

## Identity Theft Project

Measurement • Management • Policy • Tools

# Newsletter Issue 2, June 2006

Dear ORNEC Identity Theft Research Project participant,

Ironically as I sat down to write this newsletter I received a call from my back detailing \$6000 of bogus credit card charges made to my card. It is a shame that my bank is not yet a member of the IDT project.

Items to be covered in this newsletter will include:

- Working definitions of ID Theft coming out of the Measurement and Definition project following the discussions at the workshop.
- a brief summary of the IDT Workshop,
- use of The Privacy Network portal

- Updates on the projects
- Documents, conferences, news items etc.

### *Searching for Common Terminology* – Archer, Sproule

#### Introduction

As promised at our April 18 workshop, we have continued to work on developing a model of the IDT problem domain. (See Figure 1) Our objective in this exercise is to arrive at some common agreement on terminology that can be used in our various research projects.

Discussion at the workshop was based on a set of alternative models proposed in the discussion paper distributed with the workshop agenda. (A copy of the discussion paper can be found at <http://www.business.mcmaster.ca/IDTDefinition/defining.htm>.) The discussion centered

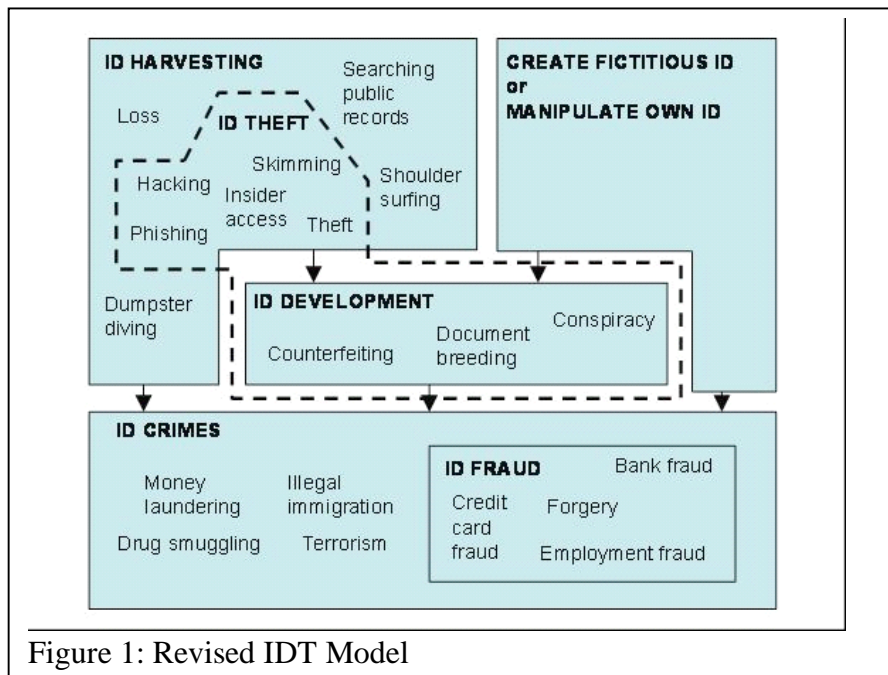


Figure 1: Revised IDT Model

around two interpretations of the difference between identity theft and identity fraud. In one model, identity theft was a subset of identity fraud. In the second model, identity theft was a precursor to identity fraud. It was noted that in any collection of definitions of identity theft you can see that some definitions include the *collection and use* of someone else's information, some the *collection* only and some the *use* only.

A poll of workshop participants showed a strong preference for a "process" model where identity theft precedes identity fraud. In other words, identity theft occurs when someone *collects* someone else's information and uses it to develop a false identity. Identity fraud occurs when someone *uses* a false identity to commit a fraud.

Above, you will see a revised model that incorporates this distinction as well as other

suggestions made at the workshop. Rather than trying to create definitions at this point, we show examples of activities that would belong in each construct.

To address the concern that some activities associated with the collection of personal information are not illegal (and will never be illegal), we introduce a concept called **ID Harvesting**. ID Harvesting includes all methods of collecting personal information. Some of these are legal (e.g. searching public records) while others are not (e.g. theft).

Other ways to create a false identity include the creation of a fictitious identity or manipulating one's own identity. While these activities generally are not included in definitions of identity theft, they pose similar problems and would be affected by many of the proposed solutions. They are included in the model so that they can be included in our discussions when appropriate.

We have introduced a concept called **ID Development**, which encompasses actions where the personal information collected in ID Harvesting is transferred or otherwise used to further develop a credible false identity. Examples of activities included in ID development are trafficking in identity information, document breeding, and counterfeiting.

Note that the model allows for the information collected in ID Harvesting to be used to commit *some* ID Crimes without further transfer or development. Similarly, a false identity based on a fictitious person or changes to one's own identity may also be sufficient for some crimes without further development.

It is suggested that the term **ID Theft** be used to describe any illegal activities (and activities that we would like to be illegal) within ID

Harvesting and ID Development. See items enclosed in the dotted line.

Finally, **ID Frauds** are a subset of a broader group of **Crimes Enabled by False Identity**. ID Fraud would include crimes where the main purpose of the crime is to gain money, goods, benefits or services, or to avoid obligations, and where the use of a false identity is *integral* to the crime. The broader set of Crimes Enabled by False Identity includes crimes where the use of a false identity is *peripheral* to a major crime such as drug trafficking or terrorism.

### Next Steps

We are asking everyone involved in the ORNEC research program to "test drive" this model. In particular:

1. Does your research or work experience fit into this model of the problem domain?
2. Can you use the terminology suggested by these constructs?
3. Are ID Harvesting and ID Development good terms to use or can you suggest alternatives?

Your answers to these questions and any other comments should be forwarded to Susan Sproule at [sprouls@mcmaster.ca](mailto:sprouls@mcmaster.ca). (In your responses, please include the time that it took you to review and comment so that we can credit this time for funding.)

We plan to put this model and its components on a Wiki so that we can collect ongoing input and feedback as we develop more specific definitions and build a library of examples and references for each construct. Look for a link to the Wiki, with initial "working definitions", in the last half of June. The link will be distributed by email and will be posted on <http://www.business.mcmaster.ca/IDTDefinit ion/defining.htm>.

## ***IDT Workshop – April 18, 2006 - Crawhall***

I would like to thank the many of you who contributed to the April 18 IDT workshop. It is an unusual opportunity to sit “in-the-round” with twenty knowledgeable people from many different backgrounds to discuss a topic in which you are professionally involved. Coming as it did at the beginning of most of the research programs, I expect the outcomes of the research to be significantly richer for it. The proposal around the model and definition of IDT Theft provided above is a good example of the richness of thought that can be brought to bear on a topic.

Detailed minutes have been issued thanks to Glenda’s extensive note taking. We also have the audio tapes from the session although they are of currently of unknown quality and consistency. Please contact Glenda if you are interested in them. [gmacdon@mcmaster.ca](mailto:gmacdon@mcmaster.ca) .

## ***The Privacy Network - Crawhall***

At the IDT Workshop Mike Gurski introduced us to “The Privacy Network”, a joint project with Bell Canada, Microsoft and the Centre for Innovation Policy and Law at the UofT. Several of you are already participants with this project. I have been working with Rebecca Johnston to set up a proprietary workspace for each of the four projects. Research outcomes can then be easily migrated to public space on the portal. On first blush the administration of the site was a bit more complicated than I would have liked. This is an early stage project and we have been working with the developers to make it easier to use and manage. I encourage you to check out [www.theprivacynetwork.org](http://www.theprivacynetwork.org) and to register as a member. Once you are a member I can set up privileges to let you into the ORNEC IDT

area. Partner logos etc. will soon be in place on the site.

## ***Prospective Protective Futures Security Workshop - Crawhall***

On March 27-29 the Office of the National Science Advisor’s Science & Technology Foresight Directorate hosted a workshop on security that looked at several future security scenarios. I was on the team looking at a Mass Identity Theft scenario associated with an international sporting event. While we, the crooks, were all amateurs (so far as I could tell) many of the “good guys” had a professional intelligence and law enforcement background. The perpetrators were an international crime family and the authorities were given a set of tools to use to catch us.

We focused the biometrics of the wealthy and the influential, targeted people not resident in Canada, developed a number of stratagems to collect fingerprints, dna etc. through venues such as bars and restaurants. The objective was to collect a complete a biometric picture of the targeted individuals. Data would be used for security breaches overseas or sold to other criminal organizations.

The conclusions were that:

- 1) Stopping this theft would be very difficult.
- 2) Once you have a biometric picture of someone the threat lasts for a long time.
- 3) Technologies readily accessible to criminal gangs such as wireless communications, distributed data bases, encryption etc. combined with a global operational footprint stresses the current approaches to law enforcement.

## ***Project Reports***

## 1) Defining and Measuring Identity Theft – Archer/Sproule

Our project team has been working on a number of follow-up items from the first workshop. We have also set up a project Web site to share files and information at <http://www.business.mcmaster.ca/IDTDefinit ion>. There is also a link to this site from the MeRC site under “Projects”.

### Defining Identity Theft

As discussed at our first Workshop, we are trying to create a model of the IDT problem domain so that we can all agree to use some common terminology in our various projects. Suggestions from the workshop have been worked into a refined version of the model. See the separate article in this newsletter. We now need to hear from you!

### Measuring Identity Theft in Canada

Ken Deal, Norm Archer and Susan Sproule have begun to design the consumer survey. All of the survey respondents will be asked about their perception of the identity theft problem, what (if any) preventative measures they are taking, and what potential measures they would find acceptable. Preliminary questions about preventative measures were circulated to a cross-section of university, industry and public sector representatives for comments and suggestions.

A copy of these questions, and others as they are developed, can be viewed on our Web site at <http://www.business.mcmaster.ca/IDTDefinit ion/measuring.htm>. We would be interested in comments and suggestions from anyone involved in the research program.

The survey will be conducted through an Internet panel. We hope to have a large enough sample to generate between 500 and

600 victim reports. A set of questions for victims are still being developed. These questions will collect information about how the theft took place, the types of fraud committed, detection, reporting and costs.

### Bibliography

The bibliography used for our discussion paper is currently available in text, RefWorks\* or EndNote formats. See <http://www.business.mcmaster.ca/IDTDefinit ion/lit&links.htm> or contact Susan Sproule at [sprouls@mcmaster.ca](mailto:sprouls@mcmaster.ca).

Susan would also like to receive any bibliographic files (EndNote, RefWorks or other formats) that other researchers have collected on the subject of identity theft. Where possible, she will integrate these files into a comprehensive bibliography that can be updated on a regular basis and made available to all.

\* RefWorks bibliographic software is licensed at all Ontario universities. See your librarian for information. RefWorks will allow a bibliography to be “shared” which means that it can be printed, exported, or used to generate a RefWorks bibliography for the recipient.

## 2) Management Approaches to Combating Identity Theft

(Dr. Yuan is in China and will provide his report in the next issue – Ed.)

## 3) Legal & Policy Approaches to Identity Theft - Lawson

A Research Assistant (Thomas Legault, a first year law student) has been hired and is now working full-time with Wendy Parkes, Senior Research Associate. Following several weeks of research, four draft papers have been produced: 1) Introduction and Backgrounder 2) Inventory of Identity Theft Techniques 3)

Inventory of Legislation and 4) Inventory of Government, Corporate and Consumer Practices which facilitate and impede Identity Theft. These papers will be circulated in early June for review and comment to participants in the ORNEC Identity Theft Project. Relevant caselaw has also been identified, to form the basis for a fifth paper. These papers will be refined and expanded over the summer. In addition, background material for the CIPPIC webpage on identity theft has been collected.

#### **4) Technical Tools To Address Identity Theft** - Miri

The team is up and running. 10 graduate students, and 2 postdocs are currently working on different sub-projects, several of them are new recruits.

Two conference papers are to be presented over the summer, and a few more are in preparation.

We have approached the executive committee of Privacy Enhancing Workshop about holding the next year workshop here in Ottawa. We should get the final word in couple of weeks at the end of this year workshop.

We have had discussion with the director and other people in University of Montreal graduate program in E-business about having a common workshop (possible in conjunction with PET workshop). We are still trying to work out the best way to proceed.

-I had a meeting with Pippa. We discussed some possibilities of collaboration, and I already have one student working on one of them (hopefully we can build on that). Abed mentioned that he has had some discussion with School of Management as well, although I am not sure at what stage that is. I still need to

follow with people at McMaster as well (I did talk to Andy and Paul specifically about contacting them based on the interest expressed in our meeting in Hamilton and emails thereafter)

#### **Identity Theft In the News**

- May 10, 2006: President Bush signs an Executive Order creating an "Identity Theft Task Force" to bring together the various US federal resources and agencies that are working on this problem.  
<http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html>  
<http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html>  
<http://www.whitehouse.gov/news/releases/2006/05/20060510-2.html>
- May 20, 2006: Veterans Affairs announces massive data breach including names, date of birth and social security numbers of 27 million veterans.  
<http://www.firstgov.gov/veteransinfo.shtml>
- Scoping Identity Theft; Rebecca T. Mercuri, Communications of the ACM, Vol49, Issue 5 May 2006. ISSN:0001-0782 . The computer's role in identity theft incidents may have been misgauged through overestimates of reported losses.  
<http://portal.acm.org/citation.cfm?id=1125944.1125961&coll=ACM&dl=ACM&idx=1125944&part=periodical&WantType=periodical&title=Communications%20of%20the%20ACM&CFID=72709251&CFTOKEN=20959744>
- Tough penalties sought to rein in retailers flouting privacy laws; Nestor E. Arellano; IT World Canada May 5, 2006, "Be careful with the secrets you reveal to on-line retailers. You just don't know where your personal data could end up and how it might be used.... the warning issued by Ottawa-based Canadian Policy and Public Interest Clinic (CIPPIC) following its release of a

survey that showed "widespread non-compliance with federal privacy laws."

<http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?id=idgml-7b8fbc6c-a78e-49f5&Portal=448d158c-d857-4785-b759-ffa1c005933c&s=334469>

## *Conferences & Seminars*

- **Identity and Identification in a Networked World: A Multidisciplinary Graduate Student Symposium.** September 29-30, 2006, New York University  
Submission deadline: July 5, 2006. The symposium will feature a keynote talk by Ian Kerr, Canada Research Chair in Ethics, Law & Technology at the University of Ottawa.

## *Distribution of Newsletter etc.*

This newsletter is distributed using the "blind cc" email feature. It is intended for the use of participants in the ORNEC Identity Theft project. It is not for public posting. Members are free to distribute the newsletter to others within their organizations. For additions or deletions to the distribution list please reply to [crawhall@ornec.ca](mailto:crawhall@ornec.ca) or [admin@ornec.ca](mailto:admin@ornec.ca). – Robert Crawhall