relating to privacy in a transnational context. Future research is needed to explore responses to this crime in detail. An important starting point for dealing with this crime is to increase awareness of the risks associated with information sharing around social networking. More research is also needed to develop further knowledge about this crime and to understand the data surrounding identity crime and the nexus of this to the responses to it. This research would aim to recognize identity crime as the pervasive and significant crime it is now and will continue to be into the future.

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 his outstanding editorial support. I would also like to acknowledge the support of the institutions I have studied at Australia and my research supervisors at Bond University. I would like to thank the ICDS peer reviewers for their comments on the draft sent to the ICDS 2014 Conference in Spain.

REFERENCES

[1] E. Holm, "Social Networking and Identity Theft in the Digital Society" The Eight International Conference on Digiatal Society ICDS2014) Mar. 2014, pp. 169-175, ISBN: 978-1-61208-324-7.

[2] 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, pp. 153-188, 2002.

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

[4] 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, pp. 51-71, Jan. 2002.

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

[6] F. Stutzman, "An evaluation of identity-sharing behavior in social network communities," International Digital and Media Arts Journal, vol. 3, pp.10-18, Aug. 2006.

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

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

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

[10] F. Stajano and P. Wilson, "Understanding Scam Victims: Seven Principles for Systems Security," Communications of the ACM, vol. 54, pp. 70-75, Mar. 2011, doi :10.1145/1897852.1897872.

[11] 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, pp. 27–53, Feb. 2011, doi: 10.1177/0093650210365537.

[12] M. Lucas, and N. Borrisov, "flyByNight: Mitigating the Privacy Risks of Social Networking," Proc. of the 7th ACM workshop on Privacy in the electronic society (WPES '08), ACM, Oct. 2008, pp. 1-8, doi10.1145/1456403.1456405

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

[14] 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, pp.1143-1168, Aug. 2007, doi: 10.1111/j.1083-6101.2007.00367.x.

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

[16] 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, pp. 263–273, May. 2007, doi: 10.1177/0165025407076439.

[17] 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, pp. 390-397, May. 2007, doi:10.1016/j.jadohealth.2006.11.146.

[18] SocialMediaToday. *Social Media in 2013: By the Numbers*. [Online]. Available from: http://www.socialmediatoday.com/content/social-media-2013-numbers

[19] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," Technology in Society, vol. 32, pp. 183-196, Aug. 2010, doi: 10.1016/j.techsoc.2010.07.001.

[20] South Korea. Organisation for Economic Co-operation and Development. Scoping Paper on Online Identity Theft [Online]. Available: http://www.oecd.org/sti/40644196.pdf 2008.01.09

[21] 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, pp. 661, Spring 1999

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

[23] Australian Crime Commission. *Organised Crime in Australia 2011*. [Online]. Available: https://www.crimecommission.gov.au/sites/default/files/oca2011.pdf 2011.01.28

[24] Criminal Code Act 1995 (Cth) div 372 (1)(a).

[25] P. Powale and G. Bhutkar, "Overview of Privacy in Social Networking Sites (SNS)," International Journal of Computer Applications, vol. 74, pp 39-46, July 2013.

[26] C. Dwyer, S. Roxanne, and K. Passerini. "Trust and privacy concern within social networking sites: A comparison of Facebook and Myspace," Proc. 2007 Thirteenth Americas Conference on Information Systems (*AMCIS 2007)*, Keystone, Aug. 2007, pp. 1-13.

[27] United Kingdom. Cabinet Office. *Identity Fraud: A Study*. [Online]. Available from: http://www.statewatch.org/news/2004/may/id-fraud-report.pdf 2013.11.10

[28] International Civil Aviation Organization. *Towards Better Practice in National Identity Managemen*t. [Online]. Available from: http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-19/TagMrtd19-wp03.pdf 2013.10.09

[29] Bureau of Justice Statistics. Victims of Identity Theft, 2012 (2013) http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4911 http://www.antifraudcentre-centreantifraude.ca/english/documents/Annual%202011%20CAFC.pdf 2013.12.12.

[30] National Crime Justice Reference Service. *Identity Theft – Facts and Figures.* [Online]. Available from: https://www.ncjrs.gov/spotlight/identity_theft/facts.html 2013.10.13.

[31] Australian Bureau of Statistics. *Personal fraud costs Australians $1.4 billion*. [Online]. Available from: http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument 2012.04.11

[32] CIFAS. *Is Identity Fraud Serious?* [Online]. Available from: http://www.cifas.org.uk/is_identity_fraud_serious 2012.06.06

[33] Symantec. *Social Engineering Fundaments, Part 1: Hacker Tactics. [Online]. Available from:* http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics 2001.12.18.

[34] Australian Bureau of Statistics. *Personal Fraud 2010-2011*. [Online]. Available from: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/65767D57E11FC149CA2579E40012057F?opendocument 2013.11.15.

[35] Carnegie Mellon. *Child Identity Theft. 2011* [Online]. Available from: http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf 2011.03.11

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

[37] CALPIRG Education Fund. *Policing Privacy: Law Enforcement's Response to Identity Theft.* [Online]. Available from http://www.calpirg.org/sites/pirg/files/reports/policingprivacy2003.pdf 2003.05.01.

[38] Ran Wei, "Lifestyles and New Media: Adoption and Use of Wireless Communication Technologies in China," New Media & Society, vol. 8, pp. 991-1008, Dec. 2006, doi: 10.1177/1461444806069879.

[39] K. Anderson, "Who Are the Victims of Identity Theft? The Effect of Demographics," Journal of Public Policy & Marketing, vol. 25, Fall, 2006.

[40] J. Paradiso, J. Heidemann, and J. Zimmerman, "Hacking involves the unauthoried interaction with computer systems," IEEE Pervasive Computing, vol. 7, pp. 13-15, July. 2008.

[41] L. Plowman, O. Stevenson, C. Stephen, and J. McPake, "Preschool children's learning with technology at home,"

Computers & Education, vol. 59, pp. 30-37, Aug. 2012, doi:http://dx.doi.org/10.1016/j.compedu.2011.11.014

[42] United States. State of New Jersey Commission of Investigation and Attorney General of New Jersey. *Computer Crime: a Joint Report; 2000*. [Online]. Available from: http://csrc.nist.gov/publications/secpubs/computer.pdf 2014.06.12

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

[44] 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, pp.169-208, Fall, 2003.

[45] 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, pp. 244-261, Jul. 2004, doi:10.1111/j.1745-6606.2004.tb00867.x.

[46] Kroll Advisory Solutions. *Global Fraud Report: The Strategic Impact of Fraud*, Regulation, and Compliance [Online]. Available from: http://www.krollconsulting.com/media/pdfs/KRL_FraudReport2011.pdf 2011.12.05

[47] R. Smith, *Addressing Identity-Related Fraud*. [Online]. Available from: http://www.aic.gov.au/about_aic/research_programs/staff/~/media/conferences/other/smith_russell/2003-09-identity.ashx 2012.12.09

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

[49] S. Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," Murdoch University Electronic Journal of Law, vol. 8, pp 1-40, June 2001, pp. 1.

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

[51] Council of Europe. *Convention on Cybercrime: Member States of the Council of Europe – Article 12* [Online]. Available from: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG 2011.07.15

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

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

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

[55] R. Mercuri, "Scoping identity theft,", Communications of the ACM, vol. 49, pp 17-21, May. 2006, Doi: 10.1145/1125944.1125961.

[56] W. Kim, O. Jeong, C. Kim, and J. So, "The dark site of the Internet: Attacks, costs and responses," Information Systems, vol 36, pp. 675-705, May. 2011, doi:10.1016/j.is.2010.11.003.

[57] Australian Government: Office of the Australian Information Commissioner. *Scanning "Proof of Identity" Document*s [Online]. Available from: http://www.privacy.gov.au/materials/types/infosheets/view/6553 2007.08.06

[58] C. Blakesley, "United States Jurisdiction over Extraterritorial Crime," The Journal of Criminal Law and Criminology, vol. 73, pp.1109-1163, January 1982.

[59] Federal Bureau of Prisons. *Recidivism among Federal Prisoners Released in 1987* [Online]. Available from: http://www.bop.gov/resources/research_projects/published_reports/recidivism/oreprrecid87.pdf 1994.08.22

[60] Organisation for Economic Co-operation and Development. *OECD Policy Guidance on Online Identity Theft* [Online]. Available from: http://www.oecd.org/dataoecd/49/39/40879136.pdf 2008.06.06

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

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

[63] B. Krishnamurthy and C. Wills, "On the Leakage of Personally Identifiable Information Via Online Social Networks," Proc. Of the 2nd ACM workshop on Online Social netowrks (WOSN'09) ACM, Aug. 2009, pp. 7-12, doi:10.1145/1592665.1592668.

[64] R. Sullivan, "Can Smart Cards Reduce Payments Fraud and Identity Fraud," Economic Review, vol. 93, pp. 35-62,.Third Quarter, 2008.

[65] G. Weir, F. Toolan, and D. Smeed, "The Threats of Social Networking: Old Wine in New Bottles?," Information Security Technical Reports, vol. 16, pp.38-43, January 2011.

[66] Trustwave, Global Security Report 2011 Trustwave. Available: http://www.secretservice.gov/Trustwave_WP_Global_Security_Report_2011.pdf 2011.05.01

[67] D. Rosenblum, "What Anyone Can Know: The Privacy Risks of Social Networking Sites," Security & Privacy, vol 5, pp.40-49, May. 2007, doi: 10.1109/MSP.2007.75.

[68] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in Online Social Networking profiles: The case of FACEBOOK," Computers in Human Behaviour, vol 26, pp. 406-418, May. 2010, doi:10.1016/j.chb.2009.11.012.

[69] G. Gackenbach and J. Karpen, J, "The Coevolution of Technology and Consciousness," in Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications, J. Gackenbach. Ed. California: Academic Press, 337-357, 1998.

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

[71] Rand Europe, *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Related Crime: Final Report*. [Online]. Available from: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf 2011.0601

[72] Centre for Problem-Oriented Policing. *The Problem of Identity Theft*. [Online]. Available from: http://www.popcenter.org/problems/identity_theft/ 2014.06.10

[73] S. Livingstone, K. Ólafsson, and E. Staksrud, "Risky Social Networking Practices Among "Underage" Users: Lessons for Evidence-Based Policy," Journal of Computer-Mediated Communication, vol.18, pp.303-320, Apr. 2013, doi: 10.1111/jcc4.12012.

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

[75] FirstMonday. *Friends, friendsters, and Top 8: Writing community into being on social network sites* First Monday. Available from: http://firstmonday.org/issues/issue11_12/boyd/index.html 2006.12.9

[76] Australian Government. *Identity Theft*. [Online]. Available from:

http://www.scamwatch.gov.au/content/index.phtml/tag/identitytheft 2011.03.11

[77] Australian Institute of Criminology. *Examining the Legislative and Regulatory Controls on Identity Fraud in Australia* [Online]. Available from: http://www.aic.gov.au/media_library/conferences/other/smith_russell/2002-07-fraud.pdf 2002.07.12

[78] Parliament of Australia. *House of Representatives Standing Committee on Communication Chapter 6: Criminal and Law Enforcement Framework* [Online]. Available from: http://parlinfo.aph.gov.au/parlInfo/search/summary/summary.w3p;adv=yes;orderBy=customrank;page=0;resCount=Default;query=Criminal+and+Law+Enforcement+Framework 2010.06.01

[79] Council of Europe. *Internet-Related Identity Theft Discussion Paper*. [Online]. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf 2007.11.17

[80] US Department of Justice. *Victims of Identity Theft, 2008* [Online]. Available from: http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf 2008.08.01

[81] Australian Institute of Criminology. *Counting the Costs of Crime in Australia* [Online]. Available from: http://www.aic.gov.au/documents/A/A/3/%7BAA329573-5D62-46FB-9E6F-4D86A6DDD9BC%7Dti247.pdf 2003.04.10