Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Brief submitted to the House of Commons
Standing Committee on Justice and Human Rights

by the

Canadian Internet Policy and Public Interest Clinic ("CIPPIC")

on

Bill C-27
An Act to amend the Criminal Code
(identity theft and related misconduct)

March 31, 2008

Université d'Ottawa • University of Ottawa
Faculté de droit • Faculty of Law
57 Louis-Pasteur, Ottawa (Ontario) K1N 6N5 Canada
(613) 562-5800 (2553) • (613) 562-5417 (Téléc/Fax)
www.cippic.ca • cippic@uottawa.ca

Brief submitted to the House of Commons
Standing Committee on Justice and Human Rights
by the
Canadian Internet Policy and Public Interest Clinic ("CIPPIC")
on
Bill C-27
An Act to amend the Criminal Code (identity theft and related misconduct)

March 31, 2007

CIPPIC's ID Theft Project

CIPPIC is a legal clinic based at the University of Ottawa, Faculty of Law. We engage in research and advocacy on issues arising from the use of new technologies. One of our major research projects, funded by the Ontario Research Network on Electronic Commerce, is on legal and policy approaches to identity theft. We have reviewed legislation, caselaw, and policy initiatives related to identity theft throughout Canada and in other jurisdictions with a view to identifying law and policy reforms aimed at better preventing, detecting and mitigating the harms from identity theft. Last year, we published a series of working papers on various aspects of identity theft, as well as a White Paper calling for Security Breach Notification laws. These can be accessed from our website at www.cippic.ca, under "Projects – Identity Theft".

We appreciate the opportunity to address this committee on the matter of Bill C-27, *An Act to amend the Criminal Code in respect of identity theft and related misconduct*.

Bill C-27

CIPPIC strongly supports this Bill. Together with Bill C-299, it will provide law enforcement authorities with much better legislative tools with which to catch and convict identity thieves. The *Criminal Code* currently includes offences of fraud, forgery and impersonation, but does not treat as offences a number of key elements of typical identity theft crimes. In particular, there is no offence at present for the obtaining of, or trafficking in, identity information for the purpose of fraudulent use. Yet, this is the first step in identity theft crimes, upon which subsequent fraud is based. Forcing the police to wait until the fraud has been committed before they can lay charges clearly exacerbates the situation and leads to increased victimization of the unsuspecting public.

Specific aspects of the Bill that we support include:

- Extending the offence of mail theft to cover theft after delivery and fraudulent redirection of mail, both of which are common techniques used by identity thieves;
- Creating a new offence for the making, selling, etc. of official identity documents;
- Creating a new offence for knowingly obtaining, possessing or trafficking in another person's identity information where there is a reasonable inference that the information will be used to comment fraud;
- Clarifying that the offence of impersonation includes using someone else's ID as if it pertains to the person using it; and
- Providing for restitution to victims of identity theft or fraud (although the benefits of such limited restitution to victims are minimal).

We also strongly support Bill C-299, insofar as it would clearly criminalize another common tactic of identity thieves known as "pre-texting" – i.e., obtaining personal information about someone else through false pretenses, such as pretending to be that person, in order to then use the information to comment fraud.

The Bill would make some currently indictable offences hybrid. This is a sensible amendment, giving greater latitude to prosecutors and courts to pursue lesser identity offences as well as more serious ones.

We wonder, though, why the new identity theft and document breeding offences carry much shorter maximum jail terms than apply to existing offences for fraud, forgery, and impersonation (5 years vs. 10 years). Similarly, we wonder why the maximum jail term for pre-texting is only 2 years.

Bill C-27 in context: the bigger picture

Although we support this legislation, it addresses only a small part of the identity theft problem. If we are to attack the problem effectively, we need to do much more than establish crimes for which police can charge offenders. We also need to provide law enforcement authorities with the *resources* they need to prosecute the new offences.

More importantly, we need to take measures to frustrate identity thieves – measures that make it more difficult for them to gather personal information in the first place, and to then successfully use it in fraudulent ways. And we need to do a better job assisting victims once identity theft is detected. *Prosecuting identity thieves is not going to solve the problem; fraudsters will always exist.* We need to address, through *non*-criminal laws and policies, the many ways in which identity crimes are facilitated by private corporations and governments

to whom we have entrusted our personal information. And we need to do a better job mitigating the harms caused by this crime to the unfortunate individuals who become victims, usually out of no fault of their own.

(1) Criminal Law

Law Enforcement Resources to Investigate ID Theft Cases

In addition to treating identity theft and fraud as offences with appropriate maximum sentences, we need to ensure that the police have the necessary human resources, in terms of both numbers and expertise, to investigate these crimes. While some identity thieves are petty criminals, others are hardened criminals, highly skilled at evading police. According to law enforcement agencies, organized crime is responsible for an increasing proportion of identity fraud. It can take hundreds, if not thousands, of hours for police to investigate these crimes. Our research suggests that difficulties in prosecuting and convicting identity thieves stem less from deficiencies in the *Criminal Code* and more from lack of sufficient resources on the part of law enforcement agencies to pursue the typically long and complicated investigations that are required. Simply amending the Code is not going to solve this problem.

Cooperation among Law Enforcement Agencies in Cross-Border ID Theft Cases

Greater cross-border cooperation among law enforcement agencies in such investigations should be encouraged and facilitated through appropriate resource allocation. Bill C-27 is helpful in this respect as it would permit the trying and punishment of convicted identity thieves either where the accused is found or where the crime was committed. But more could no doubt be done by Canadian law enforcement agencies to cooperate both domestically and internationally in the investigation of often very complicated cross-border cases of identity theft and fraud.

Appropriate Sentencing of ID Thieves

Judges should be educated as to the seriousness of identity theft crimes so that they impose truly deterrent sentences. Although some recent cases suggest that courts are beginning to treat identity fraud as a serious crime, our review of the caselaw suggests that judges are often letting identity thieves off with relatively lenient sentences. If the individual is a hardened criminal, such sentences may be treated as a mere cost of "doing business". Moreover, lenient sentencing deters police from engaging in the often long and complex investigations required in order to convict.

(2) Data Protection Law

Even if the police are given the tools and resources they need to prosecute identity thieves, the problem will not go away. Fraudsters will continue to take advantage of lax security and the increasing availability of personal data both online and offline, as long as they are able to. While individuals bear responsibility for their own data management practices, they cannot control those of corporations and governments. Indeed, it is estimated that most identity theft occurs from corporate databases, mailings or other sources completely beyond the control of individuals. Data protection law is therefore a critical component of any effective identity theft prevention plan.

Enforcing Data Protection Laws

Canada's private sector data protection law – the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") – requires that corporations take reasonable security measures to protect our data, that they limit their collection and retention of personal data to that which is necessary for the purposes they have identified, and that they be particularly careful about protecting sensitive data such as Social Insurance Numbers ("SINs"). These rules, widely accepted as "fair information practices", should ensure, for example, that a fraudster can't get a credit card or loan in my name. They should ensure that commercial entities don't use SINs as customer identification numbers, or retain other sensitive personal information unnecessarily, thereby creating a tempting target for identity thieves.

Yet, these and other practices that clearly violate PIPEDA continue to be widespread in the Canadian marketplace. Companies frequently collect and retain far more personal information than they need (including SINs), and fail to take adequate security measures to protect it. Not surprisingly, they then suffer security breaches whether in the form of insider theft or external access, some of which lead to identity fraud.

The problem is that PIPEDA lacks teeth; companies are able to ignore it with impunity. Individuals can lodge complaints with the federal Privacy Commissioner, who must investigate but is empowered to render only a non-binding "report" on the complaint. Individuals are then expected to take their privacy complaints to Federal Court in order to have them enforced or to obtain compensatory damages. Given the cost of such litigation, the risk of adverse cost awards, and the fact that many privacy violations involve no quantifiable damages, it is not surprising that few cases proceed to court.

Identity theft is a growing problem in large part because of the huge and ever-growing market in personal data. In a world of "customer relationship

management" and "behavioural targeting", there is no limit to the personal data that companies seek to collect and analyse for commercial purposes. The result is a proliferation and consolidation of databases that are of great value to criminals as well as to marketers. Although meant to limit the collection, use, retention and disclosure of personal data, PIPEDA appears to be having little effect.

Without effective enforcement of data protection laws, identity theft will remain a serious, if not growing, problem in Canada.

The need for Breach Notification laws

A significant gap in PIPEDA is the lack of an explicit obligation on organizations to report security breaches that expose personal data to unauthorized access and potential fraudulent use. CIPPIC has advocated that PIPEDA be amended to include such a rule, and Industry Canada is now acting on this recommendation. Breach notification is a key piece of any plan to address identity theft insofar as it (a) allows affected individuals to take mitigating measures when their data is compromised, and (b) creates stronger incentives for organizations to take effective security measures in the first place.

(3) Consumer Protection Laws

Much work remains to be done at the provincial level to better protect consumers from identity fraud and to empower them to mitigate damages when they find themselves victimized or at risk of being victimized. For example, consumers should have the right to place a "freeze" on their credit files so that identity thieves cannot open up new accounts or get credit in their name. Consumers in most American States have this right, but Canadians do not. Consumers should also be permitted to see the credit report relied upon by lending institutions when loans are denied. Victims of ID theft should have the right to a local police report regarding the incident, and to a copy thereof.

The federal government can and should do more to encourage and coordinate provincial law reforms designed to protect consumers and assist victims. We proposed the establishment of a Federal/Provincial/Territorial Task Force on Identity Theft to coordinate government measures toward this goal.

(4) Reporting and Statistics: the role of banks

There are few statistics on the incidence and cost of identity theft and fraud in Canada. The police collect and publish statistics on complaints they receive, but this reflects only a fraction of the problem given that financial institutions usually reimburse victims for losses. Banks choose to assume the risk of fraud

rather than force customers to authenticate themselves in person or by other methods viewed as inconvenient. The problem is therefore under-reported.

We need a national strategy for gathering reliable, reasonably comprehensive data on the incidence, types and costs of identity theft and fraud in Canada. This will require a coordinated effort by law enforcement agencies, financial institutions, consumer groups and others. Banks, in particular, occupy a key role in this effort given that much of the primary data is in their hands. They, along with other credit-granting institutions, should be required to report on incidents of identity theft and fraud on a regular basis.

(5) Public Education and Victim Assistance

While there are many good websites and brochures educating consumers about the risks of identity theft/fraud and safeguards that they can take to avoid being victimized, individuals continue to fall prey to the ever-evolving schemes used by identity thieves. The federal government, through an agency such as the Financial Consumer Agency of Canada, is well-placed to undertake a national public education campaign on ID Theft, in consultation with lending institutions, credit bureaus, law enforcement agencies, and consumer groups.

Also valuable in this effort would be the establishment of a national identity victim assistance bureau – a one-stop source of information and advice for victims. Such an agency could also play a role in gathering statistics, educating the public, and initiating law and policy reforms.

Conclusion

CIPPIC supports Bill C-27, as well as Bill C-299. However, we urge this committee to look beyond *Criminal Code* amendments to the broader problem they are addressing, and to consider other measures that Parliament can take to prevent and mitigate the harms caused by identity theft and fraud. The problem is multi-dimensional in nature, and requires a multi-dimensional response. The federal government is in a position to lead this response not just by amending the Criminal Code, but also by:

- Ensuring, to the extent possible, that law enforcement agencies have the resources necessary to investigate identity theft and fraud cases;
- Assisting in the development of effective mechanisms to investigate and prosecute cross-border identity crimes;
- Educating judges as to the seriousness of identity theft and fraud crimes;
- Amending federal privacy laws to include security breach notification requirements;

- Strengthening the enforcement regime under the *Personal Information Protection and Electronic Documents Act* so as to create real incentives for compliance;
- Coordinating provincial law reform initiatives designed to prevent identity fraud and to mitigate its effects;
- Requiring that banks report on identity theft and fraud;
- Establishing a lead federal agency to gather statistics on identity theft/fraud, to engage in public education, and to coordinate efforts by other agencies and governments; and
- Funding the creation of a national identity theft victim resource and assistance bureau.

** END OF DOCUMENT **