RUNNING HEAD: Fear of Cyber-Identity Theft

Fear of Cyber-Identity Theft and Related Fraudulent Activity

Lynne D. Roberts[1], David Indermaur[2] and Caroline Spiranovic[3]

Please address all correspondence to the first author: Lynne Roberts

[1] Dr Lynne Roberts, Senior Lecturer, School of Psychology and Speech Pathology, Curtin Health Innovation Research Institute, Curtin University, GPO Box U1987, Perth Western Australia 6845
Lynne.Roberts@curtin.edu.au
Tel: +61 8 9266 7183.
Fax: +61 8 9266 2464
[2] Dr David Indermaur, Associate Professor, Crime Research Centre, University of Western Australia, 35 Stirling Highway, Crawley WA 6009.
David.Indermaur@uwa.edu.au. Tel: +61 8 6488 3840.
[3] Dr Caroline Spiranovic, Research Assistant Professor, Crime Research Centre, University of Western Australia, 35 Stirling Highway, Crawley WA 6009.
Caroline.Spiranovic@uwa.edu.au Tel: +61 8 6488 2830

Abstract

Identity theft and related fraudulent activities affect approximately one in twenty-five adults each year across western societies. The Internet provides a new avenue for obtaining identity tokens and identifying information and increases the scale on which identity theft can be perpetrated. Recent research has suggested that fear of these types of crimes now matches or exceeds the fear of traditional place-based crimes, and has the potential to curtail online activities and hinder the further development of e-commerce applications. In this paper we conduct exploratory research identifying predictors of fear of cyber-identity theft and related fraudulent activities, based on the analysis of items included in the Australian Survey of Social Attitudes (2007). Fear was predicted by a generalised fear of crime component and a specific internet exposure component. Traditional predictors of fear of crime were insignificant or weak predictors, highlighting the need for further research.

Keywords: fear of crime; cyber-identity theft; fraud; cyber-victimisation; identity theft

Fear of Cyber-Identity Theft and Related Fraudulent Activity

The Internet provides new opportunities for criminal activities. It may be used to support existing criminal activities, provide new ways of conducting existing criminal activities, extend the geographic reach of criminal activities or create new types of criminal activity (Savona & Mignone, 2004). One type of cyber-criminal activity that is frequently featured in the media is cyber-identity theft and related fraudulent activity. The Internet enables an extension from 'traditional' identity theft (the misappropriation of identity tokens such as credit cards through non-technical means such as mail theft) to the online harvesting of identity tokens, potentially on a larger scale due to information and communication technologies increasing the ease and reducing the costs (time, financial and location) of data acquisition. Further, the Internet provides the means for conducting fraudulent activity with the stolen identity tokens, including online banking and e-commerce.

In this paper we first examine what is currently known about cyber-identity theft. Information on the incidence of identity theft and related fraudulent activity across three countries, the United States, United Kingdom and Australia is presented. This analysis highlights the difficulty of determining the percentage of this activity that is cyber-related. We then examine fear of cyber-identity theft and related fraudulent activity, situating our discussion within the body of literature concerning fear of traditional place based crimes. In the body of this article we examine possible predictors of fear of cyber-identity theft and related fraudulent activity. Three categories of predictors are considered. The first relates to demographic variables, the second to fear of traditional crime and the third to levels of access and activity on the Internet. It appears that traditional demographic predictors of fear of crime victimisation, such as

age and gender, are poor predictors of fear of cyber-identity theft victimisation. In contrast, fear of physical place-based crime and internet use variables were relatively stronger predictors of fear of cyber-identity theft. These results suggest that to comprehensively understand the nature of the fear of cyber-identity theft and related fraudulent activity a research program incorporating investigations at both quantitative and qualitative levels is needed.

Cyber-Identity Theft

Cyber-identity theft[4] involves the online misappropriation of identity tokens. Common online identity tokens include email addresses, web-pages and the combination of username and password used to access systems such as online banking. Traditional identity tokens can also be harvested online and include name, contact details (address, telephone number), tax file numbers and social security numbers. These identifiers are sufficient for an individual to obtain a credit card in the victim's name (Sweeney, 2006).

Cyber-identity theft typically combines the affordances of new Information and Communication Technologies (ICTs) with social engineering and includes methods such as hacking, phishing, pharming, traffic redirectors, advance-fee frauds, fake taxation forms, keyloggers and password stealers (Paget, 2007). Hacking has been employed successfully to obtain mass identifying information, including the account information held by Card Systems Solutions for 40 million credit card customers (Haygood & Hensley, 2006). The ease of obtaining identity tokens and identifying information online changes the scale on which identity theft can be perpetrated, expanding the range of potential victims (Finch, 2007; Marshall & Tompsett, 2005).

[4] A detailed exploration of cyber-identity theft is beyond the scope of this paper. For a review see Roberts (2008).

The number of individuals directly affected by cyber-identity theft remains difficult to estimate, partly because most victims of identity theft and related fraudulent activity are unaware of how the perpetrator obtained their identity tokens or identifying information. Whilst the individual knows they have been the victim of a fraud they remain unaware of whether this was as a result of an on-line breach or through some off-line means. For example, Synovate (2007) reported that the majority (56%) of identity fraud victims did not know how their identity information was obtained. In 2001 a US Federal Trade Commission director claimed that less than one per cent of reported cases of identity fraud could be linked to the Internet (Verton, 2001). Similarly, the results from the Pew Internet Tracking Report (Fox, 2001) indicated that only 8% of identity theft victims indicated the Internet *might* have been involved. Despite the technological and personal factors conducive to cyber-identity theft, at present offline identity theft appears to be the most commonly utilised form of identity theft, although this may change in the future.

While the proportion of identity theft and related fraudulent activity attributable to the Internet is unknown, population surveys conducted over the last decade are providing estimates of the proportion of the population affected by identity theft and related fraudulent activity of all types. Available estimates from the US, UK and Australia are reviewed below. While these prevalence statistics provide an indication of the extent of the problem of identity theft, White and Fisher (2008) caution that our knowledge of identity theft is hampered by variations in definitions used and reporting practices.

In the US, major population surveys on identity theft have been conducted by two organisations, Synovate (for the Federal Trade Commission) and Javelin Strategy and Research. Questions on identity theft have also been included in the National Crime Victimization Survey.

Javelin Strategy and Research conducted population based telephone surveys to estimate the number of identity fraud victims. Survey estimates suggest that the annual incidence of identity fraud victimisations decreased over the period 2004 (4.25%) to 2007 (3.58%), but increased in 2008 to 4.32% (Javelin Strategy and Research, 2009). It was estimated that in 2009 in excess of 11 million Americans had been the victim of identity fraud (Javelin Strategy and Research, 2010). The approximate dollar value associated with the fraudulent activity followed a similar trend, decreasing from $60 in 2004 to $45 in 2007, followed by an increase to $48 in 2008 and $363[5] in 2009 (Javelin Strategy and Research, 2009, 2010). Based on a population telephone survey, Synovate (2007) estimated that 3.7% of the adult US population were a victim of identity theft in 2005, a decline from the 2003 survey estimate provided by Synovate (2003) of 4.6%. Synovate estimated that in 2005 the median 'out of pocket' expense to individual victims was nil, and the median time spent resolving identity theft problems was 4 hours. However, some victims incurred considerably higher out of pocket expenses (95th percentile $2,000) and spent longer periods resolving their problems (95th percentile 130 hours). Costs and hours were higher for victimisations where new accounts were established than where fraudulent activities were restricted to existing credit and non-credit card accounts (Synovate, 2007). The National Crime Victimization Survey included questions about identity theft in 2004, reporting that three percent of households (3.6 million households) in the US had at least one household member who was a victim of identity theft in the previous six months (Baum, 2006). The results obtained from these population surveys are reasonably consistent. They suggest that identity theft affects about one in 25 adults in the US each year. However, for the majority of victims, the financial impact of

[5] 2009 figure based on only those who incurred costs.

victimisation is small and only limited time is required to resolve problems associated with the theft and resultant fraud.

The major report on identity fraud in the United Kingdom; Identity fraud: A study (Cabinet Office, 2002); estimated the cost of identity fraud was £1.3billion, accounting for approximately one tenth of all fraud in the United Kingdom (updated in 2006 to £1.72 billion (see http://www.ips.gov.uk/identity/downloads/FINAL-estimate-for-annual-cost-of-fraud-table-v1-2.pdf). Questions relating specifically to credit card fraud experienced by members of the public were included in the 2005/2006 British Crime Survey. Based on survey results, it was estimated that four per cent of UK credit card holders had been victim of credit card fraud over the previous twelve month period (Hoare & Wood, 2007). Thus the estimates of prevalence are very similar to those for the United States.

In Australia, the most recent reliable estimates of the extent of identity fraud come from the Australian Bureau of Statistics (ABS; 2008) Personal Fraud survey conducted in the second half of 2007. Population estimates from the survey suggest that in the previous 12 months, 3.1% of Australians over the age of 15 years were the victims of identity fraud. The majority (77%) were victims of bank card or credit card fraud and spent less than ten hours resolving the fraudulent activity. More than a third (36.3%) of credit and bank card fraud victims and more than a quarter (26.8%) of other identity theft victims in this Australian survey did not know the method of fraud used. However, Email or Internet was identified as the method of fraud in 19.8% of incidents of credit or bank card fraud and 21.2% of other identity theft incidents (ABS, 2008). Despite this, almost half (45%) of respondents in a further population based survey conducted in Australia thought the Internet was the most likely method of identity fraud, with 60% of respondent concerned about becoming a victim of identity fraud (Wallis Consulting

Group, 2007). These results indicate that the public perceive cyber-identity theft to be a more commonly used form of identity theft than the statistics indicate is likely to be the case.

Recent research has begun to analyse the risk of victimisation at state, community and individual levels. At a macro level, Higgins, Hughes, Ricketts and Wolfe (2008) examined state level correlates of identity theft victimisation in the US, utilising Federal Trade Commission reports and census data. Identity theft complaints were higher in states with lower ratios of males, but higher ratios of African Americans, residential mobility, public assistance and recreation and entertainment venues. At a micro level, Anderson (2006) reanalysed the data from the Federal Trade Commission's 2003 survey to examine the demographic characteristics of identity theft victims. Age, gender and income were predictors of identity theft victimisation, with younger adults, women and the more affluent more likely to be victims.

In Australia, data regarding the characteristics of victims of identify fraud (including both identity theft and credit or bank card fraud) is provided through the ABS (2008) Personal Fraud survey. In the twelve months prior to the survey, identity fraud victimisation was more frequently reported by males, those aged between 25 to 44 years, those with higher educational qualifications, and those with the highest weekly incomes. Contrasting these results with those from the US, it appears that there may be some cross-cultural variability with respect to the relationship between identity fraud and victim demographics such as age and gender. However, the Australian data mirrors that of the US in indicating that affluence is associated with identity fraud.

Typically, individuals are not regarded by law enforcement or legal agencies as the primary victims of identity theft related fraud. Instead, the status of primary victim is assigned to defrauded creditors; typically banks and other financial organizations; who incur the financial

cost of identity-related fraud (LoPucki, 2001). As previously outlined, for most individual victims of identity theft, there are minimal financial and time costs involved in dealing with identity-related fraud. However, some victims can incur financial costs associated with lost wages, medical expenses and expenses incurred in restoring the integrity of identity (Identity Theft Resource Centre, 2003; 2005; Jefferson, 2004; LoPucki, 2001). The cost to the individual is partially dependent upon the time interval from the theft to discovery, such that costs increase with longer intervals (Synovate, 2003). Secondary victimization in the form of denial of credit, increased insurance and credit card interest rates, cancellation of credit cards, denial of services (phone, utilities) and continued contact by collection agencies may result from impaired credit rating (Baum, 2006; Identity Theft Resource Centre, 2005; Synovate 2003). The psychological, emotional and physical impact of identity theft also increases for those who are unable to easily resolve problems associated with the identity theft (Sharp, Shreve-Neiger, Fremouw, Kane & Hutton, 2004).

While it is possible that the psychological impact of identity theft is not affected by the actual method of its completion (cyber versus traditional), there may be important differences. Our current inability to differentiate fraudulent activity by the source of identity theft means that we are not able to study the effects with accuracy. However we are able to investigate the fear individuals have of these two forms of identity theft.

Fear of Crime

While criminal activities can have direct impacts on individual, organisational and community victims, they also have a wider indirect impact on individuals and society through fear of crime. Fear of crime, whether or not it has a basis in the likelihood of crime victimisation,

can negatively impact on an individual's physical and mental wellbeing and social functioning through the curtailment of physical and social activities (Stafford, Chandola & Marmot, 2007).

Fear of crime is a concept that has been defined and measured in a variety of ways including concern about crime, perceived risk of victimisation, perceived threat and behavioural responses to fear (Skogan, 1999). Doubt has been cast over whether the much discussed concept of 'fear of crime' does indeed represent a fear, or is more accurately defined in terms of a general anxiety about crime (Warr, 2000). There are also questions about the best way to measure, reflect or tap in to the experience of fear (see Ditton and Farrell 2007).

A range of theories have been developed to make sense of what we know about the fear of crime. Briefly, these can be classified as relating to the vulnerability of the victim (the 'vulnerability thesis'); the (perceived) risk of victimisation (the 'instrumental thesis'); (perceived) incivilities within the environment (the 'incivilities thesis'); and psychological factors (Hale, 1996).

Demographic factors have been explored as predictors of fear of crime with relatively consistent findings that women and the elderly experience higher levels of fear of crime than men or younger adults, despite their lower risk of victimisation (see for example Ziersch et al., 2007), providing support for the vulnerability thesis. The vulnerability hypothesis is also supported by a range of findings which have shown that unfamiliarity is linked to the fear of crime. Perhaps not surprisingly, people tend to be more aware of situations and places they are less familiar with. Even those who live in relatively high crime neighbourhoods report feeling safer in those areas closer to home compared to other areas of the city even though those other areas may, on an objective level, be safer.

Fear of crime has consistently been shown to be out of proportion with the actual risk of victimisation (Chadee, Austen, & Ditton, 2007). Research from Canada suggests that about 12 per cent of the variance in fear of crime can be directly attributed to differences in neighbourhood context (Fitzgerald, 2008), providing modest support for the instrumental hypothesis that fear of crime simply reflects actual crime rates, at least at a local level.

Previous research has supported the proposed relationship between perceptions of incivilities and fear of crime– those that experience or perceive a higher level of incivilities also experience higher levels of fear of crime (Borooah & Carcach, 1997; Carcach, Frampton, Thomas & Cranich, 1995; Kanan & Pruitt, 2002; McCrea, et al, 2005; Roberts & Indermaur, forthcoming; Wyant, 2008). However these findings may also be interpreted as being in line with the vulnerability hypothesis as perceptions of incivilities contribute to a heightened awareness of vulnerability.

Fear of Cyber-Identity Theft

While fear of crime has received substantial research attention, limited research has been conducted on fear of cyber-crime, or more specifically fear of cyber-identity theft and related fraudulent activity. Qualitative research has suggested that fear of cyber-identity theft incorporates fear of financial losses, damage to reputation and loss of online privacy (Hille, Walsh, Brach & Dose, 2011). Some researchers (e.g. Wall, 2008a, 2008b) have argued that fear of cyber-crime is largely driven by myth perpetuated by the media, and may not be in proportion to the objective reality of cyber-crime. The results from those studies that have included measures relevant to the fear of cyber-identity theft and related fraud in the US, UK and Australia are summarised below.

In an early study by the Pew Internet and American Life Project (Fox, 2001) the majority of Americans surveyed (87%) were concerned about credit card theft online, with 69% 'very concerned'. Females, older adults and African Americans were more likely to be 'very concerned' than males, younger adults, Caucasians and Hispanics respectively.

While not directly asking about online fraudulent activity, the British Crime Survey in 2005/2006 included questions on fear of credit card fraud. More than half (57%) of the respondents who owned credit cards reported that they were 'fairly' or 'very' worried about being a victim of card fraud. Notably, this percentage was higher than worry about any of the traditional crimes also asked about in the survey. Respondents who had been the victim of credit card fraud in the previous year were more likely to be worried than those who had not (Hoare & Wood, 2007).

The Australian Survey of Social Attitudes (AuSSA) has been conducted four times between 2003 and 2009. The 2007 sweep of the survey included, for the first time, items related to worry about a range of crimes. Extending on our primary analysis of the crime and justice items included in the AuSSA 2007 survey (Roberts & Indermaur, 2009), in our recent research (Roberts & Indermaur, forthcoming) we analysed the AuSSA survey data to compare worry about traditional place-based crime with worry about emerging forms of criminal activity enabled by the rapid development of information and communication technologies, particularly the Internet. A major finding of this research was that worry about identity-related crime is now matching, and for some offences exceeding, worry about more traditional place-based crime. The illegal use of credit-cards over the Internet was one of the crimes included in this survey that generated the highest levels of worry (23% 'very worried', 27.9% 'fairly worried'). Fear of

having identity stolen via the Internet was also a source of worry (15.9% very worried, 24.4% 'worried').

These two items were combined with worry about having a credit-card stolen to produce a fear of identity theft related crime scale. Then analyses of predictors of fear as measured by this scale were undertaken. Traditional predictors of fear of crime (gender, age, years of education, location) were found to be poor predictors of worry about identity theft related crime. Fear of identity-theft related crime was lower for males than females, but accounted for less than one percent of the variation in fear of identity-related crime scores. Age was not a significant predictor. Location (metro/rural) and perceptions of incivilities were significant predictors, accounting for 5.3% of variance (Roberts & Indermaur, forthcoming).

In this paper we build on this previous research to specifically examine fear of cyber-identity theft and related fraudulent activity, using two items from the AuSSA survey that specified the Internet in relation to fear of crime. Given the poor predictive ability of traditional predictors of fear of crime to predict fear of cyber-identity theft and related fraudulent activity, we were interested in exploring a range of other possible predictors.

First, a finding from the ABS (2008) Personal Fraud survey was that individuals on higher incomes were at higher risk of victimisation. We hypothesised that if fear of crime has some basis in risk of victimisation (the 'instrumental hypothesis'), then fear of cyber-identity theft and related fraudulent activity will be higher for those with high incomes than those on lower incomes.

Second, Roberts and Indermaur (forthcoming) suggested there may be a generalised fear component underlying both fear of traditional crime and fear of identity related crime. We hypothesised that fear of place based crime will significantly predict fear of cyber-identity theft

and related fraudulent activity. Positive results here would suggest the operation of a generalised fear of crime component. The failure to find a significant relationship might suggest that fear of place-based crime and fear of cyber-crime are distinct concepts.

Third, we were interested in whether Internet use variables could add explanatory power in predicting fear of cyber-identity theft and related fraudulent activity. We hypothesised that Internet use will significantly predict fear of cyber-identity theft and related fraudulent activity (suggesting a level of exposure component). Positive results here would suggest fear may be related to the level of exposure; a finding in line with the instrumental hypothesis in regard to fear of crime. A significant but inverse relationship might suggest that fear is related to unfamiliarity; a finding in line with the experienced vulnerability hypothesis.

Method

The Australian Survey of Social Attitudes (AuSSA) is a biennial mail-out survey that measures Australians' social attitudes and behaviours (Gibson et al., 2005). The third biennial survey, AuSSA 2007, was a cross sectional mail out survey, consisting of three questionnaire versions. A random selection of 20,000 individuals was obtained from the Australian electoral roll. Pre-survey invitation letters were sent to the randomly selected individuals and were followed by the survey package and three reminders. The final set of respondents consisted of 8,133 adults from all states and territories in Australia. Final response rates for the three questionnaires ranged from 39% to 42%. Further details of the survey, methodology and weighting of the sample are provided in Roberts and Indermaur (2009). The data set analysed was provided by the Australian National University (Phillips et al, 2008).

Participants

The subset of AuSSA 2007 survey respondents included in this research are 1,550 respondents who completed Form C of the survey and answered each of the questions of interest for this analysis. Exactly half of the sample (50%) was female. The mean age of respondents was 47 years (*SD* = 15 years). The majority of respondents (74%) lived within a metropolitan area of Australia and had completed a mean of 14 years of education (*SD* = 4 years). The majority of the sample had access to the Internet. Seventy four percent of the sample used the Internet at home, with 56 percent of the sample using the Internet at work.

Measures

The AuSSA 2007 survey covered thirty five categories of attitudes and behaviours. The full questionnaires are available at http://aussa.anu.edu.au/questionnaires.php. A range of crime and justice items in the AuSSA 2007 survey were commissioned by the Australian Institute of Criminology and were included in two versions of the survey. Two of the crime and justice items were used together to produce the measure of fear of cyber-identity theft and related fraudulent activity. These items were:

How worried are you that the following will occur to you?

- *having your identity stolen via the Internet*
- *having your credit card details used illegally via the Internet.*

These items were selected as covering the two dimensions of definitions of cyber-identity theft, the stealing of identity and the use of the stolen identity in a fraudulent act (Grover, Beerghel & Cobb, 2011). Each item was measured on a four point response scale ranging from ‘not worried at all’ to ‘very worried’. The two items were computed into a scale with good internal consistency (Cronbach’s alpha = .86). Data were recoded so that higher scores on the scales reflect higher levels of fear of crime. Possible scale scores thus range from two to eight.

A further four items were used as a measure of traditional place based crime. Using the same question stem (How worried are you that the following will occur to you?) respondents were asked about being physically attacked at home; being physically attacked on the street or other public space; being sexually assaulted; and having their home/place of residence being broken into. Each item was measured on a four point response scale ranging from 'not worried at all' to 'very worried'. The four items from the questionnaire were combined to produce a scale with good internal consistency (Cronbach's alpha = .86). Data were recoded so that higher scores on the scale reflect higher levels of fear of crime. Possible scale scores range from four to sixteen.

Four items were used to provide measures of Internet use. Using the question stem 'Please tell us if you use the internet at any of the following?', two items related to the site of Internet use (at home and/or at work). A third item asked respondents 'In general, how often do you use the internet?' and was measured on a seven point scale ranging from 'several times a day' to 'do not use the internet'. The final item asked respondents 'How important are the following in informing your views of crime trends and the criminal justice system?' and respondents rated the extent to which the internet was important in this regard.

Single item measures of age (years), gender, years of education, location and gross household annual income were also retained for the analysis. Gross household income was recoded into three categories: low ($0 to $31,199 per annum), medium ($31,200 to $77,999 per annum) and high ($78,000 plus per annum).

Results

Scores were computed for each individual on the fear of crime scales. The mean scale score on the fear of cyber-identity theft and related fraudulent activity scale was 4.97 (*SD* = 1.9)

out of a possible scale score range of two to eight. The mean scale score on the fear of physical crime scale was 8.47 (*SD* = 2.68) out of a possible scale score range of four to sixteen.

To test the hypotheses that income, fear of traditional place based crime and Internet use would be significant predictors of cyber-identity theft and related fraudulent activity a hierarchical multiple regression analysis was conducted.

In the first step of the multiple regression analysis, traditional predictors of fear of crime; age, gender, years of education and location (metropolitan or non-metropolitan); along with income were entered into the analysis. Combined, these demographic variables accounted for a small, but significant 0.9% of the variance in fear of cyber-identity theft and related fraudulent activity (R^2 = .009, $F(6,1543) = 2.34$, $p<.05$). Sex was the only significant demographic predictor of cyber-identity theft and related fraudulent activity.

In the second step, fear of physical crime was entered into the analysis. This accounted for a significant additional 15.7% of variance in fear of cyber-identity theft and related fraudulent activity (ΔR^2 = .157, $\Delta F(1,1542) = 289.23$, $p<.001$). In the third and final step, the Internet use variables were entered into the analysis, and accounted for a significant additional 7.8% of variance in fear of cyber-identity theft and related fraudulent activity (ΔR^2 = .078, $\Delta F(4,1538) = 39.78$, $p<.001$). Combined, the predicting variables accounted for almost a quarter of the variance in fear of cyber-identity theft and related fraudulent activity (R^2 = .24.4, $F(11,1538)=45.07$, $p<.001$).

<insert Table 1 about here>

Table 1 provides the unstandardised and standardised regression coefficients and squared semi-partial correlations for each predictor variable in each step of the multiple regression analysis. In the final regression model (Step 3), the five significant predictors were age

(accounting for less than one percent of the unique variance), fear of traditional crime (accounting for 17.9% of the unique variance), the importance of the Internet for informing views of crime trends and the criminal justice system (accounting for one percent of the unique variance), using the internet at home (accounting for one percent of the unique variance) and Internet use frequency (accounting for less than one percent of the unique variance).

Discussion

Fear of cyber-victimisation, and in particular the fear of identity theft over the Internet, represents a significant threat to the free movement and quality of life of citizens in the 21st Century. Indeed identity theft over the Internet could be likened to highway robbery of earlier times when roads and highways began to be used on a regular basis. Just as in these earlier times there is a predictable progression. First, a new avenue of communication is established, it slowly begins to be used, it is quickly discovered as a criminal opportunity and then exploited. Eventually mechanisms are developed to address and prevent the criminal exploitation. In this process the period of greatest fear is likely to be the period when the form of communication is unfamiliar and potential users are alerted to the dangers represented by criminal opportunists. We are, arguably, at that stage now and understanding the dynamics of fear of identity theft over the internet represents a significant obstacle to the development of this new facility that is of benefit to citizens and their legitimate activities everywhere.

Worry about cyber-identity theft and related fraudulent activity is now greater than worry about many traditional place based crimes. This is despite findings that the majority of individual victims of cyber-identity theft and related fraudulent activity experience either no or minimal financial and time losses. Most costs are borne by financial institutions providing credit or access facilities. Indeed, Monahan (2009, p. 157) labels fear of cyber-identity theft a ‘moral panic’ as

"fear of being a victim of identity theft far outstrips its actual occurrence, and because extreme actions are taken to mitigate it". One potential societal impact of an exaggerated fear of cyber-identity theft is decreasing consumer trust and confidence in using the Internet to conduct business (Lynch, 2005). This has major implications for the future of ecommerce. Australian research (ABS, 2005) suggests that this may already be impacting on consumer behaviour, with security concerns preventing more than a quarter of Australians with Internet access from engaging in online purchasing and transactions. Similarly, Reisig, Pratt and Holtfreter (2009) reported that as the perceived risk of Internet theft victimisation increased, online purchasing decreased. Other service and government organisations may also be affected as fear and lack of trust mean that organisations increasingly need to adopt offline methods for customer communication (Lynch, 2005).

We found mixed support for our hypotheses regarding potential predictors of fear of cyber-identity theft and related fraudulent activity. Our first prediction, based on the instrumental hypothesis, that fear of cyber-identity theft and related fraudulent activity would be greater for those with high incomes was not supported. Fear of cyber-identity theft and related fraudulent activity appears to be a fear common across all socio-economic groups, even though victim surveys suggest that is those on higher incomes who are the most likely to be victimised.

Our second hypothesis, that fear of place based crime would significantly predict fear of cyber-identity theft and related fraudulent activity, was supported. This finding that fear of traditional place-based crime is a significant predictor of fear of cyber-identity theft and related fraudulent activity suggests that this 'new' fear is partially driven by an existing generalised fear component towards all types of crime. Indeed, fear of traditional place-based crime was the strongest predictor of cyber-identity theft and related fraudulent activity in this study, accounting

for almost three-quarters (73.4%) of the variance accounted for in the full model. This means that once we know that an individual scores high on general fear of crime we can predict that he/she will also score high on fear of cyber-identity theft. This finding supports the view that fear of crime is a general dispositional factor and not something that is highly discriminatory or dependent on risk. Put another way, an observed fear of cyber- identity theft probably tells us more about the person than it does about the real risks of identity theft, or indeed any situational contexts or cues related to cyber-identity theft. This generalised fear of crime has been discussed widely in the literature and the findings of the present study support the robustness of this construct. One implication of this observation is that in addressing fear of crime we should focus more on individual, psychological or dispositional factors related to fear and focus rather less on the object of the fear.

Our third hypothesis, that Internet use would significantly predict fear of cyber-identity theft and related fraudulent activity, was also supported. Three of the four internet use related variables had a significant positive association with fear of cyber-identity theft and related fraudulent activity. The strongest Internet use predictor was how important the Internet was in informing views of crime trends and the criminal justice system. This variable was moderately associated with frequency of Internet use. In turn, frequency of internet use and use of the internet at home were both significant predictors of fear of cyber-identity theft and related fraudulent activity. Taken together, these findings suggest an 'exposure effect', whereby the predictive power of Internet use variables relate to a rational evaluation process in which a person may reason that they use the internet frequently and hence would have a higher likelihood of being the victim of a cyber-related offence. Alternatively, it could be the case that frequent internet users are more 'savvy' users and understand the ease with which an offender could

commit cyber-crimes and hence conclude that they could unwittingly become a victim of such crimes. Nonetheless, further research is needed to ascertain the basis for the predictive power of internet use variables in the context of cyber-crime related fear.

Most traditional predictors of fear of crime included in this research; gender, education and location; were poor predictors of fear of cyber-identity theft and related fraudulent activity. These findings suggest that variables traditionally linked with fear of crime, such as gender, may not be relevant in the non-contact online environments. The lack of physicality of participants in cyberspace changes some of the fundamental relations and dynamics that underlie the study of traditional forms of crime and by extension the fear of crime. Similarly, 'physical location' is also irrelevant when it comes to cyber-identity theft. One possible area for further research is to investigate the possible role of 'virtual location' (the types of virtual environments an individual uses) as a predictor of fear of cyber-identity theft and related fraudulent activity.

The only 'traditional' significant fear of crime predictor in this study was age, accounting for less than one percent of the unique variance in fear of cyber-identity theft and related fraudulent activity. Across the three models the contribution of age varied in both significance and direction, leaving us with little confidence that it is a meaningful predictor of cyber-identity theft and related fraudulent activity.

While the findings from this study provide some interesting insights into the fear of cyber-identity theft and related fraudulent activity, a limitation of the study is the way in which the constructs of interest were operationalised. The analysis was based on an existing data-set confining the selection of variables. Future research would benefit from the development of an expanded measure of fear of cyber-identity theft and related fraudulent activity. As previously mentioned, specific measures of virtual location and the type of activities engaged in online

could be included in future research. Other measures for consideration for inclusion in future research include previous victimisation, perceptions of likelihood of victimisation and a measure of the extent to which the individual employs technical and social precautions to reduce their risk of cyber-identity theft and related fraudulent activity.

In summary, this research contributes towards an understanding of the basis of fear of cyber-identity theft and related fraudulent activity. Based on the analysis of a survey of the Australian population, predictors of this fear were identified. The strongest predictor was fear of traditional crime, accounting for approximately 18% of the unique variance in fear scores, suggesting a generalised fear of crime component underlying the fear of cyber-identity theft and related fraudulent activity. Internet use variables also significantly contributed to the prediction of fear of cyber-identity theft and related fraudulent activity, with fear increasing as use increased, and those using the Internet at home experiencing higher levels of fear than those who did not. Traditional predictors of fear of crime were insignificant or weak predictors of fear of cyber-identity theft and related fraudulent activity. To comprehensively understand the nature of the fear of cyber-identity theft and related fraudulent activity a research program incorporating investigations at both quantitative and qualitative levels is needed.

To conclude, the findings from our study contribute towards an understanding of the fear of cyber-identity theft and related fraudulent activity. This is an under-researched area within criminology, yet the impact of fear of cyber-crime may be large. This study was important in analysing fear of an acquisitive crime that is not in any way related to physicality. The findings reflect a central irony of our times: advances in technology and communication are accompanied by, or co-occur with, a generalised fear, aversion to risk and erosion of personal confidence. Some scholars (e.g., Furedi, 1997; 2006) have focussed on the culture of fear which is

exacerbated by media exposes of victims. Best (1999) discussed how in this regard media imperatives dictate a continuing focus on ‘new’ crimes and ‘new’ dangers. Internet related identity theft clearly fits into these categories and provides ready grist for the media mill, with a content analysis of media reports on identity theft identifying themes of identity theft as ‘unstoppable’ and driven by new technologies (Morris, 2008). The likelihood is that as time passes the use of identity tokens will be less novel and people will become more familiar with them and their utility. Better safety precautions and mechanisms to prevent and reduce fraud will be developed. However, the general erosion of trust and feelings of impotence are less easily remedied and belong to a much wider social project.

References

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing, 25*, 160-171.

Australian Bureau of Statistics (2005). *Household use of information technology 2004–05, Cat. no. 8146.0*. Canberra: Author.

Australian Bureau of Statistics. (2008). *Personal fraud 2007*. Canberra: Author.

Baum, K. (2006, April). Identity theft, 2004: First estimates from the National Crime Victimization Survey. *Bureau of Justice Statistics Bulletin.* Retrieved May 27, 2007 from www.ojp.gov/bjs/pub/pdf/it04.pdf.

Best, J. (1999). *Random Violence: How we talk about new crimes and new victims*. Berkeley, CA: University of California Press.

Borooah, V. K., & Carach, C. A. (1997). Crime and fear: Evidence from Australia. *British Journal of Criminology, 37*, 635-657.

Cabinet Office. (2002). *Identity fraud: A study*. Retrieved May 27, 2007 from http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf

Carcach, C., Frampton, P., Thomas, K., & Cranich, M. (1995). Explaining fear of crime in Queensland. *Journal of Quantitative Criminology, 11*, 271-287.

Chadee, D., Austen, L., & Ditton, J. (2007). The relationship between likelihood and fear of criminal victimization. *British Journal of Criminology, 47*, 133-153.

Ditton, J., & Farrall, S. (2007). The British Crime Survey and fear of crime. In M. Hough & M. Maxfield (Eds.), *Surveying crime in the 21st century* (pp. 223-243). Monsey, NY: Criminal Justice Press.

Finch, E. (2007). The problem of stolen identity and the Internet. In Y Jewkes (Ed.), *Crime on-line* (pp. 29-43). Cullompton, UK: Willan.

Fitzgerald, R. (2008). Fear of crime and the neighbourhood context in Canadian cities. *Crime and Justice Research Paper Series*. Ottawa, Ontario: Canadian Centre for Justice Statistics.

Fox, S. (2001). Fear of online crime. *Pew Internet Tracking Report*. Washington, DC: Pew Internet & American Life Project.

Furedi F. (1997). *Culture of fear: Risk-tasking and the morality of low expectation*. London: Cassell.

Furedi, F. (2006). *Culture of fear revisited: Risk-taking and the morality of low expectation.* London; New York: Continuum International Publishing Group

Gibson, R., Wilson, S., Meagher, G., Denemark, D. & Western, M. (2005). Introduction. In S. Wilson, G. Meagher, R. Gibson, D. Denemark & M. Western (Eds), *Australian social*

attitudes: The first report (pp. 1-11). Sydney, NSW: University of New South Wales Press.

Glassner B. (1999). *The culture of fear: Why Americans are afraid of the wrong things.* New York, NY: Basic Books.

Grover, A., Berghel, H., & Cobb, D. (2011). The state of the art in identity theft. *Advances in Computers, 83*, 1-50.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology, 4*, 79-150.

Haygood, R. & Hensley, R. (2006). Preventing identity theft: New legal obligations for businesses. *Employment Relations Today, 33*(3), 71-83.

Higgins, G. E., Hughes, T., Ricketts, M. L., & Wolfe, S. E. (2008). Identity theft complaints: Exploring the state-level correlates. *Journal of Financial Crime, 15*, 295-307.

Hille, P., Walsh, G., Brach, S., & Dose, D. (2011). Why online identity theft poses a major threat to e-business. In: *Proceedings of the ACM WebSci'11* (pp. 1-2). Retrieved August 20, 2011 from http://journal.webscience.org/518/.

Hoare & Wood (2007). Plastic card and identity fraud. In J. Fkatekley (Ed.), *Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey* (Supplementary Volume 2). Retrieved February 21, 2009 from http://rds.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf.

Identity Theft Resource Centre. (2003). *Identity theft: The aftermath 2003*. Retrieved March 2, 2007 from http://www.idtheftcenter.org/idaftermath.pdf.

Identity Theft Resource Centre. (2005). *Identity theft: The aftermath 2004*. Retrieved March 2, 2007 from http://www.idtheftcenter.org/idaftermath2004.pdf.

Javelin Strategy & Research (2009). *2009 Identity fraud survey report: Identity fraud on the rise but consumer costs plummet as protections increase.* Pleasanton, CA: author. Report preview retrieved February 21, 2009 from http://javelinstrategy.com/research`

Javelin Strategy & Research (2010). 2010 *Identity fraud survey report: Consumer version.* Pleasanton, CA: author. . Report preview retrieved August 16, 2011 from https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf

Jefferson, J. (2004). Police and identity theft victims-Preventing further victimisation. *Australasian Centre for Policing Research, No 7*. Retrieved March 2, 2007 from http://www.gov.au/publications2.asp?Report_ID=154

Kanan, J. W., & Pruitt, M. V. (2002) Modeling fear of crime and perceived victimization risk: The (in)significance of neighborhood integration. *Sociological Inquiry, 72*, 527–548.

LoPucki, L. M. (2001). Human identification theory and the identity theft problem. *Texas Law Review, 80*, 89-135.

Lynch, J. (2005). Identity theft in cyberspace: Crime Control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Journal, 20*, 259-300.

Marshall, A. M., & Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law & Security Report, 21*, 128-137.

McCrea, R., Shyy, T-K., Western, J., & Stimson, R. J. (2005). Fear of crime in Brisbane: individual, social and neighbourhood factors in perspective [online]. *Journal of Sociology, 41*, 7-27.

Monahan, T. (2009). Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology, 13*, 155-176.

Paget, F. (2007). Identity theft. *McAfee Avert Labs technical white paper No 1*. Retrieved May 27, 2007 from http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf.

Phillips, T., Mitchell, D., Tranter, B., Clark, J., & Reed, K. (2008). *The Australian Survey of Social Attitudes, 2007*. Canberra: Australian Social Science Data Archive, The Australian National University.

Phillips, T., Tranter, B., Mitchell, D., Clark, J. and Reed, K. (2007). *Australian Survey of Social Attitudes.* The Australian National University: ACSPRI Centre for Social Research.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*, 369-384.

Roberts, L. & Indermaur, D. (2009). *What Australians think about crime and criminal justice: Results from the 2007 Australian Survey of Social Attitudes.* Canberra: Australian Institute of Criminology.

Roberts, L. & Indermaur, D. (forthcoming). Are neighbourhood incivilities associated with fear of crime? In A. Evans (Ed.), *Australian social attitudes*, Volume 3.

Roberts, L. D. (2008). Cyber identity theft. In R. Luppicini & R. Adell (Eds.), *Handbook of research on technoethics* (pp. 542-557). Hershey, PA: Information Science Reference.

Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research, 10*, 3-26.

Sharp, T., Shreve-Neiger,A., Fremouw, W. Kane, J., & Hutton, S. (2004). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences, 49*(1), 131-136.

Skogan, W. (1999) Measuring what matters: Crime, disorder and fear. In R. Langworthy (Ed.), *Measuring what matters* (pp. 37-53). Washington, DC: U.S. Department of Justice, National Institute of Justice and Office of Community Oriented Policing Services.

Stafford, M., Chandola, T. & Marmot, M. (2007). Association between fear of crime and mental health and physical functioning. *American Journal of Public Health, 97*, 2076-2081.

Sweeney, L. (2006). Protecting job seekers from identity theft. *IEEE Internet Computing, 10*(2), 74-78.

Synovate. (2003). *Federal Trade Commission-Identity theft survey report*. Report prepared for Federal Trade Commission. Retrieved May 20, 2007 from http://www.ftc.gov/os/2003/09/synovatereport.pdf

Synovate. (2007). *Federal Trade Commission-2006 identity theft survey report*. Report prepared for Federal Trade Commission.

Verton, D. (2001). Identity thefts skyrocket, but less than 1% occur online. *Computerworld, 35*(7), 7.

Wall, D. (2008a). Cybercrime and the culture of fear. *Information, Communication and Society, 11*, 861-884.

Wall, D. S. (2008b). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology, 22*, 45-63.

Wallis Consulting Group. (2007). *Community attitudes to privacy 2007*. Report prepared for the Office of the Privacy Commissioner, Australia.

Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. *Criminal Justice, 4*, 451-89.

White, M. D., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review, 19*, 3-24.

Wyant, B. R. (2008). Multilevel impacts of perceived incivilities and perceptions of crime risk on fear of crime. *Journal of Research in Crime and Delinquency, 45*, 39-64.

Ziersch, A., Putland, C., Palmer, C., MacDougall, C., & Baum, F. (2007). Neighbourhood life, social capital and perceptions of safety in the western suburbs of Adelaide. *Australian Journal of Social Issues, 42*, 549-562.

Table 1

Unstandardised (B) and Standardised (β) Regression Coefficients, and Squared Semi-Partial Correlations (sr^2) for Each Step of the Hierarchical Multiple Regression Predicting Fear of Cyber-Identity Theft and Related Fraudulent Activity.

Variable	*B*	β	sr^2
Step 1			
Age	-.002	-.013	.000
Sex (female)	.209*	.055	.003
Education (years)	.042	.081	.001
Location (metro)	.181	.043	.002
Income (medium)	.085	.019	.000
Income (high)	.124	.032	.001
Step 2			
Age	.000	-.007	.000
Sex (female)	-.182	-.048	.002
Education (years)	.042**	.081	.006
Location (metro)	-.028	-.007	.000
Income (medium)	.195	.043	.001
Income (high)	.276	.071	.003
Fear traditional crime	.297**	.416	.157
Step 3			
Age	.014**	.107	.008
Sex (female)	-.126	-.033	.001
Education (years)	.003	.006	.000
Location (metro)	-.111	-.026	.001
Income (medium)	.107	.024	.000
Income (high)	-.009	.002	.000
Fear traditional crime	.294**	.411	.148
Internet views crime	.248**	.132	.014
Use Internet at home	.583**	.133	.008
Use Internet at work	.113	.029	.000
Internet use frequency	.119**	.140	.006

*p<.05
**p<.01