Consultation Draft – *Criminal Law Consolidation (Identity Theft) Amendment Bill 2003*

Submission by the Australian Privacy Foundation

written by Jeremy Douglas-Stewart

June 2003

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For information about the Foundation and the Charter, see www.privacy.org.au.

Introduction

As indicated in the Government's media release on 25 February 2003, the proposed identity theft offences are targeted primarily at preventing the use of information for purposes such as fraud, money laundering, drug trafficking, illegal immigration and terrorism.

The Australian Privacy Foundation encourages the Government to broaden the objects of the proposed legislation to encompass not only providing protection against the financial and social costs and security risks that mis-use of individuals' personal information poses but also providing protection against the invasions of privacy that result from such mis-use.

Protection of individuals' privacy is important in view of the fact that privacy has now become an important social value that the public expects to be protected, as has been reflected by the rapid increase in privacy legislation in most jurisdictions around Australia in recent years.

This submission looks at, firstly, whether the proposed laws are necessary in view of existing offences, and, secondly, assuming that such laws are necessary, how they could be

structured to ensure that they appropriately address the privacy issues associated with identity theft.

Privacy guidelines & principles relevant to Australia

The Organisation for Economic Cooperation and Development Guidelines ("OECD Guidelines") governing the protection of privacy and transborder flows of personal data were adopted in Paris in 1980. The Guidelines have formed the basis of privacy legislation in most industrialised nations, including Australia's *Privacy Act 1988* (Cth), and comprise eight principles relating to the collection, use, accuracy, security and disclosure of personal information as well as rights of access and correction.

The Australian Privacy Charter[1] ("Charter"), developed by the Australian Privacy Charter Council under the chairmanship of Justice Michael Kirby in December 1994, provides a benchmark against which the adequacy of legislation may be measured. The Charter sets out 18 principles relating to all categories of privacy rights and is intended to inform Australians of the level of privacy that they are entitled to expect and see observed.

As identity theft involves the use by a perpetrator of a victim's personal information, the establishment of the relevant offences should be in accordance with the OECD Guidelines and the principles set out in the Charter.

To what extent is there a need for the legislation?

While the Foundation supports protection against identity theft, it is concerned that there is already in existence a significant body of legislation in all Australian jurisdictions[2] that establishes varying crimes under which identity related offences may be prosecuted. In particular, sections 134 (theft and receiving), 139 (deception) and 140 (dishonest dealing with documents) of the *Criminal Law Consolidation Act 1935* (S.A.) are wide enough to cover many of the types of activities targeted by the proposed legislation.

In order to avoid unnecessary and confusing overlap with existing laws and increasing the already high level of difficulty and resources required to successfully prosecute identity theft offences (owing, for example, to the fact that offences are often multi-

1. The Charter is available at www.privacy.org.au.
2. For example – Commonwealth: *Criminal Code Act 1995* ss.134.1 (obtaining property by deception), 134.2 (obtaining financial advantage by deception), 135.1 (general dishonesty), 135.2 (obtaining financial advantage) and 135.4 (conspiracy to defraud); A.C.T. – *Crimes Act 1900* ss.89 (theft), 95 (obtaining financial advantage by deception) and 124-128 (making and using false instruments); N.S.W. – *Crimes Act 1900* ss.178A (fraudulent misappropriation), 178BA (obtaining money etc. by deception), 178BB (obtaining money by false or misleading statements), 178C (obtaining credit by fraud), 179 (false pretences), 184 (fraudulent personation) and 250 (forging and uttering); N.T. – Criminal Code ss.210 (stealing), 227 (criminal deception), 258 (forgery), 260-261 (uttering) and 276B-C (unlawfully accessing and modifying data); Qld. – Criminal Code ss.398 (stealing), 408 (misappropriation), 408C (fraud), 441 (fraudulent falsification of records), 488 (forgery and uttering); S.A. – *Criminal Law Consolidation Act 1935* ss.131 (larceny), 195 (false pretences), 204 (false impersonation), 204 (impersonation) and 234 (forgery); Tas. – *Criminal Code Act 1924* ss.228-234 (stealing), 250-251 (false pretences), 252A (dishonestly acquiring financial advantage), 253-255 (fraud), 257E (inserting false information on data); Vic. – *Crimes Act 1958* ss.81 (obtaining property by deception), 82 (obtaining financial advantage by deception) and 83A (falsification of documents); W.A. – Criminal Code ss.378 (stealing), 409 (fraud), 473 (forgery and uttering) and 474 (preparation for forgery).

jurisdictional, electronic equipment used renders evidence difficult to access and relevant laws around Australia are not harmonised), a comprehensive review of relevant existing offences in both South Australia and other Australian jurisdictions is necessary in order to identify:

- existing offences that cover the targeted conduct; and
- the areas in which such offences are inadequate to enable the investigation and prosecution of such conduct.

The Foundation is not convinced that sufficient research has been undertaken in this area to justify the conclusion that there is a need for the type of broad offences proposed or that they will offer greater protection for individuals against identity theft.

The remainder of this submission applies to the extent that identity theft laws are necessary in South Australia.

Content of offences

As identity theft inherently involves an invasion of the victim's privacy, a primary objective of the proposed offences, in addition to protecting against and penalising fraudulent and other illegal activities, should be to protect an individual's right to privacy.

In order to do this, it is necessary to ensure that the proposed offences apply regardless of whether the intended offences relate to "identity fraud" or "identity theft".

Identity fraud vs. identity theft

"Identity fraud" refers to where a perpetrator uses another person's personal information under that person's name (usually credit card details or other financial information) on a limited number of occasions and in a single context (for example, to commit credit card fraud) for material gain.

In contrast, "identity theft" refers to where a perpetrator uses another person's personal information on numerous occasions to masquerade as that person over an extended period of time to commit various acts in more than one context (as occurred in the relatively recent and much publicised case of Mr Derek Bond, the 72 yr old Englishman detained in South Africa after an offender had used Mr Bond's identity since 1989 to commit various crimes), whether or not such acts are for material gain. Identity theft compromises the victim's identity in a much more serious manner than identity fraud, as the victim's personal reputation is affected by the offender's actions. The damage is not easily reversed owing to the difficulty in identifying, locating and correcting records that relate to acts or crimes committed months or years earlier by the perpetrator.

Ensuring offences address both identity fraud & identity theft

In the United States, where the U.S. Federal Government and all but three U.S. State Governments have passed laws establishing identity related offences[3], many of those laws only address the issue of identity fraud and do not address the issue of identity theft (despite the fact that the names of the offences purport to address the latter). As such, those offences only directly penalise fraud and, consequently, interferences with privacy are only indirectly penalised in the cases where fraud is proved.

The proposed legislation should not repeat the flaws in the U.S. statutes and should ensure that each of the proposed offences applies irrespective of whether they are committed in pursuance of identity fraud or identity theft.

The Foundation notes that the proposed Part 5A of the Act protects against identity theft to the extent that, in relation to the "serious criminal offence" that an offender must be intending to commit, there is no distinction between serious offences in which financial gain will be obtained and serious offences in which such gain will not be obtained.

Exemptions

The Foundation supports the inclusion of the proposed exemptions under s.144E to reflect the fact, and to provide re-assurances to the public, that less serious forms of misrepresentations of identity are not targeted by the legislation.

However, the provisions under s.144E do not go far enough and should specify a broader range of exemptions and circumstances in which the Act shall not be deemed to apply. These exemptions and circumstances should include:

- authors writing under a pseudonym (it was indicated in the Government's media release of 25 February 2003 that this would be included in the bill);

- situations in which persons of all ages (and not just minors) may seek to misrepresent their age but which do not constitute serious offences, for example, where a person specifies a lower age when signing up at a dating agency or where a junior athlete seeks to compete in an age category for which he or she is too old;

- legitimate circumstances in which a person may choose to adopt a fictitious identity in order not to reveal his or her identity, for example, when communicating with strangers on the internet or, where appropriate, when desiring to deal with an organisation anonymously (as permitted under National Privacy Principle ("NPP") 8 of the *Privacy Act 1988* (Cth)); and

- the testing of security systems that have been put in place to protect against identity fraud and identity theft. Similar provisions exist under the Revised Washington Code (see s.9.35.010(4)(a)) (however, that Code extends exemptions to financial

3. A list of links to all U.S. Federal and State anti-identity theft laws is available at www.consumer.gov/idtheft.

institutions that are investigating alleged employee misconduct or negligence or are attempting to recover information obtained by a fraudster. The Foundation does not support the inclusion of these exemptions as there appears to be little justification for such institutions assuming a false identity for those purposes and carries with it a significant risk that such a privilege may be abused).

Jurisdiction

Given the ease with which offences may be committed outside South Australia using the personal identifying information of a South Australian, the Government should ensure that the courts are afforded appropriate jurisdiction over offences relating to a victim residing within South Australia regardless of whether the relevant act or crime was committed within or outside South Australia.

A provision to this effect is included in the Revised Code of Washington (see s.9.35.020(4)) which provides that:

> *…the crime will be considered to have been committed in any locality where the person whose means of identification or financial information was appropriated resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in that locality.*

Assisting victims

Given the severe damage that can be caused to a victim's reputation, the proposed legislation should, in addition to establishing relevant offences, make appropriate provision that empower victims to combat identity fraud and identity theft and to re-establish their identities.

Database of victims

A database of victims of identity fraud and of the acts or crimes that have been carried out in their name to which victims and their authorised representatives have access via a toll-free telephone information line should be established. The purpose of such a database would be to enable victims to easily prove to other persons that they have been the victims of identity theft and that certain acts or crimes were not committed by them. A toll-free line would mean that there would be no cost to third parties to verify a claim by a victim that they have been a victim of identity theft. If other jurisdictions enact similar legislation, this could lead to the formation of a national database.

A similar database has been provided for under the Californian Penal Code (see s.530.7).

Right to factual finding of innocence

Victims of identity theft should be entitled to petition a court to make a factual finding of innocence in relation to crimes that have been committed, or are alleged to have been committed, in his or her name or where his or her name has been mistakenly associated with a record of a criminal conviction. Such a right will enable a victim to establish that an allegation, arrest or conviction does not relate to him or her.

Provisions of this type are contained within the Californian Penal Code (see s.530.6(b)).

Correction of documents

It is imperative that victims are empowered to correct information relating to acts or crimes that have been carried out in their name but in relation to which they have had no involvement. This is an essential part of assisting victims to re-establish their identities and is a fundamental tenet of information privacy rights.

Upon finding an accused guilty of a crime that has been committed in another's name, the sentencing court should be required to ensure that its relevant public records indicate the victim's innocence and to order that any other relevant public record of which it is aware be amended to indicate the victim's innocence. Provisions similar to these are provided for under the Californian Penal Code (see s.530.5(c)) and the Revised Washington Code (see s.9.35.020(6)) respectively (although the latter merely gives the court a discretion to order such an amendment).

Similarly, the proposed legislation should require, upon request by the victim, any person, entity or agency (in either the private or State public sector) holding incorrect information relating to a relevant act or crime entered into by the perpetrator to amend the information to indicate the victim's innocence or lack of involvement.

In relation to the public sector, an agency is already required to provide an individual with access to his or her information in accordance with Freedom of Information legislation. Further, an agency is likely to amend incorrect information as Information Privacy Principle 6 ("IPP 6") of *Cabinet Administrative Instruction No.1 of 1989*[4] provides that an agency "should" correct inaccurate information. However, as IPP 6 does not give a victim a right to demand a correction, victims should be given a statutory right to do so by the proposed legislation.

In relation to the private sector, a victim already has a statutory right to demand of most organisations that they provide access to and correct inaccurate information pursuant to NPP 6 of the *Privacy Act 1988* (Cth). However, such rights do not exist in relation to private sector entities that are not bound by the Act. Consequently, the proposed legislation should require entities that are not bound by the Act to comply with NPP 6 to the extent that any request relates to information they hold regarding relevant acts or crimes carried out by the offender.

4. The administrative instruction is available at www.archives.sa.gov.au.

In the United States, similar laws are reported to have been put in place by the Federal *Identity Theft Victims Assistance Act of 2002* which is intended, among other things, to facilitate a victim's correction of false records[5].

Excessively broad provisions

The Foundation is concerned that the offences have been drafted in excessively broad terms. Generally, each proposed offence describes a very broad category of conduct that could be committed in numerous circumstances. The only limitation on criminal liability for the conduct is the requirement that it be carried out with the intent of committing a criminal offence. For example, if it were not for the requirement under proposed s.144C that a person intends his or her conduct to be in pursuance of a serious criminal offence, nearly every citizen would at some stage be caught by that section as it is not uncommon to use another person's personal information at one stage or another, for example, to withdraw funds from a spouse's bank account using an ATM card and pin number or to use a spouse's credit card details to purchase a product over the telephone.

Similarly, the circumstances that are proposed to constitute a "false pretence" under s.144B(b) are very wide, particularly those under sub-section (ii) (falsely pretending "to have, or to be entitled to act in, a particular capacity"). For example, in view of the very large number of job titles that exist today and the fact that many job descriptions are so general and non-descriptive that they do not always reveal the nature of the job or qualification, there is a very broad scope for a person to be accused of mis-representing his or her job title and of making a "false pretence", such as where a "junior assistant" describes his or her role as "an executive assistant". The term "false pretence" is defined so broadly that this type of mis-representation would be deemed to be a false pretence to which the section applies.

As the purpose of criminal law is to proscribe certain types of conduct, it is preferable not to draft criminal offences in such broad terms. Rather than describing a very broad category of conduct that will constitute the physical elements of the offence and limiting its application by requiring a specific mental element, the proscribed conduct should itself also be specific. In the case of proposed s.144C, for example, rather than the requisite conduct being the "use of another person's personal identification information", specific ways in which the information must be being used could be specified, such as the "use of another person's personal identification information in the process of creating a fake identity card".

We note that this approach of specifying specific elements has been taken in defining the meaning of "personal identification information".

Specifying the specific purposes will not in any way affect a main object of the Act which is to empower police to investigate and prosecute a suspected offence before the relevant information is actually used for the offence.

5. See under "Keep Informed About ID Theft and Fraud Legislation" at www.fightidentitytheft.com.

Limitation on excessive police powers

The result of drafting broad criminal offences is to afford police a very high level of discretion regarding the exercise of their powers of investigation and prosecution. If the police are afforded such a high level of discretion, an appropriately high level of suspicion should be required before they are able to exercise their powers in order to protect individuals from unnecessary interferences by police.

Consistency with existing information privacy laws

The proposed legislation should be consistent with existing Commonwealth information privacy laws, for example the *Privacy Act 1988* (Cth), including its NPPs, credit reporting provisions (for example, ss.18S and 18T relating to unauthorised and fraudulent access to credit information) and tax file number provisions, and the *Taxation Administration Act 1953* (for example, s.8WB relating to prohibitions on recording tax file numbers and using them in connection with the person's identity).

Conclusion

The Foundation is cautious about the need for legislation regarding identity theft in view of the fact that it could overlap with existing offences.

To the extent that the laws are necessary, the offences should recognise that privacy is now a social value that is expected to be protected by taking into account the significant privacy issues involved. This will entail ensuring that the provisions operate in circumstances relating to both identity fraud and identity theft, that they provide for appropriate mechanisms to assist victims re-establish their identities and that they are not drafted in unnecessarily broad terms which would have the effect of eroding an individual's right to privacy.