Investigating identity crime and misuse in Australia: The role of prevention technologies and the likelihood of victimisation

Journal:	*Journal of Criminological Research, Policy and Practice*
Manuscript ID	JCRPP-08-2024-0056.R1
Manuscript Type:	Research Paper
Keywords:	Identity theft, Information misuse, Indigenous status, Victimisation, Technology use, Public health

MANUSCRIPT DETAILS

TITLE: Investigating identity crime and misuse in Australia: The role of prevention technologies and the likelihood of victimisation

ABSTRACT:

This study examines identity theft as a significant and growing issue in Australia, not only due to its financial impact but also because of the emotional, psychological, and physical harm it causes, making it a public health concern. The research aims to analyse the results of the 2019 Australian Institute of Criminology (AIC) survey to identify factors associated with an increased likelihood of identity theft victimisation.

The study involved a detailed analysis of the 2019 AIC survey, which had 9,968 respondents from a sample of 10,000. The research focused on whether respondents had ever been victimised by identity theft and analyzed various characteristics, including demographics (gender, age, Indigenous status, education), income, computer usage, and preventive technology use, as potential indicators of future victimisation. Univariate analysis (Chi-squared test and two-sample t-test) was used to assess individual associations, while multivariate analysis (logistic regression) identified significant predictors of victimisation.

The univariate analysis indicated that all sub-variables were individually associated with identity theft victimisation. However, the multivariate analysis revealed that only identifying as Aboriginal and Torres Strait Islander, having an income between $18,201-$37,000, and using multiple preventive technologies were significant predictors of victimisation. The unexpected finding that increased preventive technology use correlates with a higher risk of victimisation contradicts the survey's suggestion that victims adopt more careful behaviour post-victimisation.

CUST_RESEARCH_LIMITATIONS/IMPLICATIONS__(LIMIT_100_WORDS) :No data available.

The research highlights the need for further investigation into the counterintuitive finding that greater use of preventive technologies may increase the risk of identity theft. Understanding this discrepancy could inform the development of more effective identity theft prevention strategies by the government and related agencies.

CUST_SOCIAL_IMPLICATIONS_(LIMIT_100_WORDS) :No data available.

This study contributes to the existing literature by offering a nuanced understanding of the factors associated with identity theft victimisation in Australia, that may be applicable globally. The unexpected findings regarding the use of preventive technologies provide a basis for further research and have the potential to influence future policy-making and identity theft prevention efforts.

Investigating identity crime and misuse in Australia: The role prevention technologies play in the likelihood of victimisation

Identity theft is a significant and growing issue in Australia, exacerbated by the internet and ease of sharing personal information. Beyond its financial impact, identity theft also causes emotional, psychological, and physical harm, making it a public health concern. To assess its prevalence, the Australian Institute of Criminology (AIC) conducts an annual survey, with the 2019 survey involving 9,968 respondents from a sample of 10,000. This study aims to analyse the 2019 survey results to identify factors that are associated with an increase in the likelihood of identity theft victimisation. The primary focus was on whether respondents had ever been victimized by identity theft and which characteristics, including demographics (gender, age, Indigenous status, education), income, computer usage, and preventive technology use, were significant indicators of future victimisation. Univariate analysis (Chi-squared test and two-sample t-test) showed that each sub-variable was individually associated with victimisation. However, multivariate analysis (logistic regression) found that only identifying as Aboriginal and Torres Strait Islander, having an income between $18,201-$37,000, and using multiple preventive technologies were significant predictors of victimisation. The finding that more preventive technology use correlates with higher victimisation risk is surprising and counterintuitive, contradicting the survey's indication that victims adopt more careful behaviour post-victimisation. While there could be plausible explanations for the finding, this discrepancy suggests a need for further investigation and replication of the results with more recent data. Nonetheless, this research offers the government potential directions to improve identity theft prevention strategies.

Keywords: Identity theft, information misuse, victimisation, Indigenous status, technology use, public health

Introduction

Identity theft, defined by Koops & Leenes (2006) as "…fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool with that person's consent" (pp. 5), is a growing problem in today's digital age where sensitive personal information is readily accessible online. Identity theft has also been defined as a form of social engineering that exploits vulnerabilities in individuals, organisations, and systems to gain access to personal information, financial assets, or other valuable resources (Kshetri, 2017). In Australia, identity theft is one of the most prevalent types of crime (Cross 2017; Franks & Smith, 2020) with significant impacts on the victims' financial, psychological, and emotional well-being, as well as on the reputation of the affected organisations (Cross & Layt, 2022; Kshetri, 2017).

In 2007, the Australian Institute of Criminology (AIC) was engaged by the Attorney-General's Department to monitor identity crime and misuse nationwide in response to the National Identity Security Strategy which aimed to protect the identities of Australians in a more efficient and regulated manner, and better quantify the nature and extent of identity crime (Criminology, n.d.). Each year, the AIC surveys Australians about their experience with identity crime during the preceding 12-month period, as well as within their lifetime – the results of which are then used to help raise awareness of identity crime and reduce its impact on Australians (Franks & Smith, 2020).

In 2019, the crime and misuse survey results showed that 25% of the respondents had experienced some form of personal information misuse within their lifetime, with 12%

experiencing it in the previous 12-months (Franks & Smith, 2020). With the results of the survey being mainly descriptive, the overall purpose of this article is to statistically scrutinize the 2019 survey results on identity crime and misuse in Australia to identify which characteristics increase one's likelihood of being victimised by identity theft. To accomplish this aim, the analysis will endeavour to answer three main questions:

1) Are they any demographic variables that are significantly associated with increased victimisation?
2) What is the relationship between the number of hours spent on a digital device and one's likelihood of being victimised by identity theft?
3) What is the relationship between the number of technologies used to prevent the misuse of personal information and one's likelihood of being victimised by identity theft?

To answer the first question, several demographic variables, such as gender, age, and Indigenous status, as well as education, and income levels will be statistically analysed alongside the prevalence of identity theft to identify who has an increased risk of victimisation. For questions two and three, following a similar conceptual framework to Cross (2017), the analysis fits within the context of the 'prudential citizen' (Walklate & Mythen, 2010), which in the context of identity theft, posits that a person is responsible for maintaining the integrity of their identity through protecting their personal data (Whitson and Haggerty, 2008; Monahan, 2009; Cross, 2017). Within this framework, the authors wish to demonstrate whether a prudential citizen, someone who is ensuring the integrity of their personal data, is more or less likely to be victimised by identity theft.

Background

Due to the increased use and availability of personal information, the ease of perpetrating identity-based crimes has also increased (Holt & Turner, 2012). These offenders can obtain personal information through 'low tech' and 'high tech' methods (Holt & Turner 2012, p. 309), including stealing personal information from mailboxes or through burglary and robbery, as well as through computers (or digital devices) and/or the Internet, respectively. With the widespread use of, and reliance on, the Internet, including social media, electronic banking, and online shopping, the latter method is becoming one of the most significant problems that have arose in the last 20 years because of the economic harm faced by the victims (Holt & Turner, 2012).

While identity theft is not a new crime, the magnitude of the problem has increased and it is now considered, according to Burnes, DeLiema, and Lynn (2020), a public health problem. This is because of the significant emotional and physical consequences of identity theft, including severe emotional distress, sleep problems, anxiety, irritation, depression, anger, worry, and a sense of vulnerability (Golladay & Holtfreter, 2017; Harrell, 2019; Sharp et al., 2004; Button et al. 2014), as well as increased hospitalisation and all-cause mortality rates in older adults (Burnett et al., 2016; Dong & Simon, 2013). Although not considered a violent crime, and sometimes even considered a 'victimless' crime, or a crime that causes no real harm (Copes et al. 2013), identity theft victims share many of the same consequences, however, the services available are not as comprehensive (Button et al. 2014).

To explain crime, Cohen and Felson's (1979) routine activity theory (RAT), which proposes that criminal opportunities arise through routine activities that bring suitable targets together

with motivated offenders in the absence of capable guardianship (Reyns & Henson, 2016), is often used. In essence, crime cannot happen without those three elements converging. Since its conception, some victimologists integrated both lifestyle-exposure theory and RAT, subsequently creating lifestyle-routine activity theory (L-RAT) which emphasizes the importance of lifestyles and routine activities in generating victimisation opportunities (Reyns & Henson, 2016). Although conventionally applied to criminal activities where the victim and offender have direct contact, it can also be used to explain criminal activities where the victim and offender do not physically, or even simultaneously, meet, such as cybercrime (Burnes et al., 2020). While generally considered a place-based theory, RAT (or L-RAT) can account for temporally disconnected crimes, as well as those that are long-distance (i.e., the victim and offender are not in the same physical space; Reyns and Henson 2016). When applied to identity theft, the temporal overlap to converge the motivated offender and suitable target in an absence of a capable guardian is lagged by a short (seconds or minutes) or long (hours or days) period of time (Reyns & Henson, 2016).

As such, research has identified a number of risk and protective factors, based on an individual's lifestyle and routine activities that can increase or decrease the likelihood of being victimised by high tech (computer-based) identity theft – see Table 1.

Table 1. Risk and protective factors associated with high tech victimisation.

Risk factors	
Age	Older adults have a higher likelihood of identity theft victimisation (Burnes et al., 2020; DeLiema et al., 2021; Zaeem et al., 2016; Irvin-Erickson, 2024). That being said, Irvin-Erickson (2024) also highlighted that the risk of identity fraud decreases for individuals aged 65 and over and that those aged 75 and over have a lower risk compared to other age groups (Anderson, 2006; Harrell & Langton, 2013) Individuals who are transitioning into adulthood can be more likely to experience identity theft, potentially because of the major financial decisions occurring at this time (Navarro & Higgins, 2017). Minors, those under the age of legal adulthood, can be at a greater risk of identity fraud because they have clean credit histories and limited control over their finances (Irvin-Erickson, 2024; FTC, 2011).
Socioeconomic status	Individuals with a higher socioeconomic status have more purchasing power and thus are more likely to be victims of identity theft (Reyns & Henson, 2016; Zaeem et al., 2016)
Cultural identity	Literature on the risk of identity theft and cultural identity is mixed; Zaeem et al. (2016) found that White respondents [with higher education] were more likely to be victims of identity theft whereas Reyns and Henson (2016) and Navarro and Higgins (2017) found that non-White and mixed-race respondents, respectively, had increased odds of being victimised.

Online banking and purchasing behaviours	Increased online purchasing and banking behaviours can increase identity theft victimisation (Reyns & Henson, 2016; Zaeem et al., 2016)
Participation in online deviance	Those who reported harassment or malicious software infection victimisation also reported online deviance (Bossler & Holt, 2009; Holt & Bossler, 2009). Increased software piracy can increase identity theft due to the constant downloading and files with an unknown origin (Choi, 2008; Holt & Bossler, 2009; Holt & Turner, 2012; Reyns & Henson, 2016). Increased hacker behaviours, such as guessing passwords, accessing personal devices, and viewing personal files increase cybercrime victimisation (Holt, 2007; Holt & Bossler, 2009). Increased perpetration of online harassment can lead to retaliatory identity-based attacks (Holt & Bossler, 2009).
Experiencing other forms of cybercrime, or previous identity theft	Holt and Turner (2012) hypothesized that those who have previously been a victim of cybercrime may have an increased chance of being victimised by identity theft. This was also discussed in Cross and Holt (2023). Victims of online harassment also victimised by identity-theft as a means of further harassment (Finn, 2004; Holt & Bossler, 2009). If previous cybercrime victimisation involved malicious software, a secondary offence could be identity-based crime (Chu et al., 2010; Holt & Lampke, 2010; Morris, 2010; Reyns & Henson, 2016). Victims of large data breaches, especially those where social security numbers were exposed, can be more likely to be subsequent victims of identity theft (Burnes et al., 2020; Cross, 2017; Reyns & Henson, 2016; Smyth 2014).
Protective factors	
Presence of protective software	Including anti-virus, ad-ware, and spyware programs; designed to reduce harmful malware from infecting computer, thus reducing potential of identity-theft victimisation (Choi, 2008; Holt & Turner, 2012; Mell et al., 2005; Taylor et al., 2010).
Presence of firewalls	Including hardware and software firewalls; hardware firewalls minimise likelihood of penetrating network defences and compromising individual computers (Nazario, 2004; Szor, 2005); software firewalls provide immediate alerts to possible malicious attacks (Turner and Holt 2012).
Knowledge of computer systems	Increased knowledge of computer systems can equate to a decreased likelihood of victimisation because a well-informed user can correctly identify malware infection-associated

	anomalies (Holt & Turner, 2012); greater likelihood of keeping protective softwares up-to-date (Choi, 2008; Furnell, 2003; Holt & Bossler, 2009; Mell et al., 2005; Szor, 2005; Taylor et al., 2010).
Knowledge of computer security	Greater awareness of online risks, such as opening suspicious emails or communicating with strangers can decrease odds of online victimisation, including identity theft (Choi, 2008; Holt & Bossler, 2009; Wolak et al., 2006; Zaeem et al., 2016).
Passwords	Keeping passwords private, using different passwords, and consistently changing passwords can decrease risk of online victimisation (Furnell, 2003; Nazario, 2004; Taylor et al., 2010; Zaeem et al., 2016).

Descriptive results of the 2019 AIC survey

The following section will briefly summarise the results of the 2019 AIC survey, to better inform the statistical analyses below. In 2018-2019, the (reported) economic impact was estimated to be three billion Australian dollars, with $583 million of that being used to combat identity crime and implement measures to strengthen identity security, such as biometrics (Franks & Smith, 2020). The lifetime victimisation rate, which was 25%, has remained steady since 2017; however, nearly 12% had their personal information misused in the last 12 months – a 5% increase from 2016/17 but a 0.1% decrease from 2018. Forty-eight percent reported that their personal information was misused on one occasion (up from forty-six percent in 2018) while twenty-two percent reported two separate occasions (down from twenty-three percent in 2018). Fifty-two percent of the respondents stated that their personal information was misused in multiple ways (up from forty-eight percent in 2018), with an average of six different ways of misuse being reported (up from the mean of two in 2018).

The total out-of-pocket losses increased by $1.5m between 2018 and 2019; however, this was mostly due to a single respondent who reported a one-million-dollar loss in 2019. The mean out-of-pocket loss was nearly $4,000 in 2019 (up from ~$2,000 in 2018), with the median being $300 (same as 2018). The amount of money recovered by victims in the last 12 months increased by $247,663 from 2018 to 2019 ($613,800 and $879,463, respectively), with the mean increase up by $400 ($817 in 2018 and $1,217 in 2019) and the median staying the same at $200 in the same time period (Franks & Smith, 2020).

Finally, the 2019 survey reports that the impact on the victims included tangible losses such as being refused credit (27.2% in 2018 and 20.4% in 2019), government benefits (14.7% in 2018 and 10% in 2019), and other services (2.4% in 2018 and 1.2% in 2019), experiencing financial difficulties (12.2% in 2018 and 12.3% in 2019), having to take legal action (11.8% in 2018 and 7.7% in 2019), and being wrongfully accused of a crime (10.3% in 2018 and 6.8% in 2019), to intangible losses, such as experiencing mental/emotional stress (13.8% in 2018 to 15.4% in 2019), physical health problems (6.0% in 2018 to 5.3% in 2019), and reputational changes (3.2% in 2018 and 2.0% in 2019). Other impacts include 'Other', decreasing from 8.5% in 2018 to 7.6% in 2019 and not experiencing any consequences at all, decreasing from 46.6% to 45.8% in the same time period.

Methods

As reported by Franks and Smith (2020), the 2019 data on the misuse of personal information in Australia used a quantitative and cross-sectional survey design, sampling a selection of residents (sampling frame = 10,000) from all states and territories across varying age groups (15-65+). The research design was consistent with the previous years' surveys. The survey hosting was provided by iLink Research Solutions who then provided raw de-identified data for analysis. The online questionnaire contained 40 closed- and open-response questions on the following, taken directly from Franks & Smith (2020, pp. 4-5):

- demographic and other characteristics of respondents including age, gender, usual place of
- residence, income, language spoken at home, Aboriginal and Torres Strait Islander status
- and computer usage;
- experience of misuse of personal information at any time in the past and over the
- preceding 12 months;
- method of victimisation on the most serious occasion in the preceding 12 months;
- actual financial losses, funds recovered and other consequences of victimisation;
- whether and how respondents reported misuse of personal information and their
- satisfaction with the responses;
- behavioural changes arising from the misuse of personal information;
- awareness of court-issued Victims' Certificates;
- perceived seriousness of misuse of personal information;
- perceived risk of identity crime over the next 12 months; and
- use of security measures in the past, including biometric technologies, and willingness to
- use them in the future to reduce the risk of identity crime victimisation.

To reflect the spread of the respondents across Australia, the data were weighted by age and gender using the demographic statistics from the Australian Bureau of Statistics (2019).

To accomplish the aims of this study, a secondary data analysis of the AIC's 2019 survey on identity theft (see Franks & Smith (2020) was conducted. Permission from the AIC was granted to re-examine the data and ethical clearance was obtained by UTS HREC (ETH22-6966).

The primary outcome variable of interest was the response to question 16: "Please indicate if you have had your personal information misused at any time in the past" , where the respondents could respond "Yes, I have had my personal information misused in the past" or "No, I have not have my personal information misused in the past" (Franks & Smith, 2020. pp. 58). From those responses, the following variables were re-examined and subject to univariate (Chi-squared test, two-sample t-test, and odds ratio) and multivariate (multiple variable logistic regression model) analyses:

- Gender (male, female);
- Age (17 and under, 18-24, 25-34, 35-44, 45-54, 55-64, 65 and over);
- Indigenous status (Aboriginal or Torres Strait Islander or both, No, Rather not say);
- Education (Associate degree, Bachelor's degree, high school, other/rather not say, postgraduate qualification);
- Income ($0-$18,200, $18,201-$37,000, $37,001-$80,000, $80,001-$180,000, $180,001 and over, Rather not say);
- Number of hours spent using a computer or computerised device;
- Number of technologies used in the past.

Additionally, relationships between the number of hours spent on a digital device as well as the number of technologies used to prevent the misuse of information, and the likelihood of being victimised were also investigated.

Results

The analysis began by examining the univariate associations between demographic characteristics (gender, age, Indigenous status, education level), income, number of hours spent on using a computer or computerised devices, and the number of technologies used in the past to prevent the misuse of personal information. For categorical variables (gender, age, Indigenous status, education, and income), the counts are presented in each category according to the binary responses to question 16 (yes or no), and a Chi-squared test of independence was used to obtain the p-values. For the continuous variables (number of hours spent using a computer or computerised devices and number of technologies used in the past), the means are presented, and the p-values were calculated using a two-sample t-test. For both types of variables, the odds ratio was also calculated. This data is presented in Table 2.

Table 2. Univariate associations of the misuse of personal information from the 2019 AIC survey on identity crime and misuse in Australia.

Variable	Yes	No	P-value	Odds ratio
Gender				
Male	1076	2974	0.002	Ref
Female	1383	4420		0.865*
Age				
17 years and under	4	17	<0.001	Ref
18-24	197	685		1.222
25-34	693	1562		1.886
35-44	590	1491		1.682
45-54	355	1117		1.351
55-64	275	1216		0.961
65 and over	345	1306		1.123
Indigenous status				
Aboriginal or Torres Strait Islander or both	205	168	<0.001	3.908*
No	2239	7170		Ref
Rather not say	15	56		0.858
Education				
Associate degree (advanced diploma, diploma, professional qualification without a degree, certificate III or IV)	766	2319	<0.001	Ref
Bachelor's degree	664	1728		1.179*
High school	523	2107		0.751*
Other/rather not say	22	98		0.672
Postgraduate qualification	484	1142		1.279*

Income				
$0-$18,200	300	1116	<0.001	Ref
$18,201-$37,000	526	1552		1.261*
$37,001-$80,000	789	2315		1.268*
$80,001-$180,000	614	1501		1.522*
$180,001 and over	79	185		1.589*
Rather not say	151	725		0.269*
Number of hours spent using a computer or computerised devices				
	38.03	35.52	<0.001	1.004*
Number of technologies used in the past				
	2.51	3.24	<0.001	1.342*

'Ref': Reference category for odds ratio calculation
* - denotes significance $p<0.05$

In total, the survey collected 9,968 responses; the majority of which being female (59%), aged 25-34 (23%), non-Indigenous (96%), with an Associate degree (31%), in the $37001-$80,000 income bracket (32%). Of the 25% (2459 respondents) that responded yes to having their personal data misused at any point in the past, 56% (1383 respondents) were female, 28% (693 respondents) were aged 25-34, 91% (2239 respondents) were non-Indigenous, 31% (766 respondents) had an Associate degree, and 32% (789 respondents) were in the $37,001-$80,000 income bracket. A total of 38.03 hours were spent using a computer/computerised device for those who selected yes, which was a statistically significant difference and a statistically significant odds ratio ($p<0.05$) from those who selected no.

The Chi-squared tests of independence (categorical variables) and the two-sample t-tests (continuous variables) resulted in statistically significant p values ($p < 0.01$) for each of the variables in Table 2, indicating that these variables are significantly associated with lifetime victimisation. Finally, the results of the odds ratio from univariate logistic regression models indicate that each of the variables that we considered is statistically significant. More specifically, the following factors are associated with a significant increase in the odds of having personal information misused: being male; self-identify as an Aboriginal or Torres Strait Islander; have a Bachelor degree or Postgraduate qualification (compared to an associate degree) and higher income. There was also a significant difference in the number of hours spent using a computer or computerised devices between those who had their personal information misused and those who had not: with each additional hour spent the odds of victimisation increases by 0.4%. A similar result is found for the number of technologies used in the past to prevent misuse of personal information: for each additional technology used the odds of victimisation increases by 34%.

The result of the multiple logistic regression model is given in Table 3. Many of the variables identified as having significant association with lifetime victimisation ceased to be statistically significant in the joint model. Variables that are significantly associated with increased odds of victimisation include: self-identify as Aboriginal or Torres Strait Islander; income bracket $18,201-$37,000 (as compared to the reference $0-$18,201), and a greater number of technologies used in the past to prevent misuse. On the other hand, significantly lower odds of victimisation were estimated for those who have high school qualification (compared to those who had an associate degree) and those who choose not to disclose their income.

Table 3: Multivariable logistic regression model.

Variable	Odds ratio	P-value
Gender		
Male	Ref	
Female	0.951	0.320
Age		
17 years and under	Ref	
18-24	0.921	0.887
25-34	1.367	0.586
35-44	1.343	0.608
45-54	1.314	0.635
55-64	1.041	0.944
65 and over	1.299	0.649
Indigenous status		
Aboriginal or Torres Strait Islander of both	2.603	<0.001*
No	Ref	
Rather not say	0.834	0.548
Education		
Associate degree	Ref	
Bachelor's degree	0.997	0.961
High school	0.828	0.005*
Other/rather not say	0.873	0.578
Postgraduate qualification	1.047	0.530
Income		
$0-$18,200	Ref	
$18,201-$37,000	1.196	0.036*
$37,001-$80,000	1.018	0.823
$80,001-$180,000	1.015	0.870
$180,001 and over	0.864	0.372
Rather not say	0.759	0.015*
Number of hours spent using a computer or computerised devices	1.001	0.222
Number of technologies used in the past	1.291	<0.001*

* - denotes significance p<0.05

Since the number of technologies used in the past was a significant predictor for lifetime victimisation, a closer look was taken at each individual technology used. This is question 10 of the survey "Have you ever used any of the following technologies in the past? (in any way, not just to prevent misuse of personal information) (Select all that apply)" (Franks & Smith, 2020. pp. 56)." For each of the technologies listed, the proportion of respondents who reported

lifetime victimisation are presented in Table 4. For instance, 25.1% of those who used password protection reported victimisation and 24.2% of those who have not used password reported victimisation. This difference in proportion was not statistically significant when assessed using the test of proportions (p-values presented in last column of Table 4). However, we found for the other six technologies, significantly lower proportions of victimisation were found among those who have not utilised them in the past.

Table 4: proportions of respondents who reported lifetime victimisation for each of the technologies listed in question 10*.

Technologies	**Yes**	**No**	**P-value**
Password	0.251	0.242	0.657
Signatures	0.291	0.193	<0.001**
Voice recognition	0.368	0.214	<0.001**
Fingerprint recognition	0.298	0.203	<0.001**
Facial recognition	0.338	0.220	<0.001**
Iris recognition	0.437	0.227	<0.001**
Computer chip implanted under your own skin (no pets or devices)	0.555	0.229	<0.001**

*Question 10 states: "Have you ever used any of the following technologies in the past (in any way, not just to prevent misuse of personal information) (Select all that apply)" (Franks and Smith 2020, pp. 56). ** - denotes significance p<0.05

Discussion

The aim of this study was to statistically scrutinize the AIC's 2019 information misuse survey data to identify any statistically significant variables that increase the likelihood of identity theft victimisation. More specifically, the research set out to answer three research questions, including 1) if any demographic variables contributed to increased victimisation, 2) whether there was a relationship between the number of hours on a computerised device and in increased chance of victimisation, and 3) whether there was a relationship between the number of protective technologies and an increased chance of identity theft victimisation.

As shown in Table 2, each of the variables, including gender, age, Indigenous status, education, and income when subject to univariate statistical tests, were statistically significant indicators of victimisation. However, when analysed together using a multiple variable logistic regression model (see table 3), only identifying as Aboriginal and Torres Strait Islander or both, having an income of $18,201-$37,000, and the number of technologies used in the past were still statistically significant indicators of future identity theft victimisation. The decrease in the number of demographic variables statistically associated with identity theft victimisation when analysed together versus separately, is in line with the works by Cross and Holt (2023) who also found a lack of demographic variables in determining victimisation. Although their study investigated romance fraud, there are still aspects of identity theft involved.

Similar to the demographic variables, and in response to the second research question, although the univariate analysis demonstrated that the number of hours spent on a computerised device was a statistically significant contributor to victimisation, when analysed using a regression model, the variable was found to no longer be significant.

Perhaps one of the most interesting findings from this secondary analysis was that the chances of identity theft victimisation increase when respondents who had experienced previous identity theft used technologies designed to increase data security, such as those listed in Table 4. Except for the use of passwords, the use of signatures, voice-, fingerprint-, facial-, and iris recognition, and implanted computer chips demonstrated a statistically significant difference between those who had used them and those who had not (all of which had been previously victimised by identity theft). This finding is unexpected as the purpose of employing multiple protective technologies would be to decrease the likelihood of victimisation. It is also contradictory to the 2019 survey findings on behavioural changes due to previous identity theft. 46% of the respondents who had been victimised reported to be more careful when using/sharing personal information (statistically significant increase from 2018) and an increased use of better security for computers/computerised devices (Franks & Smith, 2020).

The reason behind the relationship between an increased number of technologies used and an increased likelihood of victimisation is yet unclear, however, there are some explanations that can be offered. First, those who use (multiple) protective measures might be already at higher risk of identity theft because of their profession, finance, social status, etc, so they might be more targeted. Second, those who use protective measures might have been victims of identity theft in the past. This is in line with Burnes et al. (2020), who found that individuals who were previously victimised by identity fraud are more likely to be victimised later. Third, those who use protective measures might be less vigilant and less cautious about other digital behaviour, whilst fourth, the technologies in use may have their limitations. However, it is important to note such observations are not clear, reflecting aspects of victimological scholarship around the indicators of victimisation to non-cyber-related crime, with the most significant predictor of victimisation is previous victimisation (Farrell, 1992). In this context, no matter how many security technologies are used by those who have been previously victimised by cybercrime, they still have a higher likelihood of subsequent identity theft victimisation.

In line with Cross (2017), this finding, within the presented conceptual framework of people being prudential citizens, could indicate that the increased victimisation after using protective technologies is more of a misguided belief of the perceived benefits of using such technologies (and thus a misguided belief of the perceived risks of identity crime) rather than a deliberate act to share identifying information. Although not a direct rejection of prudentialism, these findings indicate that other theoretical frameworks, such as L-RAT, have more of an influence on one's chances of victimisation, and re-victimisation. Perhaps, the risk of (re)victimisation is simply linked to spending time online where motivated offenders are, especially now that many vital tasks that involve personally identifying information is done online (banking, shopping, etc…).

Other interesting findings in the study include that those who fell within the income bracket of $18,201-$37,000 were significantly associated with increased odds of victimisation (when compared to the reference brackets which was $0-$18,201) which was contradictory to what was found in an American (Zaeem et al., 2016) and Canadian (Reyns & Henson, 2016) population where those with a higher income are more likely to be victimised. Additionally, those who have a high school qualification (compared to those with an associate degree) and those who did not disclose their income had significantly lower odds of victimisation. While no concrete reasoning can be drawn by this, the analysis of more recent survey data should be used to corroborate as a trend or indicate that it was a one-time anomaly.

The increased victimisation of those who identify as Aboriginal or Torres Strait Islander or both is not well documented in the literature. As shown above in Table 1, Reyns and Henson (2016) and Navarro and Higgins (2017) found that non-White and/or mixed race respondents are more likely to be victimised, however, it does not specifically mention Indigenous status. Additionally, Burnes et al. (2020) found that those who identified as Asian American/Pacific Islander/American Indian/Alaskan Native were statistically associated with being victimised using personal information from existing credit/bank accounts. This would be an important avenue to continue to investigate as Indigenous Peoples are already overrepresented in the criminal justice system (Cunneen & Tauri, 2019) and according to Stubbs (2011) while referring to Indigenous women, "Over-represented but rarely acknowledged" (pp. 18).

As only the 2019 data was re-examined, future research should statistically scrutinise the findings of the more recent surveys to identify if the use of more technologies continues to increase identity theft victimisation. In light of this finding, however, prevention programs focusing on reducing first-time victimisation to identity theft may be more beneficial than those focusing on reducing subsequent victimisation. The results of this research have also identified that a portion of the Australian government's resources allotted to identity theft prevention should go directly into programs for those who identity as Aboriginal or Torres Strait Islander or both.

The impact of identity theft, reported in dollars lost or in the severity and/or length of the emotional or physical consequences, is often underrepresented. In fact, almost 60% of the respondents in the 2019 AIC survey only reported the crime to a family member or friend and almost 10% did not report to anyone (Franks & Smith, 2020). These high under-reporting rates can be attributed to the complexity in reporting, as well as victim blaming/shaming (Franks & Smith, 2020; Smith & Franks, 2020). Unfortunately, the complex reporting system, which relies on the individual victims' performance of 45 out of the 67 tasks necessary to detect, dispute, protect, and correct their compromised identities, only exacerbates the emotional and physical consequences (Franks & Smith, 2020; Wyre et al., 2020). Out of those who did report, satisfaction was highest when reported to IDCARE (not-for-profit organisation that supports victims of identity theft) or to a bank/credit card company; however, regardless of who they reported to, victims felt the most satisfied when they felt as though they were being listened to, if the person they reported to showed empathy, and if no resolution was reached, the person they reported it to was able to provide them with next steps or advice about avoiding revictimization (Franks & Smith, 2020). These findings support those by Irvin-Erickson (2024), who published a systematic review of the empirical research on identity fraud victimisation in the US, which found that a trauma-informed approach to victim services could have a positive impact on the victims' experience. Unfortunately, as Button et al. (2014) point out, the services for victims of identity theft are not as comprehensive and therefore studies such as this one, and the numerous others in the field, can be used by governmental bodies to support the need for more, improved, and trauma-informed services for victims.

A clear limitation of the current research is the reliance on a 2019 dataset, yet despite this, the findings presented through this research are still important. They are important to report as they identify a potential over-reliance or a misrepresented confidence in protective technologies, and the findings also act as support for governmental bodies to increase the support services available to victims of identity crime. As a consequence, the results yielded

from this study support further research in conjunction with more recent data obtained by the AIC in the area of identity theft.

Conclusion

Since the proliferation of the internet and an increased ease in sharing personal information, identity theft has become one of Australia's most prevalent crime-types that has lasting financial, emotional, and psychological impacts on the victims. In an effort to quantify the prevalence of identity theft so that proper awareness and prevention can be put in place, the AIC conducts a (almost) yearly survey to accurately capture its extent and the impacts on Australian residents. As the results of the surveys are primarily descriptive, this research further analysed the 2019 survey results which found that those who identify as Aboriginal and Torres Strait Islander or both, those who fell within the $18,201-$37,000 income bracket, and those that use an increased number of security-oriented technologies are significant indicators of subsequent victimisation.

Through a prudentialism framework, the findings of this secondary research demonstrate that someone who has been previously victimised by identity theft who then turns to protective technologies may have a misguided belief of the perceived risks of re-victimisation and a potential over-reliance on its abilities to keep data safe. This is supported by the 2019 survey results which reported that those who had been victimised reported (self-report) a change in their online and information sharing behaviours, such as being more careful.

As the methods of this study only analysed the 2019 data, it would be important to replicate the study on the more recent survey findings to see if the above trends continue. Ultimately, this information can be used to better guide and implement evidence-based prevention plans that can not only decrease the vast financial burden of identity theft on Australia as a nation, and to each of the victims, but also to decrease the emotional, psychological, and physical burdens of identity theft, a crime that, according to Burnes, DeLiema, and Lynn (2020), is now considered a public health problem. In addition, the results of this research can be used to guide the creation or amelioration of the services available to victims of identity theft as well as to implement education-based resources around the (potential) limitations of relying solely on protective technologies.

Acknowledgements: The authors would like to acknowledge the AIC and giving us permission to re-examine the 2019 survey data. The authors would also like to acknowledge the funding sources that made this research possible.

References

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, 25(2), 160–171

Australian Bureau of Statistics. (2019). *Australian demographic statistics, Jun 2019*. ABS.

Australian Institute of Criminology (AIC). (n.d.). *Identity Crime and Misuse*. https://www.aic.gov.au/statistics/identity-crime-and-misuse. Accessed 22 Mar 2024.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive medicine reports*, *17*, 101058.

Burnett, J., Jackson, S. L., Sinha, A. K., Aschenbrenner, A. R., Murphy, K. P., Xia, R., & Diamond, P. M. (2016). Five-year all-cause mortality rates across five categories of substantiated elder abuse occurring in the community. *Journal of elder abuse & neglect*, *28*(2), 59-75.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*, 36-54.

Choi, K.-s. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1).

Chu, B., Holt, T. J., & Ahn, G. J. (2010). Examining the creation, distribution, and function of malware on-line. *Department of Justice Abstract*, 1-183.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *44*(4), 588-608. https://doi.org/10.2307/2094589

Copes, H., Vieraitis, L. M., Cardwell, S. M., & Vasquez, A. (2013). Accounting for identity theft: The roles of lifestyle and enactment. *Journal of Contemporary Criminal Justice*, *29*(3), 351-368.

Cross, C. (2017). But I've never sent them any personal details apart from my driver's licence number …': Exploring seniors' attitudes towards identity crime. *Security Journal*, 30, 74-88. https://doi.org/10.1057/sj.2015.23.

Cross, C., & Holt, T.J. (2023) More than Money: Examining the Potential Exposure of Romance Fraud Victims to Identity Crime. *Global Crime*, 24:2, 107-121. https://doi.org/10.1080/17440572.2023.2185607.

Cross, C., & Layt, R. (2022). "I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. *Social Science Computer Revieiw*, 40(4), 955-973. https://doi.org/10.1177/0894439321999311.

Cunneen, C., & Tauri, J. M. (2019). Indigenous peoples, criminology, and criminal justice. *Annual Review of Criminology*, *2*, 359-381.

DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, *5*(4), igab043.

Dong, X., & Simon, M. A. (2013). Elder abuse as a risk factor for hospitalization in older persons. *JAMA internal medicine*, *173*(10), 911-917.

Farrell, G. (1992). Multiple victimisation: Its extent and significance. *International Review of Victimology*, *2*(2), 85-102.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal violence*, *19*(4), 468-483.

Franks, C., & Smith, R. (2020). *Identity crime and misuse in Australia: Results of the 2019 online survey* (Statistical Report no. 27, Issue.

Federal Trade Commission (FTC). (2011). Stolen futures: A forum on child identity theft. https://www.ftc.gov/news- events/events- calendar/2011/ 07/stolen- futuresforum- child-identity- theft. Accessed 16 Oct 2024.

Furnell, S. (2003). Cybercrime: vandalizing the information society. International conference on web engineering,

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741-760.

Harrell, E. (2019). *Victims of Identity Theft, 2016*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://bjs.ojp.gov/library/publications/victims-identity-theft-2016. Accessed 16 Oct 2024.

Harrell, E., & Langton, L. (2013). *Victims of identity theft, 2012*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https:// bjs.ojp.gov/content/pub/pdf/vit12.pdf. Accessed 16 Oct 2024.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171-198.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, *33*(4), 308-323.

Irvin-Erickson, Y. (2024). Identity fraud victimization: a critical review of the literature of the past two decades. *Crime Science*, *13*(1), 3.

Koops, B. J., & Leenes, R. E. (2006). ID theft, ID fraud and/or ID-related crime-definitions matter. *Datenschutz und Datensicherheit*, *30*(9), 553-556.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, *41*(10), 1027-1038. https://doi.org/https://doi.org/10.1016/j.telpol.2017.09.003

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling*. US Department of Commerce, Technology Administration, National Institute of ….

Monahan, T. (2009) Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology* 13(2): 155–176.

Morris, R. G. (2010). Identity thieves and levels of sophistication: Findings from a national probability sample of American newspaper articles 1995–2005. *Deviant Behavior*, *31*(2), 184-207.

Navarro, J. C., & Higgins, G. E. (2017). Familial identity theft. *American Journal of Criminal Justice*, *42*, 218-230.

Nazario, J. (2004). *Defense and detection strategies against Internet worms*. Artech House.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

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), 1-6.

Smith, R., & Franks, C. (2020). *Counting the costs of identity crime and misuse in Australia, 2018-2019* (Statistical Report, Issue.

Smyth, S. (2014) The greening of Canadian cyber laws: What environmental law can teach and cyber law can learn. *International Journal of Cyber Criminology* 8(2): 111–155.

Stubbs, J. (2011). Indigenous women in Australian criminal justice: Over-represented but rarely acknowledged. *Australian Indigenous Law Review*, *15*(1), 47-63.

Szor, P. (2005). *Art of Computer Virus Research and Defense, The, Portable Documents*. Pearson Education.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2010). *Digital crime and digital terrorism*. Prentice Hall Press.

Walklate, S., & Mythen, G. (2010). Agency, reflexivity and risk: cosmopolitan, neurotic or prudential citizen. *The British Journal of Sociology*, 61(1), 45-62.

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

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006). Online Victimization of Youth: Five Years Later.

Wyre, M., Lacey, D., & Allan, K. (2020). *The identity theft response system* (Trends & issues in crime and justice, Issue.

Zaeem, R. N., Manoharan, M., & Barber, K. S. (2016). Risk kit: Highlighting vulnerable identity assets for specific age groups. 2016 European Intelligence and Security Informatics Conference (EISIC),

Rejoinder: JCRPP-08-2024-0056 entitled "Investigating identity crime and misuse in Australia: The role of prevention technologies and the likelihood of victimisation"

Reviewer Comments	Response
R1	
There are a number of studies that have covered this - not currently cited that the authors could look at: **Definition:** Koops, B. J., & Leenes, R. E. (2006). ID theft, ID fraud and/or ID-related crime-definitions matter. Datenschutz und Datensicherheit, 30(9), 553-556. **Types:** Irvin-Erickson, Y. (2024). Identity fraud victimization: a critical review of the literature of the past two decades. Crime Science, 13(1), 3. **Impact of identity fraud:** Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27, 36-54. **Copes has written extensively and here is one example:** Copes, H., Vieraitis, L. M., Cardwell, S. M., & Vasquez, A. (2013). Accounting for identity theft: The roles of lifestyle and enactment. Journal of Contemporary Criminal Justice, 29(3), 351-368.	These references have been included.
Are there any broader Australian stats to set the context of trends in this area in Australia too?	The current study had access to only the 2019 survey. The reliance on the 2019 data is set out as a limitation in the paper and one that can prompt future research.
I thought more could be said on limitations of this type of study.	The limitations have been reflected on in the discussion and conclusion when reflecting on implications for future research/directions.
I felt some could be discussed more either in this section or the discussion to offer some more context to the implications and explain possible reasons for the results.	Further reflections have been added to the discussion. We have been, however, mindful of the word count and the key message the paper is seeking to offer.

R2	
There is also a need to tackle head-on why you have based the article solely on analysis of data from AIC 2019 when you acknowledges that subsequent data is available. It may simply be that further work is planned but if this is the case then that needs to be stated in the article otherwise the reader could be left with the suspicion that this unexpected finding is some sort of anomaly.	This has been addressed – see comment above re: contextualising the study.
I feel that you could have made more of this in the article both in terms of engagement with literature that conflicts with this finding and in pulling out the implications. In particular, you might want to be a little more specific about the potential impact of the research beyond saying that it could influence evidence-based protection plans. What, specifically, might happen as a consequence of the research?	The literature has been developed, being mindful of the word count. The implications of the study have been developed in the latter stages of the article, as well as explicitly stated in the conclusion.
The article has publishable potential but there are two things which give rise to reservations about its readiness for publication. Firstly, the discussion around the finding that victims who increased security behaviours were at a greater risk subsequent victimisation was fine as far as it went but it needed to go further. This is a significant finding and it needed to be more visible and explored in greater detail. In particular, greater engagement with the literature the goes against this finding is needed and an expansion of the speculation around explanations for why increased security increases risk is needed. There is some comment on this but it feels lacking in depth given the potential significance of the finding.	It has been explicitly stated in the discussion that a clear limitation of this article is the sole reliance on the 2019 data. Despite this, the authors feel (and have discussed) that the results are still important for publication, if only to be used as a spring-board for future research projects that look at the more recent data. This is a new finding and is presented in the paper. This point is an implication for future research.

Secondly and more significantly, the paper is based upon data from AIC 2019. The author acknowledges that there is more recent data which could be analysed to see if the trends noted in the article are continue. This is not done and there is no explanation of why it is not done. Readers might legitimately wonder why an article published in 2024 is based upon five-year old data when more recent data is available and its analysis has been flagged as necessary. At the very least, some explanation of why that has not yet been done is needed. If this article is one of a series of papers then that needs to be stated.	As noted above, the data presented in this paper is based on access to data from the 2019 study. This has been addressed in the paper and used a direction for future research. The two points noted by the reviewer don't detract from the paper's contribution, but provides scope for further research.