

Identity Theft Project

Measurement • Management • Policy • Tools

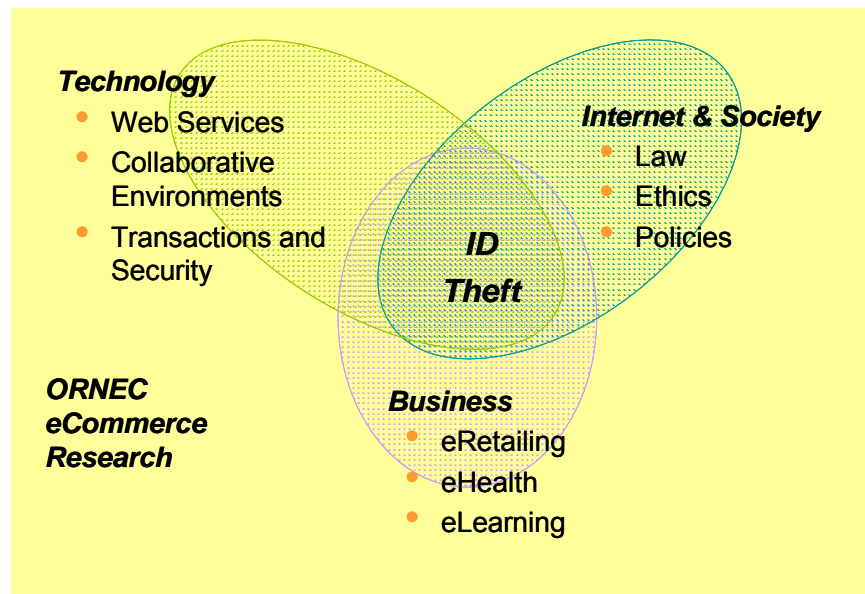
Progress Overview: December 2007

Background

The Ontario Research Network for Electronic Commerce (ORNEC) was established in 2001 as a collaborative project between ORDCF (Ontario Research and Development Challenge Fund) and the University of Ottawa in partnership with the three Ontario Universities (McMaster, Carleton and Queen's) and leading private and public sector partners. According to the agreement with the Ontario Ministry of Research and Innovation (MRI), the ORNEC project was originally slated to end on December 31, 2007 however to compensate for delays encountered at the beginning of the project the MRI granted ORNEC an extension till June 30, 2008. This extension has been applied to many ORNEC research projects including Identity Theft. The mandate of ORNEC is to establish multidisciplinary research capacity and undertake research in priority topics of interest to private sector partners in eCommerce areas involving law, business and information technology. ORNEC private sector partners supporting ORNEC research include large corporations as well as SMEs (Small and Medium Enterprises) from the Information Technology, Business and Law Sectors. ORNEC funding and support comes from three sources:

- \$13,364,567 ORDCF Cash Grant from the Government of Ontario
- \$13,364,567 in cash and/or inkind from private sector partners
- \$14,282,806 in cash and/or inkind from participating institutions

ORNEC invested its funding in eCommerce Capacity Building and eCommerce Research projects. eCommerce Capacity Building focused on establishing eCommerce Facilities, Organizations and Education and Training Projects. As illustrated, eCommerce Research is structured in three categories, Technology, Business and Internet & Society. Research in Identity Theft (ID Theft or IDT), the ORNEC Flagship Project occurs at the intersection of these three categories.



Important News

- **ORNEC ID Theft Documents available on-line, see page 2**
- **Next-Generation PKI Technology to combat on-line credit card fraud. See Dr. Carlisle Adams research on page 16**

ORNEC ID Theft Research

ORNEC-funded research in IDT is structured in four projects:

1. **Defining and Measuring Identity Theft**
Principal Investigator: Dr. Norm Archer, Professor Emeritus, Management Science and Information Systems, DeGroot School of Business, McMaster University
2. **Management Approaches to Combating Identity Theft**
Principal Investigator: Dr. Yufei Yuan, Professor of Information Systems, Wayne C. Fox Chair in Business Innovation, DeGroot School of Business, McMaster University
3. **Legal & Policy Approaches to Identity Theft**
Principal Investigator: Ms. Philippa Lawson, Executive Director and General Counsel, Canadian Internet Policy and Public Interest Clinic (CIPPIC), Faculty of Law (Common Law Section), University of Ottawa
4. **Technical Tools to Address Identity Theft**
Principal Investigator: Dr. Ali Miri, Associate Professor, School of Information Technology & Engineering (SITE), University of Ottawa

This progress report is intended to provide a comprehensive overview of the ORNEC IDT project to date in terms of results, events and publications.

ORNEC ID Theft Documents

The documents referenced in the “Results to date” Sections for Projects #1, #2 and #4 are available from the ORNEC Website www.ornec.ca under ORNEC Exchange. Because of copy right issues, access to these documents is restricted to ORNEC ID Theft partners and is therefore protected by a password available from ORNEC (contact Robert Crawhall at crawhall@ncit.ca or Mohamed Zaid at mzaid@ncit.ca).

For Project #3 the documents referenced in the “Results to date” Section are available from the CIPPIC Website <http://www.cippic.ca/> under the Identity Theft link.

Project #1: Defining and Measuring Identity Theft

Research Team:

[Dr. Norm Archer](#), Professor Emeritus, DeGroot School of Business, McMaster (**Principal Investigator**)

Dr. Susan Sproule, Postdoctoral Fellow, DeGroot School of Business, McMaster University

[Dr. Milena Head](#), Assoc. Prof. & Assoc. Dean, DeGroot School of Business, McMaster

[Dr. Ken Deal](#), Associate Professor and Area Chair, DeGroot School of Business, McMaster University

[Dr. Yolande Chan](#), Professor of Management Information Systems at Queen's University School of Business

[Dr. Vinod Kumar](#), Professor, Sprott School of Business, Carleton University

[Dr. Uma Kumar](#), Professor, Sprott School of Business, Carleton University

Research Objectives:

Until now there has been little published research that organizes and classifies clear definitions of what identity theft and identity fraud mean. Until such classifications are clarified, it is difficult for business, government, and the public to understand the level of such activities and their impact on organizations and individuals, in making comparisons over time and among different jurisdictions. If such an understanding is developed and comes into general use, it will be easier to organize methods to combat identity theft and fraud, through improvements and attitudes relating to laws, education, security, and privacy, both within and external to affected organizations, and in the population at large.

Given an improved understanding of appropriate classifications of identity theft and fraud, an important next step is to measure the incidence of related criminal activities. This would help in the development of concerted efforts to combat these activities. Other industrialized countries, in particular, the United States and the United Kingdom, collect statistics on the level of identity theft and fraud on a regular basis. In Canada, the collection and public reporting of these statistics is fragmented and probably not representative of the real rates of identity theft and fraud. In addition, there has been little effort to track trends in these rates, or to use them to estimate the economic and social impact in an organized and logical manner. This lack of useful statistics is evident in the widespread lack of knowledge about identity theft displayed in the Canadian consumer population, business, and government.

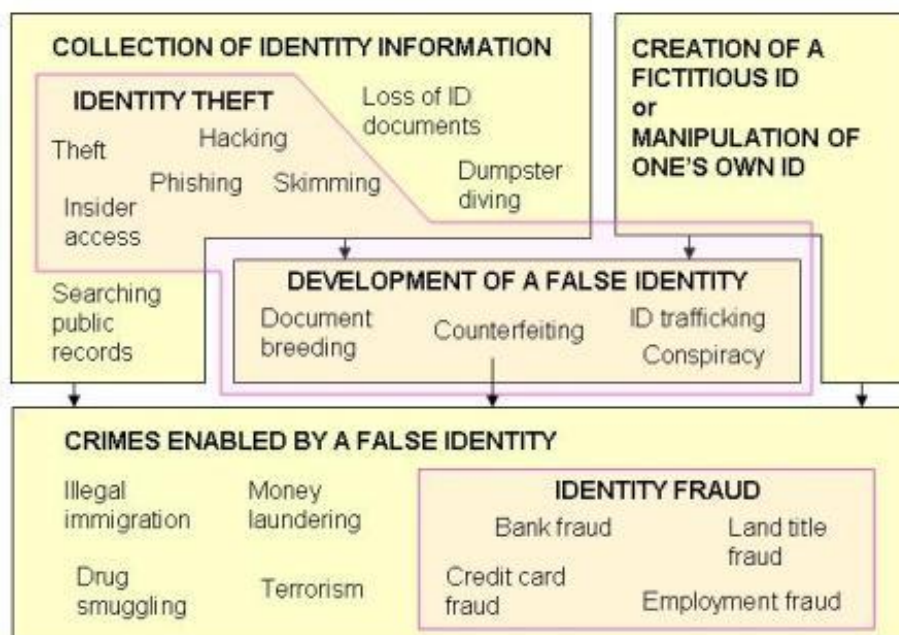
The objectives of this project relate to the development of suitable classifications of identity theft and fraud that can be used in measuring and combating these crimes in Canada. One aspect of the research will be directed to corporate information security management, and the repercussions of unlawful data access on company reputation, the strength of social and market ties with customers, and the impact on financial performance. A second major thrust of the project will be directed towards consumers, with appropriate definitions developed and statistics gathered through separate surveys of Canadian consumers, and businesses in selected industries, to measure the level and type of identity theft and fraud. This is necessary because statistical data currently available on ID theft in Canada are fragmented or missing. Finally, indexes will be developed that can be used to monitor the level of identity theft and fraud and their impact on business, government, and society. These indexes will be very useful in measuring trends in these levels, so the impact of efforts to combat identity theft and fraud can be evaluated.

Results to date:

1. Dr. Susan Sproule has completed a literature review and prepared a discussion paper entitled "Defining Identity Theft – A Discussion Paper" that was presented and discussed during the first kickoff IDT workshop held on Tuesday April 18, 2005 at McMaster eBusiness Research Centre

(MeRC). This paper established background knowledge needed to achieve a common and essential agreement on a definition and terminology for Identity Theft. See the discussion paper entitled **“Sproule-Archer (Defining IDT Paper) IDT Wkshp-1 McMaster-18Apr06”**

2. Norm Archer, “Combating Identity Theft”, Presentation to Canadian Marketing Association Regulatory Affairs Conference, Toronto, Ontario, September 14, 2006.
3. Model incorporating definitions of identity theft and identity has been developed and presented at the second IDT workshop held on Friday October 13, 2006 at SITE, the University of Ottawa. Diagram of this model with an overview of the terminology and definitions proposed for identity theft and identity fraud is shown below. See the presentation entitled **“Archer-Sproule (Defining ID Theft) IDTWkshp-2 Ottawa-13Oct06”**.



4. Norm Archer, “Identity Theft: A Major Public Issue”, Presentation at Law Symposium, Iroquois Ridge High School, Oakville, Ontario, December 7, 2006
5. Consumer survey to measure ID Theft and ID fraud in Canada conducted by *OpenVenue* using an Internet Panel of n=3550. The survey is representative of Canadian population by region, gender and age (excluding Quebec). Respondents were over 18 years of age holding bank accounts and at least one credit card. The survey employed the terminology and definitions for ID Theft and ID Fraud that have been discussed and developed at McMaster. Survey results provided insight knowledge in public perceptions, how to identify victims, incidence rate and categorization and nature and characteristics of ID Theft and ID Fraud incidents. See the presentations entitled **“Sproule-1 (Defining Measuring IDT) IDTWkshp-3 Toronto-7Jun07”** and **“Sproule-Deal (Defining Measuring IDT) IDTWkshp-3 Toronto-7June 07”**.
6. Developing an IDT Composite Index (similar to a Consumer Price Index) to measure and report trends in individual categories of identity theft and fraud, and to report on overall categories of these,

for consumers, businesses, and governments has been discussed. See the presentation entitled *“Archer (Index Measures of IDT) IDTWkshp-3 Toronto-7June07”*

7. Results of work to describe and measure the characteristics of ID Theft and ID Fraud e-Identifiers were presented in the IDT Workshop #3 held in Toronto on June 7, 2007. See the presentations entitled *“Kumar-Lavassani (IDF Identifiers) IDTWkshp-3 Toronto 7Jun07”* and *“Kumar-Lavassani (IDF Measurement) IDTWkshp-3 Toronto-7Jun07”*. For more details see research progress report *“IDT Measurement Project Report Nov07”* entitled “Measures of Identity Fraud by Vinod Kumar, Uma Kumar, Kayvan Lavassani and Bahar Movahedi”.
8. Willingness-to-Act to Avoid Identity Theft has been characterized, measured and statistically presented to throw light on what will people do and not do and how such actions apply to everyone. See the presentation entitled *“Deal (Willingness to avoid IDT) IDTWkshp-3 Toronto-7June07”*.
9. A presentation based on the results of the consumer survey was given by Dr. Susan Sproule as part of the Surveillance Project Seminar Series at Queens University (April 2007).
10. A paper by Dr. Susan Sproule and Dr. Norm Archer entitled “Defining Identity Theft” was presented at the 8th World Congress on the Management of eBusiness (Toronto, July 11-13, 2007) and is published in the conference proceedings. Revisions are underway so that this paper can be submitted to an academic journal.
11. Dr. Norm Archer, Dr. Yufei Yuan and Dr. Susan Sproule presented summaries of their research at the Ontario Government’s Access and Privacy Workshop 2007 (Toronto, October 2-3).
12. Dr. Norm Archer and Dr. Susan Sproule participated as members of the advisory committee for the Data Development Project to Measure Consumer Fraud. This project is being organized by the Canadian Centre for Justice Studies and Statistics Canada. Dr. Norm Archer, Dr. Susan Sproule and Dr. Yufei Yuan also advised on the CCJS’s Pilot Survey of Fraud Against Businesses. It is expected that results from both of these projects can be incorporated into the IDT Composite Index.
13. Dr. Susan Sproule attended the 18th Annual Conference of the Economic Crime Institute held in McLean, VA on October 21-23, 2007. This conference brought together leading researchers in identity management and information protection.
14. A working paper with the results of the 2006 consumer survey is underway and will be ready for publication by the end of the year.
15. Dr. Susan Sproule and Nicole Wagner are working on a paper that will examine the demographic characteristics of Canadian identity theft victims. This paper will be submitted to an academic journal.

Project #2: Management Approaches to Combating Identity Theft

Research Team:

[Dr. Yufei Yuan](#), Professor & Wayne C. Fox Chair, Degroote School of Business, McMaster University (Principal Investigator)

[Dr. Khaled Hassanein](#), Associate Professor, McMaster DeGroote School of Business, and Director of McMaster eBusiness Research Centre [MeRC](#)

[Dr. Milena Head](#), Associate Professor and Associate Dean, McMaster DeGroote School of Business, McMaster University

[Dr. Vinod Kumar](#), Professor, Sprott School of Business, Carleton University

[Dr. Uma Kumar](#), Professor, Sprott School of Business, Carleton University

[Dr. Shaobo Ji](#), Assistant Professor, Sprott School of Business, Carleton University

Research Objectives:

The objectives of this research are to study management approaches to combating ID Theft focussing on developing an in-depth understanding of ID Theft and measures required to prevent and/or combat it. See ORNEC ID Theft Backgrounder¹ for ID Theft background information.

The first objective is to develop a carefully designed ID Theft risk management model. Building on a recently developed framework for combating ID Theft², this project will utilize the framework to analyze ID Theft as a risk that institutions must manage. This must take into account the environment of consumers, businesses, and governments. Most organizations do not know how to manage the risk, and where the most appropriate investments need to be made. For example, the development of an optimal strategy for a balance among increased security, employee training, monitoring, etc. in order to minimize identity theft and at the same time apply efforts where they will have the best effect. Such an approach would be built on the general principles already outlined in the framework from the previous studies.

The second objective is to investigate the current status and effectiveness of tools, techniques and practices to address and prevent ID Theft and to identify and analyze the costs and benefits of countermeasures to ID theft. To identify effective tools and practices, comparison will be performed in terms of the extent of use in the industry, efficiency, cost and complexity of implementation. The cost and benefit analysis of ID Theft countermeasures may depend on different types of ID uses, such as ID for social use (such as passport, social security, driver license, and healthcare card), financial use (such as credit card, insurance), and educational use (such as certificate). It is also associated with different stakeholders (issuers, checker, owners, and protectors). There are also different types of measurements of cost and benefit. It is imperative to analyze costs and benefit of all kinds of ID Theft countermeasures in order to achieve a reasonable and effective security management. For example, signatures are used in Western countries for credit card authentication. But in China, PIN numbers are required for credit card authentication and a small portable device is used to let the customers enter their PIN number. The cost and benefit analysis of using PINs or password countermeasure needs to be done in order to evaluate their implementation costs for credit card issuers, credit card checkers, credit card owners and credit card protectors and the benefit in terms of effectiveness in enhancing credit card security management. Similar analysis of some new technologies, such as biometric and smart card technology can also foster broader

¹ ORNEC – sponsored research report: “Identity Theft – Backgrounder”

² Wen Jie Wang, Yufei Yuan and Norm Archer: “A Theoretical Framework for Combating Identity Theft” MeRC Working Paper # 12 (September 2004).

technical applications. The results developed in this study will provide financial institutions and other organizations with a comprehensive list of available solutions they can implement to fight ID Theft effectively. It will also guide them in their decisions regarding implementation of new technologies and procedures in combating the growing problem of identity theft. Finally it will provide them with a framework of effective ID Theft prevention program they can relate to.

The third objective is to understand consumer acceptance of various countermeasures to ID Theft across various applications. Countermeasures can impact consumer privacy and convenience to varying degrees. From a consumer's perspective, the negative consequences of identity protection may be perceived to be too high for certain applications or scenarios. Business and government must understand the tolerance and acceptance of various countermeasures before blindly applying them to all potential applications and vulnerability points within those applications. At some of these vulnerability points, the burden and hassle of applying certain countermeasures may not be justified in the eyes of the consumer.

The fourth objective is to study the effectiveness of various approaches to multi-party coordination in combating ID theft. Numerous authors in business literature agree that the success in combating ID theft relies on joint efforts and coordination among all the stakeholders involved in the process, such as the ID owner, ID issuer, ID checker, and ID protector, in every relevant activity, such as prevention, detection, and prosecution. For example, in the process for issuing US biometric visas, fingerprints of the applicant are electronically compared with fingerprint records in criminal databases. This comparison process requires coordination between the visa issuer (consular posts abroad) and protectors (DHS: Department of Homeland Security; FBI). Multiparty coordination among owners (fraud reports), issuers (status of credit cards), checkers (abuses), and protectors (investigation and prosecution), is also very important in ID theft prosecution procedures. In particular, the role of the banking industry is seen as a very important. Some authors promote a view that the banking industry leaders could develop a commission of concerned victims, law enforcement, credit grantors, credit reporting agencies, governmental agencies, bankers, and others in a group, with technology and security support people. Each group could in this way gain insight from the others to foster better solutions. In order to provide best protection and efficiency in combating identity theft numerous entities involved need to cooperate. Although multiparty collaboration is seen as a very important and even crucial condition of achieving success in combating ID theft, little work has been devoted in the literature to provide framework of multiparty collaboration in ID theft context. Also, it is not known what factors affect its performance. Therefore, the focus of this research is to identify various approaches to multi-party coordination in combating ID theft and to study their effectiveness. The research will in particular provide a framework of multiparty-collaboration: parties, roles, information flows, and interactions; discuss current issues and solutions regarding to cross boundary collaboration, and conduct requirement analysis of multiparty ID management information systems. The model developed and findings from the research will provide guidelines for the institutions affected by identity theft and will enable them to focus on these collaboration practices that could lead to best results in combating identity theft.

The fifth objective is to study the interrelationship and interaction between security, privacy, trust, and ID theft prevention. The relationship and interaction between security, privacy, trust, and ID theft prevention is complex and to manage a balance among these constructs is challenging. For example, security usually enhances ID theft prevention. However, to combat ID theft requires more rigid user authentication which may raise the concerns on privacy violation. For instance, if we request finger print input or PIN number with the use of credit card for online shopping, it could help to prevent ID theft, but people may not willing to do so. Thus there is a need to balance among these constructs and understand the user reaction to different IDT countermeasures. To formulate proper strategy to counter the impact of identity theft/identity fraud it will be quite helpful if one understands what goes behind the consumer mind with respect to various IDT preventive measures. Systematic understanding of the decision process to fulfill an online transaction from the consumer point of view and how to identity theft/ identity fraud prevention steps relate

to security, privacy, and trust formation will definitely help professional managers to formulate suitable IDT combating strategy and thus improve the adoption of e-commerce.

Other objectives may be identified as additional researchers from the ORNEC universities or elsewhere join this research team, or as suggestions are received from business, government, and non-profit institutions interested in contributing to the project and collaborating with the research team.

Results to date:

1. Risk Analysis using an Identity Management Lifecycle Approach was presented to the IDT workshop #2 held in Ottawa on October 13, 2006. See *"Yuan (Identity Management) IDTWkshp-2 Ottawa-13Oct06"*. The Risk Analysis using an Identity Management Lifecycle Approach was applied to ID management in public sector, particularly the passport management. It was presented by Dr. Yuan to Ontario Access & Privacy Workshop organized by Ontario Government in Toronto, on October 2, 2007. See <http://verney.ca/onapw2007/>. Dr. Yuan is also invited to give a presentation at 2008 Visa Canada Security Symposium in Toronto, March 26, 2008. A paper on this topic is in the draft stage and will be submitted for possible journal publication.
2. Proposal for a "Survey on Identity Theft: Its Impact, Organizational Awareness, and Practice of Countermeasures". The objectives of the survey are to obtain an understanding of how organizations perceive ID theft problems (Awareness), evaluate the impact of ID theft (Impact) and combat ID theft (Practice). See the presentation entitled *"Yuan-Guo (Survey on ID Theft) IDTWkshp-3 Toronto-7Jun07"*. We have learned later that Statistic Canada will conduct a business survey on IT Fraud. By invitation, we provided feedback and comments to them for further improvement. Since it has considerable overlapping with our proposed business survey, we decided not to duplicate the effort from us.
3. The results for the 3rd objective to date are as follows: Developed a theoretical model of consumer acceptance of biometrics for identity verification in financial transactions; Model presented and validated at various workshops with banking partners; Interviewed various bank representatives to further validate the model and research questions; Designed survey which will be run with 400 banking customers to empirically validate the above model; Engaged a consumer research company to identify customer pool and run survey; Applied for research ethics approval (waiting for response). To date this work is documented in a 60 page report (Ph.D. desertion proposal document). Next Steps: Secure research ethics approval (next week or two); Conduct survey (January); Analyze results (February); Write reports/papers (March – June); Present at update workshops.
4. Collaboration in Combating Identity Fraud has been discussed. Collaboration generally defined as the process of working together as different individuals, groups or organizations towards a common aim encompassing all the three levels of interaction, cooperation and coordination. See presentation entitled *"Kumar-Kumar (Collaboration) IDTWkshp-2 Ottawa-13Oct06"*.
5. Results of the fourth objective - Multiparty Collaboration project- the objective is to explore the current best collaboration practices among various stake holders that are taking place in combating identity theft. The project report is available now. For more details see research progress report *"IDT Collaboration Project Report Nov07"* entitled "Collaboration in Combating Identity Fraud by Vinod Kumar, Uma Kumar and Danuta de Grosbois"
6. Ji, S., Wang, J., Min, Q., and Smith-Chao, S. (2007) Systems Plan for Combating Identity Theft – A Theoretical Framework was presented at 2007 International Symposium on Information Systems & Management (2007 ISM: the Management Track of IEEE WiCOM2007), July 25-28, 2007,

Shanghai, China. It was published in Conference Proceedings (IEEE Xplore). See <http://ieeexplore.ieee.org.proxy.library.carleton.ca/iel5/4339774/4339775/04341345.pdf>

Project #3: Legal & Policy Approaches to Identity Theft

Research Team:

[Ms. Philippa Lawson](#), Executive Director of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) (Principal Investigator)

[Dr. Robert Biddle](#), Professor, Human-Oriented Technology Laboratory, Carleton University

[Jennifer Chandler](#), Assistant Professor, Faculty of Law (Common Law Section), University of Ottawa

[Dr. Elizabeth Judge](#), Associate Professor, Faculty of Law (Common Law Section), University of Ottawa

[Dr. Valerie Steeves](#), Assistant Professor, Department of Criminology, Faculty of Social Sciences, University of Ottawa

[Dr. Daniel Gervais](#), Professor, Department of Criminology, Faculty of Social Sciences, University of Ottawa

Ms. Wendy Parkes, Research Associate at CIPPIC (worked for CIPPIC on this project until February 2007)

Dr. Mark Erik Hecht, Visiting Professor, Faculty of Law, University of Ottawa (works for CIPPIC on this project starting February 2007)

Research Objectives:

Aided by the increase in digitization and online use of information, ID Theft is rapidly becoming a major worldwide problem for businesses, governments, and citizens. An effective response to this burgeoning problem requires a multi-tiered approach: in addition to technological tools, smart business practices, and improved consumer awareness, government policy and legislative reform have key roles to play in the effort to contain this growing problem.

This project proposes to examine the role of law, government policy, industry self-regulation, and both industry and consumer self-help in combating ID Theft and related fraud.

Canada has no legislation specifically addressing ID Theft. We have criminal laws prohibiting fraud, privacy laws requiring the protection of personal information in the possession of governments and corporations, and a patchwork of general consumer protection laws.

In contrast, the United States has numerous federal and state laws specifically targeting identity thieves, and more on the way. In May 2004, a New York State man who sent out 825 million bulk email messages using stolen identities and forged addresses was sentenced to three and a half to seven years in jail under that state's new identity theft statute.

In addition, there is a significant amount of legislation in the USA providing consumers with the tools they need to prevent and manage identity theft. For example, California requires companies that conduct business in that state, and store data electronically to warn customers of security breaches in their computer networks. California law also requires that credit issuers verify the address of the consumer if: (a) an application for credit shows an address different from that on the pre-approved offer; or (b) a request for a duplicate credit card is received within 10 days of a request for a change of address. Indiana recently passed a law that gives courts the authority to order credit reporting agencies to restore a victim's credit history. Federal legislation in the USA also provides consumers with tools to prevent identity theft and clean up after it.

The Canadian Association of Chiefs of Police has called for a new criminal offence of possession of multiple identities, in order that its members can prosecute identity theft cases. The Canadian Bankers' Association has likewise called for amendments to the *Criminal Code* so as to clearly define "Identity Theft" and "personal information", and to outlaw certain practices that are clearly implicated in ID theft.

The federal department of Justice is currently considering these and other amendments to the *Criminal Code* in order to better address the growing problem of ID Theft.

Some states in the USA have legislated consumer protection from debt collectors once the consumer has reported a fraud, or court-ordered restoration of victim credit reports. California operates a special ID Theft registry for victims of criminal ID Theft. Credit bureaus in some jurisdictions offer "fraud alerts" and "credit freezing".

Provincial consumer affairs ministries are working with the federal Office of Consumer Affairs through the Consumer Measures Committee to harmonize information efforts and to identify effective policy and legal approaches to ID Theft that could be taken at the provincial and/or federal levels. It is important that Canada learns from other jurisdictions that have experimented with such approaches and encourage private sector stakeholders to take measures that have proven to be effective in either, preventing, detecting or mitigating the effects of ID Theft.

With respect to law enforcement, there may also be lessons to be learned from other jurisdictions. In the US, the Federal Trade Commission (FTC) assists in criminal law enforcement and alerts state Attorneys General to the FTC resources, emphasizing how they can be used to assist state residents who are ID Theft victims. The FTC also maintains a centralized database of victim complaints that is made available to law enforcement agencies nationwide.

Moreover, regardless of efforts to prevent it, ID Theft will no doubt continue to occur, robbing its victims of personal security and peace of mind, as well as money and time spent on recovery. As stated by the USA General Accounting Office in a report on Identity Theft,

“Identity Theft can cause substantial harm to the lives of individual citizens – potentially severe emotional or other non-monetary harm, as well as economic harm. Even though financial institutions may not hold victims liable for fraudulent debts, victims nonetheless often feel “personally violated” and have reported spending significant amounts of time trying to resolve the problems caused by identity theft – problems such as bounced checks, loan denials, credit card application rejections, and debt collection harassment.”

Where we have not been successful in preventing identity theft, we can at least ease the recovery phase for victims. Some businesses and governments have implemented measures in recent years to assist victims. For example, Canadian governments have jointly developed a standard "Identity Theft Statement" for use by consumers in this country, but experience to date suggests that this initiative has not been particularly useful. Representatives from federal and provincial consumer affairs departments are working together through the federal/provincial Consumer Measures Committee to harmonize information efforts and address the issue further.

The FTC operates a toll-free hotline for ID theft victims. There is no similar single source of information or assistance for ID theft victims in Canada.

There is a need to assess various approaches being taken to victim assistance in order to identify and implement those most likely to be effective in Canada.

The proposed project constitutes six-sub-projects, each of which is severable (e.g., can stand on its own, or can be dropped if there is insufficient funding). The sub-project titles are as follows:

1. Comparative analysis of legal and policy approaches to preventing, detecting, and mitigating ID theft (CIPPIC);
2. The legality of "self-help" approaches to ID theft (Chandler);
3. The privacy implications of criminal law responses to ID theft (Steeves);
4. The role of consumer trust and e-commerce usability factors in ID theft (Biddle et al);

5. Legal methods for ID theft redress: common law tort and intellectual property law (Judge & Gervais); and
6. Legal approaches to ID theft: the civil law doctrine of personality rights (Goudreau)

Results to date:

Results of the research in this project are best seen through the numerous publications made. These are listed in the following section and are available from the CIPPIC website at <http://www.cippic.ca/> and follow the Identity Theft link.

- CIPPIC has published a set of working papers (see list below) on various aspects of identity theft/fraud, and is completing a draft set of recommendations for law and policy reform to circulate for feedback among the project's partners. CIPPIC has already submitted some recommendations to the House of Commons Standing Committee on Access to Information, Privacy and Ethics (see below). We also organized and hosted a one-day workshop on our research January 30, 2007, in which a number of public sector and private sector representatives participated and provided feedback on the research. CIPPIC has been attempting to gather Canadian ID Theft victim case studies this summer, but this has proven to be difficult.
- Professor Chandler has a forthcoming publication (see below), which contains a thorough review of U.S. jurisprudence on liability of data custodians (e.g. banks and retailers) to customers for breaches in the security of customer data. It considers how Canadian courts are likely to deal with this matter, as well as the advisability of using negligence law in this way to address identity fraud. She will be continuing in the autumn with the work on permissible limits of online self-help to deal with identity fraud involving internet-related techniques and forums.
- Professor Elizabeth Judge is completing her research on appropriation of personality and tort causes of action, and has a working version of a paper to be submitted for publication on this topic. She is also now researching public uses of personal information contained in 3d party submissions to government, and is preparing a paper for publication on this topic as well.
- Professor Valerie Steeves is currently surveying the political science, economics, sociology, and legal academic literature to identify any ethical, legal, or social implications that have been raised to date with respect to the use of biometric identification to combat identity theft. She has a draft publication, in final edits, to be submitted shortly for publication.

Documents and Publications:

1. CIPPIC Working Paper Series on ID Theft (published in March/April 2007):
 - No.1: Identity Theft: Introduction and Backgrounder
 - No.2: Techniques of Identity Theft
 - No.3: Legislative Approaches to Identity Theft
 - No.4: Caselaw on Identity Theft
 - No.5: Enforcement of Identity Theft Laws (in progress)
 - No.6: Policy Approaches to Identity Theft
 - No.7: Identity Theft: A Bibliography
2. CIPPIC White Papers
 - Approaches to Security Breach Notification: A White Paper I (January 2007)
3. Academic Publications (published and forthcoming):
 - Jennifer Chandler, "Negligence Liability for Breaches of Data Security", presented at:

November 2006 - Stikeman, Elliott, Toronto

January 2007 - ORNEC Workshop, Ottawa

February 2007 - University of Toronto, Faculty of Law

The paper has proceeded through peer review and revisions and is forthcoming in the Banking and Finance Law Review.

Philippa Lawson: “Privacy and Identity Theft”, presented at Riley Seminar on “Assessing Current Privacy Issues” held in Ottawa on Feb.21, 2007.

Mark Hecht, “Identity Theft in Canada“, presentation to Association of Certified Fraud Examiners, Quebec Chapter, Montreal, Quebec: June 01, 2007.

Mark Hecht, “Just who do you think you are? Identity Theft in the Age of New Technologies”, presentation to ORNEC Stakeholder meeting, Toronto, ON: June 6th, 2007

Valerie Steeves, “Criminalization of ID Theft: Social and Privacy Implications,” Legal and Policy Approaches to Identity Theft, Assessing Current Privacy Issues Conference, Ottawa, February, 2007.

Valerie Steeves, “What You (Don't) See is What You (Don't) Get: Identity Theft Provisions and the Invasion of Privacy,” Thinking about (In)justices: 1st International Symposium of the Centre for Justice Studies, Department of Criminology, University of Ottawa, April, 2007.

Valerie Steeves, “Criminalization ID Theft: Research, Activism and Social Policy,” Surveillance Summer Seminar, Surveillance Project, Queen’s University, Kingston, June, 2007.

Project #4: Technical Tools to Address the Identity Theft Problem

Research Team:

[Dr. Ali Miri](#), Associate Professor, and Director [Computational Laboratory in Coding and Cryptography \(CLiCC\)](#), SITE, University of Ottawa, (Principal Investigator),

[Dr. Abdulmotaleb El Saddik](#), Associate Professor, SITE, University of Ottawa

[Dr. Carkisle Adams](#), Professor, SITE, University of Ottawa

[Dr. Andrew Adler](#), Associate Professor and Canada Research Chair in Biomedical Engineering, Department of Systems and Computer Engineering, Carleton University

[Dr. Liam Peyton](#), Associate Professor, SITE, University of Ottawa

[Dr. Thomas Tran](#), Assistant Professor, SITE, University of Ottawa

[Dr. Paul van Oorschot](#), Professor and Canada Research Chair in Network and Software Security, School of Computer Science, Carleton University, [Digital Security Group](#)

Research Objectives:

This research proposal defines an advanced research program, using the ORNEC and CITO network of researchers, on technological aspects of the ID Theft problem. The proposal combines work in IT with research in management science and human decision making. Specifically, we propose to work on technologies that provide an infrastructure for secure IDs (biotechnology, digital credentials, trust management) with technologies that verify compliance with existing laws and detect potential instances of ID theft. The research team combines researchers from University of Ottawa, McMaster, and Carleton.

The research starts with a premise that technological tools can go a long way towards solving the ID Theft problem, and in some contexts may address it completely. In general, however, practical and comprehensive solutions will have to combine knowledge, processes, and procedures from business, law and IT to be deployable, effective, and socially acceptable.

In our research, we will evaluate alternative technical solutions to identity theft (e.g. digital signatures, PKI, smartcards, biometrics), and determine their effectiveness in a broad context, including their impact on privacy and other social values. We will propose and test new cost-effective technical solutions that improve upon existing solutions to identity theft. Research in this area is expected to lead to commercially viable applications in the computing and communications community. Another set of topics for which we will do technical work and draw on our colleagues from business and psychology for the societal and motivational aspects is how can security systems be designed to give consumers informed choice in the level of security they are provided (vs. risk that they are exposed to) in online transactions or other contexts? Is such choice desirable from a public policy perspective? How can systems designers ensure that consumers are in fact making informed decisions in such contexts?

We plan to coordinate this research with the user sector employing user workshops (one half way through the project, one in the final phase) as the vehicle and the venue for this coordination.

In order to focus the proposed project, we suggest the following definition of ID Theft (IDT): Identity theft occurs when one entity (Bob) illegitimately uses the identity of another entity (Alice) for his own purposes. Typically, this involves Bob impersonating Alice in one or more transactions for Bob's personal gain, though Bob may maliciously impersonate Alice with the sole intent of damaging or discrediting Alice, or Alice's reputation, in some way. In all situations, however, identity theft is possible when Bob is able to collect sufficient personal information about Alice that he can convince others that he is Alice

We propose here a research program that combines the expertise of several researchers that, for the most part, already cooperate within the ORNEC network. The proposal consists of projects that fall into three main themes and six projects with emphasis on collaboration among the various researchers involved:

1. **Theme #1 IDT Prevention:** Propose techniques to prevent identity theft, which includes biometrics and digital credentials. An interesting confluence here might be to consider having the biometric as one of the attributes in a digital credential, which a user can then choose to prove ownership of without having to reveal it.

Sub-project #1: Digital Credentials (Carlisle Adams)

Design and implementation of a novel framework for Digital Credentials

Sub-project #2: Biometrics (Ali Miri and Andy Adler)

Detailed design and development of privacy-enhanced biometrics framework and development specific use cases in the context of IDT

2. **Theme #2 IDT Detection and Recovery:** Design and development of techniques to notice in an automated way when identity theft is occurring and to provide some recourse to the affected user. This area includes profiling and legal compliance. The challenge here is to investigate whether the data mining and other techniques that allow profiling of the normal behaviour of the user population can also be used to profile an organization to determine its compliance with applicable laws

Sub-project #3: New Authentication Systems (Van Oorschot)

Explore and investigate the development of privacy technologies to counter ID Theft

Sub-project #4: Legal Compliance with Privacy Legislation (Peyton)

Explore, investigate and development Legal Compliance of Intelligent User Profiling with Privacy Legislations

3. **Theme #3 Usability Issues in IDT Protection Systems:** Implementation of techniques that allow the user to be actively involved in the identity theft protection process, which includes reputation assessment and TTP selection. An interesting convergence here is to see whether the tools that allow a user to compute the reputation and therefore the trust of a Web site can be used to assess whether a TTP should be trusted to hold the user's location data

Sub-project #5: Trust Management Systems (Tran)

Review and analysis of research literature on trust/reputation management systems and investigate, design and develop a privacy-enhanced Trust Management System

Sub-project #6: Intelligent User Profiling (El Saddik)

Analysis of the requirements and main challenges of intelligent profiling

Results to date:

1. Generic **architecture and protocol to detect identity fraud** has been discussed at the IDT Workshop #2 held in Ottawa on October 13, 2006. See presentation entitled "**Oorschot-Nali (CROO) IDTWkshp-2 Ottawa-13Oct06**".
2. Research on **legal compliance** focused on the need for users to have privacy and identity protection. The work addresses:
 - a. How to document and enforce legal compliance (e.g. generally accepted accounting practices and laws for disclosure of revenues and expenses) and relevant legislation (e.g. PIPEDA, PATRIOT Act, PHIPHA, Criminal Code)

- b. Existing Technology and Initiatives: liberty foundation (e.g. MS InfoCard, Shibboleth), privacy policies (e.g. P3P, EPAL, XACML) and information transfer registry. See presentation entitled **“Peyton (Legal Compliance) IDTWkshp-2 Ottawa-13Oct06”**.
3. Proposal for a **trust management** system as a means of privacy preservation for the prevention of ID Theft has been presented to the IDT Workshop #2 held in Ottawa on October 13, 2006. See presentation entitled **“Tran (Trust Management) IDTWkshp-2 Ottawa-13Oct06”**.
4. Work on **digital credentials** focused on modifying and extending PKI protocols to make them more privacy preserving and suitable for two practical, real-world types of people:
 - a. Business users (delegation of credentials in a corporate setting)
 - b. Ordinary users (use of a constrained device with limited memory and processing power)See the presentations entitled **“Adams (Digital Credentials) IDTWkshp-2 Ottawa-13Oct06”** and **“Adams (Digital Credentials) IDTMtg SITE-Ottawa-28Nov07”**.

Next-Generation PKI Technology to combat on-line credit card fraud

At the November 28 Workshop on the use of Digital Credentials technology to combat ID Theft, PKI Technology has been identified with its particular applicability to combating fraud during on-line shopping. Dr. Carlisle Adams and his fourth year undergraduate team demonstrated a software implementation of the work that has been done by two of his graduate students over the past year. Behind the simple one-step sign-on what appears no more complicated than a password entry lays a sophisticated authentication process based on extensions to the Digital Credential technology developed in 2000 by Stefan Brands at MIT. This process is based on PKI technology, blind signatures, and zero-knowledge protocols. A private key is provided to the customer when they activate their card or account. At the first time the card is used (activated), the client goes to the specified URL and is prompted to enter the authentication string which was mailed to her along with the new card. This string is used by the credit card company to look up the proper credit card number that was sent to the client. The digital credential software on the client platform engages in the issuing protocol with the website, which results in the client having a digital credential and CA signature on his/her computer or other device, which she can then use in subsequent shopping protocols with merchants. This is arguably no more cumbersome than the current requirement for people to phone a specified number (from their home phone) to activate their new credit card, but has the potential to be far more effective in reducing credit card fraud because possession of the credential and corresponding private key are needed in order to engage in an online purchase transaction (rather than mere knowledge of the credit card number and related information, as is the case today). Thus, a hacker who breaks into a database of credit card numbers, or who intercepts credit card numbers from wireless telephone calls, will be unable to use these numbers in a fraudulent way.

An additional advantage of Digital Credentials is that the public key can be used for transactions with other organizations without releasing unnecessary information. For example the client could prove that she was over 18 or over 65 without releasing any more information, ensuring privacy and limiting liability if records are subsequently compromised.

To date, the project has focused on developing and implementing four novel extensions to the DC technology. In the next phase of the project Dr. Adams plans to work through transactional scenarios from the perspectives of both the customer and the merchant.

Publications:

CAdams Proxy Paper CCECE (Can Conf in Elect & Comp Eng)-23-25Apr07 **ORNEC Identity Theft**

Workshops and Events

1. IDT Workshop #1 held at McMaster eBusiness Research Centre (MeRC) on Tuesday April 18, 2005. This was a kickoff meeting of ORNEC IDT research.
2. IDT Workshop #2 held at SITE, the University of Ottawa on Friday October 13, 2006
3. [MITACS Digital Security Seminar Series at Carleton University](#)
4. Thom Hounsell (CIBC) Visit SITE, University of Ottawa and Sprott School of Business, Carleton University. May 15, 2007
5. IDT Workshop #3 held in Toronto on Wednesday and Thursday June 6 and , 2007
6. IDT Meeting with Professor Carlisle Adams and his research team held at SITE, University of Ottawa Wednesday November 28, 2007

ORNEC Identity Theft Newsletters

1. ID Theft Newsletter Issue #1, March 2006
2. ID Theft Newsletter Issue #2, June 2006