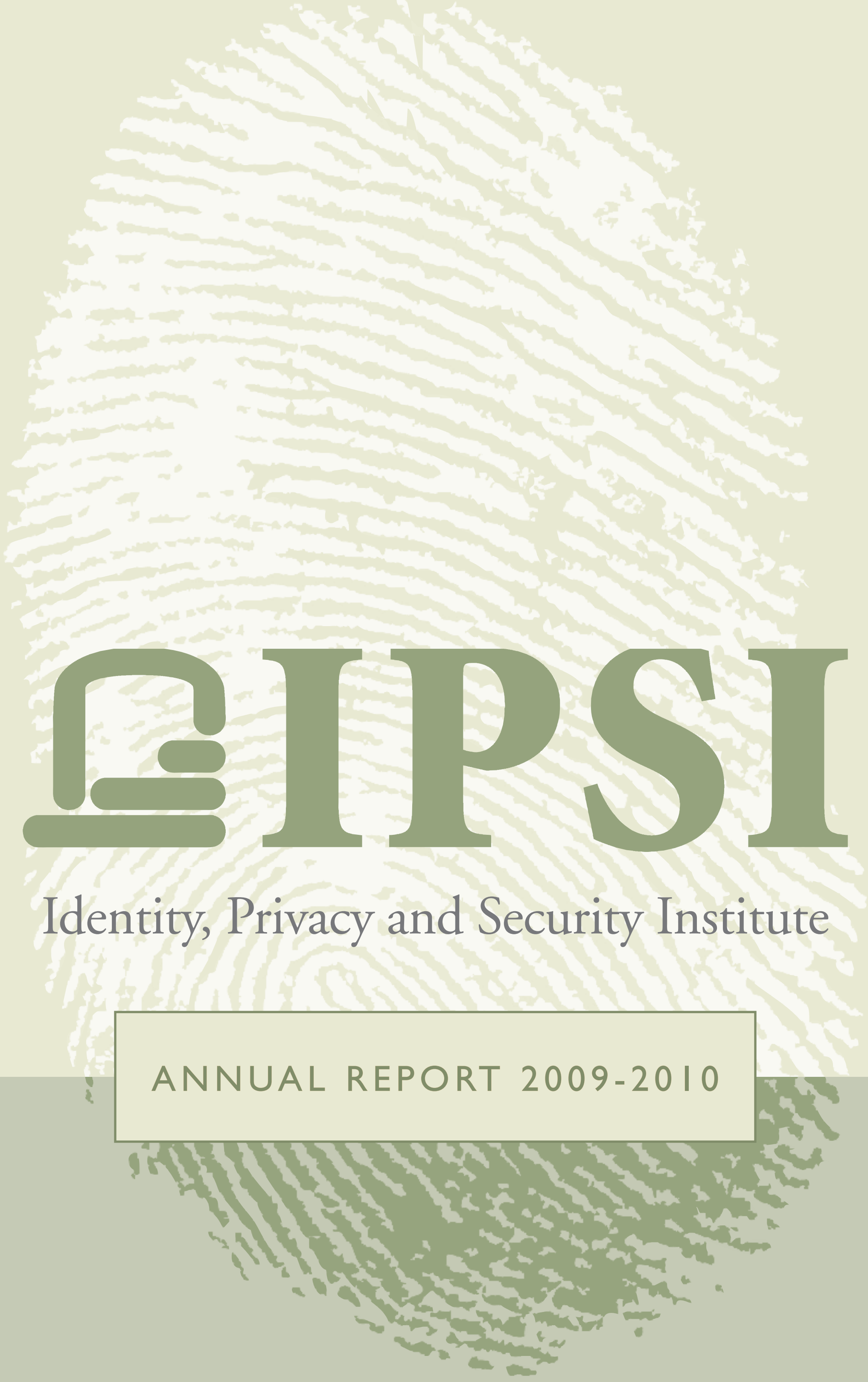


IPSI

Identity, Privacy and Security Institute

ANNUAL REPORT 2009-2010

UNIVERSITY OF TORONTO

CONTENTS

ABOUT IPSI

The Identity, Privacy, and Security Institute (IPSI) was established in 2007 with the support of the University of Toronto's Academic Initiatives Fund to be a leading interdisciplinary Canadian research institution exploring issues of Identity, Privacy and Security. Through the administrative support of the Faculty of Engineering and in partnership with the Faculty of Information, IPSI's research community spans the humanities, social sciences, technology and the sciences. IPSI's academic collaborators also include faculty from Medicine, Arts and Science, and Law. This diverse community considers not only the applications, policy, and social implications of today's identity, privacy, and security issues but also considers tomorrow's challenges. IPSI's pioneering interdisciplinary program of research, education, outreach, industry collaboration, and technology transfer is focused on developing new approaches to privacy that maintain the security, freedom, and safety of the user and the broader community.

IPSI continues its mandate through:

- the delivery of public seminars, workshops, and symposia that share research and insights and foster dialogue
- the delivery of formal education programs such as the M.I. concentration in Security Policy, the M.Eng. concentration in Security Technology and the developed IEEE sponsored education series on Biometrics
- the continued research in collaboration with academic members, policy and industry partners

IPSI is governed by a management committee of academics responsible for the day-to-day operations and strategy. IPSI's advisory committee is currently comprised of partners from government and industry and provides guidance for IPSI's strategy and support for IPSI projects.

IPSI'S OBJECTIVES FOR 2010

IPSI was founded to:

- advance the integration of the basic, social, and engineering science research required to generate sustainable solutions to identity integrity, privacy, and security
- assemble a cross-disciplinary community of researchers and community partners to create excellence in interdisciplinary research and education in the field of identity, privacy, and security technologies, policies, and sciences
- provide the interdisciplinary high-level training in identity, privacy, and security applications of related technologies, policies, and sciences
- facilitate the commercialization of technologies through effective technology transfer mechanisms and industrial partnerships
- work with policy-makers and regulatory agencies
- inform their judgment of identity, privacy, and security realities with evidence-based considerations of the scientific, ethical, legal and social issues involved

Building on IPSI's initial foundational years, the management team will focus in the coming year on three main areas:

- continuing outreach activities and growing partnerships both within the university and externally to engage a multitude of disciplines and embark on industry-relevant collaborations
- securing revenues for growth beyond the term of the AIF funding through specific industry research collaborations and new funding opportunities
- building the IPSI brand and establishing IPSI as a pre-eminent centre for research and exploration of the identity, privacy, and security challenges faced by society today and those challenges that will arise with the developments of tomorrow

MESSAGE FROM THE CHAIR OF THE ADVISORY COMMITTEE

I would like to congratulate everyone at IPSI for another successful year! As information and communications technologies continue to advance unabated, so does the amount of personal information that is collected and stored – the challenges that we face in maintaining our privacy and freedom will only grow more complex. I believe that IPSI is perfectly situated to find answers to those challenges and I am proud to be participating in a program that will take the relationship between privacy, security and technology well into the 21st century.

With regards to the future, I am predicting that we only have 10 years: unless we begin to look at privacy through a new lens, we will not continue to enjoy our privacy, as we know it, in future decades. In my 20 years as a privacy professional, the greatest impact has come from the explosive growth of information and communication technologies – more specifically, the rise of online social networking, accompanied by the explosion in mobile devices and wireless communications. The IT revolution not only brought with it a myriad of advances with everyday benefits to society, but also gave birth to an entire new catalogue of privacy concerns as a result of increasingly sophisticated data mining techniques.

The future of privacy will require a paradigm shift – compliance with laws and regulations alone will no longer be sufficient to ensure our privacy. I have consistently advocated for taking a Privacy by Design approach, whereby privacy is proactively embedded directly into the design of technology and business practices – as the default option. Privacy by Design (PbD) also shatters the zero-sum paradigm in which privacy is traded off in favour of security, or other functions. In that sense, PbD is doubly-enabling or positive-sum ("win-win") in nature.

The concept of PbD has attracted the attention of officials globally. Viviane Reding, Vice-President, Justice, Fundamental Rights and Citizenship, of the European Commission, speaks of how PbD will increase consumer trust. Peter Hustinx, European Data Protection Supervisor, calls for PbD to be incorporated into the framework of revisions to EU data protection legislation. In the United States, Federal Trade Commission Chairman Jon Liebowitz describes PbD as the first of three key principles of online privacy. But let us not forget the enormity of the task ahead – convincing governments and businesses of the merits of adopting Privacy by Design, on a day-to-day basis – is indeed a Herculean task.

In conclusion, I again offer my congratulations to all of IPSI's staff and researchers, for another great year. Events and developments of particular note included: IPSI's successful 2010 Research Symposium which explored "Developing a trusted cyber-infrastructure for Canadians;" the naming of Professor Konstantinos Plataniotis as a Fellow of the Engineering Institute of Canada, for his exceptional contributions to the field of engineering in Canada; and the publication of SmartData: Make the data "think" for itself: Data protection for the 21st Century, in the Journal of Identity in the Information Society. SmartData's highly innovative approach to protecting privacy will create the strongest form of protection possible, and place it directly in the hands of the individual – personal control at its best.

We have much reason to be proud, and I have every confidence that we will have another exemplary year because IPSI has proven to be a world-class organization in the study of privacy, security and technology.

ANN CAVOUKIAN, PH.D.
Information and Privacy Commissioner of Ontario, Canada

MESSAGE FROM THE ACADEMIC DIRECTOR

It is a pleasure to share IPSI's accomplishments during its third year of operation. We have continued delivering our educational activities, been active in building our team and creating new partnerships, and embarked on new and exciting research initiatives in Identity, Privacy and Security.

We have made a concentrated effort to engage public and private sector partners to participate in the development of joint research projects and the submission of research proposals. The response from associates, collaborators and partners has been enthusiastic. Our coordinated efforts have resulted in the submission of four major proposals in the NSERC Research Partnerships and Strategic Project grants programs and many smaller proposals to other sponsors.

One of the most visionary endeavours this year has been our work on "Smart Data". The objective of this research initiative is to develop web-based evolutionary agents that will securely store personal or proprietary data, and protect the privacy and security of the data in accordance to proper authorization. This has become a focus research area for IPSI and has resulted in preparation and submission of a funding proposal to the NSERC Strategic Project Grants program.

Our continued outreach to the potential members in other faculties and institutes has engaged new collaborators in areas as diverse as e-Health, Political Science, and Physics. We have significantly increased our collaborative activities with the Knowledge Media Design Institute (KMDI). We have successfully engaged public and private sector partners to participate in the development of a proposal for the recent NSERC CREATE round of applications.

The fall public lecture series was once again a success attracting attendees from academia, the private sector and government. Our Research Symposium was held May 10 with Dr. Stefan Brands as keynote speaker. We have also co-organized with KMDI a Digital Economy Roundtable to respond to the federal government's call for submissions. Over 30 identity and security professions collaborated on a document which was submitted to the federal government.

We have significantly improved our communication avenues. All public events including the fall public lecture series and the spring Research Symposium were recorded and are available online as a searchable archive. The symposium was webcast live and viewers could participate.

Offering of joint Master's degrees with concentration in security technologies (M.Eng.) and policies (M.I.) was continued. Next year we plan to increase the visibility of these programs, improve their educational role in areas of high interest to IPSI, and attract more students. Our vision is to provide true interdisciplinary training and involve our industrial and private partners in the training process.

I would like to take this opportunity to thank anyone who has contributed to a successful year for IPSI. Also, I wish to thank the Faculty of Applied Science and Engineering, the Department of Electrical and Computer Engineering and the Faculty of Information at the University of Toronto for their support. With the AIF funding ending this year, the major challenge for the next few years is to ensure sustainability of the institute by attracting new partners and funding. This can only be achieved by continuing to offer quality educational activities and innovative research initiatives.

DIMITRIOS HATZINAKOS, PH.D., P.ENG.
Director, IPSI
Professor, ECE Department, Faculty of Applied Science and Engineering, University of Toronto

MANAGEMENT COMMITTEE

Dimitrios Hatzinakos, M.A.Sc., Ph.D.
Chair and Academic Director
Professor, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

Andrew Clement, B.Sc., M.Sc., Ph.D.
Policy Director
Professor, Faculty of Information
University of Toronto

Kostas Plataniotis, B.Eng., M.S., Ph.D.
Research Director
Professor, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

ADVISORY COMMITTEE

Ann Cavoukian, Ph.D.
Chair, Advisory Committee
Information and Privacy Commissioner of Ontario

Richard Alvarez
President and CEO, Canada Health Infoway

Ken Anderson
Assistant Commissioner, Office of the Information and Privacy Commissioner of Ontario

Dean Barry
Manager, Security Policy and Identity Management
Public Safety Canada

Stefan Brands
Founder and CEO, Credentica

Yim Chan, CIPP/C
Global Privacy Executive, IBM Corporation
Chief Privacy Officer, IBM Canada

Richard Owens
Counsel, Stikeman Elliott LLP
Adjunct Professor, Faculty of Law, University of Toronto

Angela Power
Senior Privacy Consultant, Bell Canada

Arthur Smith
Founder and CEO, GS1 Canada

George Tomko
Expert-in-Residence for Cognitive Agent Development
Neuroscientist

EDUCATIONAL INITIATIVES

IPSI is spearheading a number of exciting educational initiatives aimed at helping to address the need for informed professionals. Below are descriptions of our graduate courses.

MASTER OF ENGINEERING (M. ENG.) IN COMMUNICATIONS WITH FOCUS ON INTEGRATED SECURITY TECHNOLOGIES

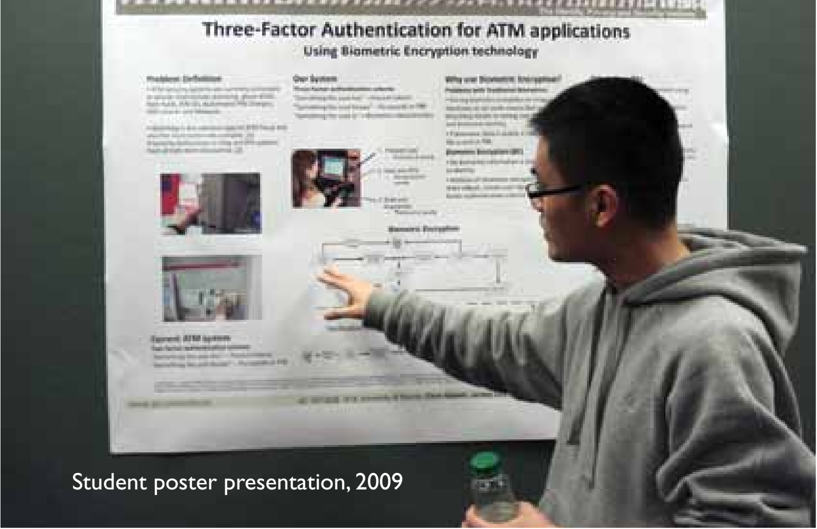
A recent census indicates that Canada has over 700 information and communications technology (ICT) security companies. Demand for qualified IT security staff is growing fast, with the global total of professionals expected to increase to 2.1 million by 2008 at a compound annual growth rate of 13.7% from 2003.

The M.Eng. focuses on Integrated Security Technologies and Policies aims to provide interdisciplinary training in the new era of security technologies which requires “IS Professionals”, that is, engineers with a comprehensive know-how and a holistic understanding of security technologies, policies and sciences.

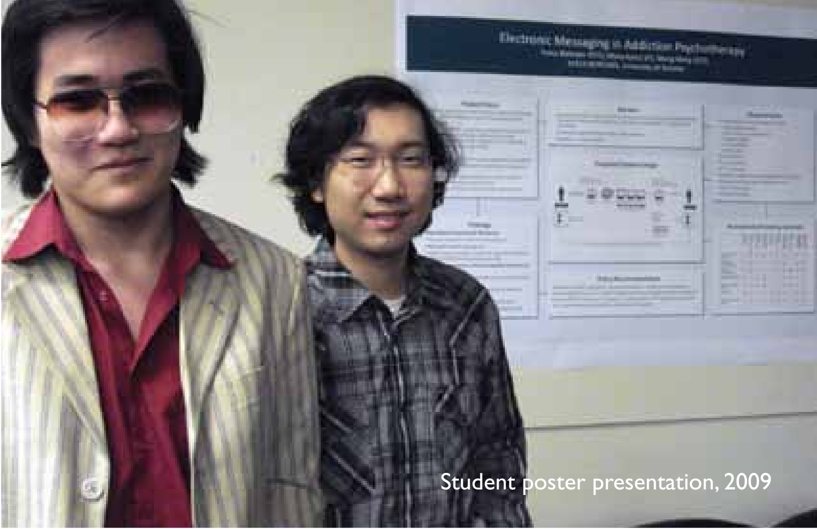
MASTER OF INFORMATION (M.I.) WITH FOCUS ON IDENTITY, PRIVACY AND SECURITY

Identity, privacy and security are a set of closely related socio-technical issues of growing importance in contemporary, networked society. The Identity, Privacy and Security Institute at the University of Toronto was established to carry out a pioneering, interdisciplinary program of research, education, outreach, industry collaboration and technology transfer around the complex interplay of these focal issues. The overall goal of IPSI is to develop new approaches to security and identification that maintain the privacy, freedom and safety of the user and the broader community.

The Identity, Privacy and Security (IPS) curriculum is intended mainly for students who want to take the Identity, Privacy and Security specialization offered jointly by the Faculty of Information and the Department of Electrical and Computer Engineering (ECE).


Three-Factor Authentication for ATM applications
Using Biometric Encryption technology

Student poster presentation, 2009



Student poster presentation, 2009

Student poster presentation, 2009

Dr. Ann Cavoukian, Ontario Privacy Commissioner

David Lie, Dept of Electrical & Computer Engineering, U of T

Andrea Slane, University of Ontario Institute of Technology

Stefan Brands, Credentica

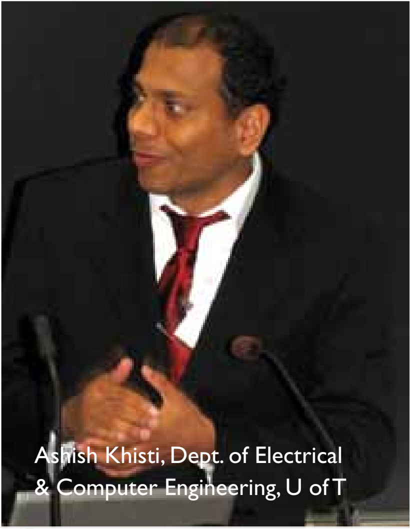
Ron Deibert, CitizenLab, U of T

Matt Ratto, Faculty of Information, U of T

Andrew Clement, Faculty of Information, U of T

Student poster presentation, 2009

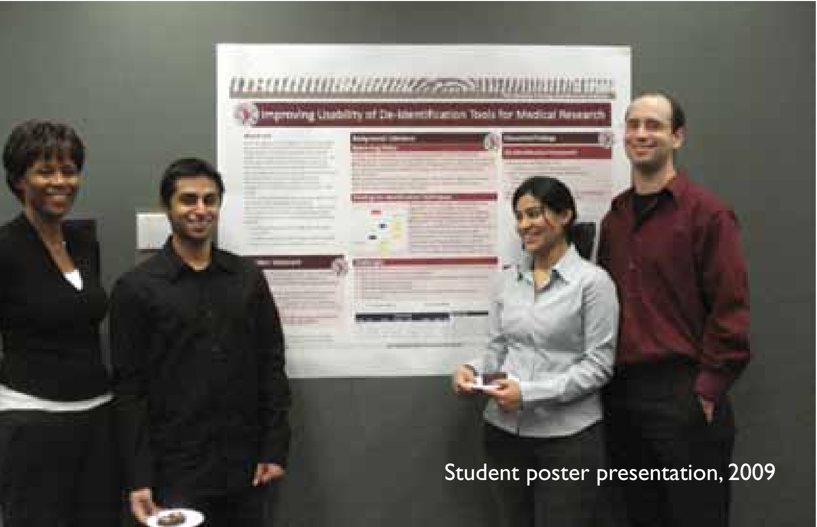
Guy Herriges, Office of the Chief Information & Privacy Officer, Ontario


Ashish Khisti, Dept. of Electrical & Computer Engineering, U of T

Carlisle Adams, University of Ottawa

Al Leon-Garcia, Dept. of Electrical & Computer Engineering, U of T

from left to right: Catherine Johnston (ACT Canada), Stewart Aitchison (U of T), Maria Athina Martimianakis (U of T), Matt Ratto (U of T)


Improving Usability of De-Identification Tools for Medical Research
Student poster presentation, 2009

Catherine Johnston, Advanced Card Technologies [ACT] Canada

Lisa Austin, Faculty of Law, U of T

PUBLIC SEMINAR SERIES

In keeping with IPSI's interdisciplinary approach, our third public seminar series featured experts from engineering, sociology, law, information science, and security fields.

Andrew Clement, Professor, Faculty of Information, University of Toronto
Toward Secure, Privacy Sensitive ID/ Authentication

Kostas Plataniotis, Professor, Department of Electrical and Computer Engineering, University of Toronto
Introduction to Biometrics for ID and Authentication

Roger Clarke, Xamax/Visiting Professor, Australian National University/Australian Privacy Foundation (Chair)/Australian Computer Society
A Sufficiently Rich Model of (Id)entity, Authentication and Authorization

David Lyon, Professor, Queen's Research Chair, Sociology, Queens University
Identifying Citizens: ID Cards as Surveillance

Carlisle Adams, Professor, School of Information, Technology and Engineering, University of Ottawa
Credential Systems: Promise, Risks and Possible Mitigations

Lorrie Cranor, Program Director, Carnegie Mellon University, CyLab/Engineering and Public Policy/Institute for Software Research/School of Computer Science
Usable Privacy and Security

Dmitry O. Gorodnichy, Senior Research Scientist and Group Leader, Video Surveillance and Biometrics Technologies, Applied Research and Development Division, Laboratory and Scientific Services Directorate, Canada Border Services Agency
Recognition in Video

Ian Kerr, Professor, Canada Research Chair in Ethics, Law and Technology, University of Ottawa, Faculty of Law/Faculty of Medicine/Department of Philosophy
All Smile and No Cat? How Soft Surveillance and Ubiquitous Computing Challenge Privacy and Anonymity

IPSI RESEARCH SYMPOSIUM

In May 2010, IPSI hosted a full day symposium that tackled the thorny and often-ignored subjects of online privacy and security. This event delved into both present day and proposed future methods intended for securing online identities, as well as the many legal, social and economic consequences resulting from the failure to deliver on user expectations of a trusted infrastructure.

Keynote Presentation: The Future of Digital Identity
Stefan Brands, Credentica

Panel: Response and Discussion

Chair: Andrew Clement, Professor, Faculty of Information; Policy Director, IPSI, University of Toronto
Respondents: Ann Cavoukian, Commissioner, Information and Privacy Commissioner of Ontario
Ashish Khisti, Professor, Electrical and Computer Engineering, University of Toronto
Guy Herriges, Manager, Access, Discovery and Business Recordkeeping, Office of the Chief Information and Privacy Officer, Government of Ontario

Session I: Protecting Identity and Privacy in Cyber-Infrastructure Use: Ubiquitous Surveillance, Anonymity and De-Identification

Chair: Konstantinos N. (Kostas) Plataniotis, Professor, Electrical and Computer Engineering; Director, Knowledge Media Design Institute; Research Director, IPSI, University of Toronto
Speakers: Ruth Vale, Senior Analyst, Privacy, eHealth Ontario/Smart Systems for Health Agency
Peter Pennefather, Professor, Leslie Dan Faculty of Pharmacy; Academic Director, Laboratory of Collaborative Diagnostics, University of Toronto

Karl Martin, Researcher, Multimedia Lab, Electrical and Computer Engineering, University of Toronto

Session II: Developing Trust in Critical Cyber-Infrastructure: Open, Public, Secure Networks??

Chair: Al Leon-Garcia, Professor, Electrical and Computer Engineering, University of Toronto
Speakers: Ron Deibert, Professor, Political Science; Director, Citizen Lab, University of Toronto
Lisa Austin, Professor, Centre for Innovation Law and Policy, Faculty of Law, University of Toronto
David Lie, Professor, Electrical and Computer Engineering, University of Toronto

Session III: Interdisciplinary Collaborative Research and Training: Bridging the Gaps

Chair: Dimitris Hatzinakos, Professor, Electrical and Computer Engineering; Chair and Academic Director, IPSI, University of Toronto
Speakers: Matt Ratto, Professor, Faculty of Information; Director, Critical Making Lab, University of Toronto
Maria Athina Martimianakis, Lecturer, Department of Paediatrics; Fellow, Department of Psychiatry and Wilson Centre for Research in Education, University of Toronto
Stewart Aitchison, Vice-Dean (Research), Faculty of Applied Science and Engineering; Professor, Electrical and Computer Engineering, University of Toronto
Catherine Johnston, President and CEO, Advanced Card Technologies (ACT) Canada

Readers can now stay in touch with IPSI's initiatives and other privacy and security news in three ways: through our web page; by joining our listserv, IPSI-L; or on Twitter: IPSIns.

DIGITAL ECONOMY ROUNDTABLE

The federal government recently held a public consultation on the Digital Economy, inviting:

"views on the goals of a Canadian digital economy strategy, the concrete steps needed to reach these goals and how governments, the private and not-for-profit sectors can best collaborate to create a strategy for future success."

The specific themes mentioned in the consultation document were:

- Innovation using digital technologies
- Digital infrastructure
- Growing the ICT industry
- Canada's digital content
- Building digital skills

In response, Andrew Clement (IPSI/Faculty of Information) and Karen Louise Smith (Knowledge Media Design Institute) convened a roundtable discussion to discuss these five themes and collaboratively prepare a "consensus" submission in advance of the July 9, 2010 deadline.

Three forms of participation were offered:

1. Contributing to the submission draft document online using a wiki;
2. Attending a roundtable June 14 at the University of Toronto, where small break-out groups focused on the five consultation themes and drew upon the contributions already posted to the wiki;
3. Endorsing (in full or in part) the interim submission before July 9.

The roundtable was sponsored by the Identity Privacy and Security Institute (IPSI), Knowledge Media Design Institute (KMDI) and Faculty of Information (FI) at the University of Toronto.

More than 30 experts in information and communication technology took part in the roundtable and the document was submitted to the federal government on July 9. The executive summary includes the following recommendations:

- Focus on developing a foundation for innovation across the entire economy and not just large private sector organizations;
- Provide affordable access to open, neutral, high-quality broadband networks;
- Provide open and free access to all publicly-funded research publications and public sector information;
- Develop digital skills through programs based on principles of accessibility, continuity, and flexibility;
- Promote innovation through open, neutral networks.

The full document can be read at:
http://de-en.gc.ca/wp-content/themes/clf3/upload/121/2010July9_DigEconSubmissionFinal.pdf

RESEARCH

SMARTDATA: MAKE THE DATA "THINK" FOR ITSELF

On the front page of the Ottawa Citizen this summer, our chairperson Dr. Ann Cavoukian, was headlined as stating, "The World is Losing Grip on Privacy." In this article, she said that "the world has less than a decade to make protection of personal information and online privacy a priority before the concepts are lost forever … legislation meant to safeguard privacy already can't keep pace with the flow of information and advances in technology." She went on to frame this as, "a David vs. Goliath issue." SmartData is an attempt to create "artificial Davids" for individuals in order to give them control over their information in a cyber-world. By transforming one's data into a digital servant or "virtual agent" which will do one's bidding, SmartData will become an embodied proxy for each individual and their personal information, even when they are not present and attempts to access their information are made half way around the world. SmartData is presently the subject of a multi-disciplinary research program in the Identity, Privacy and Security Institute at the University of Toronto.

The concept of privacy as an individual right is coming under great pressure from the prevailing paradigm that privacy and public safety are a zero sum game – the view that public safety is enhanced by governments having access to more personal information, and that "too much" privacy presents a threat to national security. Furthermore, corporations are realizing that the effectiveness of their business systems can be improved by having virtually unfettered access to personal data, which can lead to greater profitability. These views have resulted in increasing demands to obtain and store personal information of all kinds, especially in light of increasingly sophisticated data mining techniques where valuable "nuggets" of information may sometimes be found using elements of one's personal data set, initially collected for no *primary* purpose whatsoever. As a result, organizations are attempting to accumulate as much personal information as possible, whether or not they have a use for it at the time of initial collection. This has led many governments to prioritize gaining access to personal data in their war on terrorism, above the right to privacy.

Corporations with access to personal information and private communications are also coming under subtle and, at times, outright pressure from governments to share this data with them in the name of public safety – sometimes without informing the data subject. It is becoming more the rule now, rather than the exception, that whatever personal data corporations collect may eventually be made available to governments. Individuals are rapidly losing control over their personal information; as this situation escalates in more and jurisdictions, the world will increasingly lose its grip on privacy.

Current technologies that embody a positive sum paradigm whereby both privacy and public safety or business effectiveness are preserved will have a very difficult time in penetrating the marketplace. In order for privacy enhancing technologies to gain entry into the marketplace requires that they be adopted by the very same governments and corporations that want easy access to personal data. However, since by design, privacy-enhancing technologies will restrict unfettered access, and, generally make it more difficult for governments and corporations to acquire such data, it will be a "hard" sell. Presently, in the public safety and security arena, governments do not have to obtain anyone's consent to access data. And they certainly would not favour technology that placed obstacles in their acquisition of such data. Similarly, corporations would not want to place additional hurdles in the way of collecting more personal information for their business practices. The current situation appears to be one where the rabbits are in charge of the lettuce, so to speak, and clearly would not want to finance fences to prevent them from having continued unfettered access. What is needed is privacy-enhancing technology that can be rolled out by businesses directly to individuals, and which is not dependent on the support of organizations that want to gain access to the data. SmartData is an attempt to fill this market niche.

SmartData is a research program which will endeavour to place individuals in control of their own information, subject to existing laws – meaning that if an individual does not consent to the release of his/her personal information, then only a court order or warrant to release the information would grant such access. Its goal is to develop web-based intelligent agents that will securely store an individual's personal and/or proprietary data, and protect the privacy and security of that data by only disclosing it in accordance with instructions authorized by the data subject. The vision consists of a web-based SmartData agent that would serve as an individual's proxy in cyberspace to protect their personal or proprietary data. The SmartData agent (which 'houses' the data and its permitted uses) would be transmitted to, or stored in a database, *not* the personal data itself. In effect, there would be no personal or proprietary "raw" data out in the open – it would instead be housed within a SmartData agent, much like we humans carry information in our "heads;" and extending this analogy, it would be the "human-like clone" that would be transmitted or stored, not the raw data.

The key to the "smart" in SmartData is context – the ability for an artificial agent to release personal information based, not only on a set of programmed rules, but on an interpretation of the situation behind the request. This property of contextual decision-making, which presents the major challenge in this program, has led us in the direction of incorporating the advances made in the technology of simulating virtual worlds together with the ideas in the field of evolutionary robotics and embodied cognition within a framework of chaotic dynamical systems into our research. In exploring the issue of context using the model of non-linear dynamics, we believe that many of the other difficulties involved in developing artificial agents will start to be addressed.

Over the past year, a considerable amount of activity has taken place: an introductory paper on Smart Data was published; an NSERC grant proposal with HP and GS1 as industrial partners has been submitted, and presentations on SmartData were made to a number of organizations: Google, IBM, HP, GS1, GENI, Linden Labs of Second Life, and the Identity in the Information Society conference in Rome. The purpose of these efforts is to recruit research partners across a wide spectrum of academia and industry, to form a multidisciplinary team in our pursuit of a truly challenging goal. As a result of these presentations, our group has been invited to give a presentation to researchers at the IBM Watson Lab in Armonk, to explore the potential of future collaboration. We are currently in the process of writing a proposal which will form the basis of our presentation to IBM. It should be an interesting year.

GEORGE TOMKO
IPSI, Expert-in-Residence for Cognitive Agent Development

ONGOING RESEARCH PROJECTS

BIOMETRIC USER-CENTRIC SENSOR NETWORKS (BUSNET)

Researchers: Dimitrios Hatzinakos and Kostas Plataniotis (NSERC Strategic Research Project)
Industry Partners: DRDC Toronto, Bell Canada

The aim of the project is to develop integrated security architecture to effectively and efficiently secure and protect sensitive information and data within the domain of a care enterprise such as wireless health care and home care applications and services. Specifically, this research initiative will be examining issues and developing solutions for processing of biometrics signals, biometrics registration and authentication, biometrics key generation and management as well as biometrics-based data authentication. Implementations of the proposed architecture using specific realizations of suitable wireless Body Area Network (BAN) configurations will be also developed, examined and analyzed in collaboration with our industrial partners.

Selected publications and presentations:

F. Agrafioti, F.M. Bui, and D. Hatzinakos, "Medical biometrics in mobile computing", Wiley's Security and Communication Networks Journal — Special Issue on Biometric Security for Mobile Computing. Accepted February 2010.

F. Agrafioti, F.M. Bui, and D. Hatzinakos, "On supporting anonymity in a BAN biometric framework", DSP-2009, Santorini, Greece, July 5, 2009.

PARTICIPATION IN "MUSES_SECRET: MULTIMODAL-SURVEILLANCE SYSTEM FOR SECURITY-RELATED APPLICATIONS"

Researchers: Dimitrios Hatzinakos and Kostas Plataniotis (ORF Research Excellence Project)
Industry Partners: IBM Canada, Visual Cortek

The proposed MUSES-SECRET project aims at the development and commercialization of new multimodal (video and infrared, voice and sound, RFID and perimeter intrusion) intelligent sensor technologies for location and socio-cultural context-aware security risk assessment and decision support in human-crowd surveillance applications in environments such as school campuses, hospitals, shopping centers, subways or railway stations, airports, sports and artistic arenas etc. The resulting system should provide efficient multi granularity-level function-specific feedback for the human users who are the final assessors and decision makers in the specific security monitoring situation.

Selected publications and presentations:

L. Song and D. Hatzinakos, "Cognitive networking of large-scale wireless systems", Networks and Distributed Systems, vol. 2, no. 4, pp. 452-475, 2009.

H. Lu, K.N. Plataniotis, and A.N. Venetsanopoulos, "MPCA: Multilinear principal component analysis of tensor objects", IEEE Transactions on Neural Networks, vol. 19, no.1, pp. 18-39, January 2008.

"SMART" PRIVATE EYES IN PUBLIC PLACES? VIDEO SURVEILLANCE ANALYTICS, NEW PRIVACY THREATS AND PROTECTIVE ALTERNATIVES

Researchers: Andrew Clement, Kostas Plataniotis, Joseph Ferenbok (OPC)

This research proposes to examine the use of video analytics ("smart" processing) in the area of video surveillance. The research will review state-of-the-art video analytics technologies, and assess a privacy protection scheme developed by the university in laboratory. Researchers also plan to survey businesses in the Toronto area that are using video surveillance, and to assess compliance with PIPEDA for video records that should be available under the Individual Access Principle. The results will be shared in a report and public forum.

A PRIVACY PROTECTIVE "PROPORTIONATE ID DIGITAL WALLET" FOR CANADIANS: OPEN PROTOTYPING AND PUBLIC POLICY ALTERNATIVES

Researchers: Andrew Clement, Matt Ratto, Joseph Ferenbok (OPC)

This research project aims to demonstrate publicly the technical and operational viability of a mobile digital device that offers a privacy protective alternative to conventional ID schemes. Rather than routinely turn over fully identifying data, the device would reveal identity information only in proportion to what is actually needed. What we refer to as a 'proportionate ID digital wallet' would securely dispense the minimum necessary identity certificates for conducting in-person service transactions.

THE NEW TRANSPARENCY: SURVEILLANCE AND SOCIAL SORTING

Researchers: Andrew Clement (SSHRC)

The goal of the New Transparency is to create a benchmark for surveillance studies that is comparative and critical, informed by multi-disciplinary approaches and has cutting-edge policy relevance. It will move beyond the limitations of existing local- and present-oriented studies to comparative and cross-disciplinary studies, and will take into account rapid information technology changes and pivotal political-economic and cultural shifts, not least the developments since 9/11. No previous collaborative research project worldwide has undertaken the examination of surveillance in the way proposed.

Selected publications and presentations:

"IXmaps or CHmaps: Rendering visible the "interesting" features of internet backbones, especially sites of surveillance", Presentation, Ryerson University, June 18, 2009.

"Transparency and surveillance: Perspectives on identity, privacy and security", Presentation to IPSI Research Symposium, 2008.

PERFORMING IDENTITIES

Researchers: Andrew Clement, David J. Phillips, Colin J Bennett (SSHRC funding)

The Performing Identities project seeks to fill academic and practical gaps in our understanding of how people perform and experience their individual identities in their everyday encounters with identification based services and technologies. It will contribute to the articulation of 'identity rights,' as human rights distinct from other informational rights such as privacy. This will also provide the basis for the development of sound 'human-centred' identification devices, systems, policies, legislation, agencies and practices.

Selected publications and presentations:

"Toward secure and privacy sensitive ID/ authentication?", IPSI public lecture, Sept. 28, 2009.

PIPWATCH: THE COLLABORATIVE PRIVACY ENHANCING TOOLBAR (completed)

Researchers: Andrew Clement (SSHRC and BUL)

PIPWatch is a software tool designed to help Canadian Internet users quickly determine if a website they visit is compliant with Canadian legislation, in particular the Personal Information Protection and Electronic Documents Act (PIPEDA), before they submit their personal information. PIPWatch uses social navigation and web annotation techniques to allow privacy concerned Canadians to compare websites based on how well they protect personal data.

Selected publications and presentations:

A. Clement, D. Ley, T. Costantino, D. Kurtz, and M. Tissenbaum, "PIPWatch Toolbar: Using social navigation to enhance privacy protection and compliance", IEEE Technology and Society Magazine, Spring 2010, pp. 50-57, Volume: 29 Issue: 1.

SMARTDATA: MAKE THE DATA "THINK" FOR ITSELF: DATA PROTECTION IN THE 21ST CENTURY

Researchers: George Tomko, Don Borrett, Hon Kwan, Greg Steffan
Partner: Office of the Information and Privacy Commissioner

The inaugural meeting of IPSI Cognitive Agents Roundtable took place on March 13, 2009, and included 18 participants from a variety of disciplines, including physiology, cognitive science, philosophy, computer science, engineering, neuroscience, mathematics and privacy. Following this meeting, and a number of wiki discussions, a 2nd roundtable meeting was held on the 21st of May. During these meetings, it was determined that the concept of 'Smart-Data' - in which personal or proprietary information is embedded within, and protected by, an intelligent agent - is an avenue that could lead to significant research success for the IPSI team.

We have been encouraged by the significant progress that we have seen on this initiative, and are currently pursuing various funding possibilities with interested industry partners. With the leadership of IPSI's Expert-in-Residence, Dr. George Tomko, and the co-operation of IPSI staff and researchers, especially Professors Kostas Plataniotis and Dimitris Hatzinakos, we are looking forward to creating a highly successful research program, and potentially introducing the next Big Idea in privacy and online data protection.

Selected publications and presentations:

G. Tomko, D.S. Borrett, H.C. Kwan, and G. Steffan, "SmartData: Make the data "think" for itself: Data protection for the 21st century", Identity in the Information Society, Volume 3/ 2010.

HEALTH PROMOTION IN THE AGE OF SOCIAL NETWORKS: YOUTH PERSPECTIVES ON NEW MEDIA FOR HEALTH (completed)

Researcher: Cameron D. Norman (Ontario Tobacco Research Unit)

This research project investigated the use of new media in public health, through three main research questions: How are young adults using social media for health purposes? Where should public health focus its (social media) efforts for engaging young adults? What privacy and security concerns do young people have about engaging in eHealth? The project revealed that Google and Wikipedia are the primary tool and resource and that young adults use to seek integrated information and health services. The team concluded that social media should be integrated into normal public health communication and that multiple media formats should be explored for communication.

BEYOND PRIVACY: EXPLORING THE ROLE OF PSYCHOLOGICAL CONTRACT BREACH IN THE RELATIONSHIP BETWEEN KNOWLEDGE-BASED MARKETING PRACTICES AND ATTITUDES

Researchers: David Zweig and Pankaj Aggarwal, Department of Management, UTSC (SSHRC)

This research examines two related explanations underlying the processes that drive consumers' concern about use of their personal information in marketing databases: privacy invasion, and breach of psychological contract between the brand and the consumer. Results of two studies indicate that the sale of personal information results in greater perceptions of privacy invasion, psychological contract breach, and negative brand attitudes. Further, both privacy invasion and psychological contract breach partially mediate the relation between sale of personal information and brand attitudes. The results also revealed that although privacy is important, perceptions of psychological contract breach best predict negative attitudes towards brands that collect and distribute personal consumer information.

BIOMETRICS ENCRYPTION FOR FACE RECOGNITION SOLUTIONS: IMPLEMENTATION & COMPARATIVE EVALUATIONS

Researchers: Kostas Plataniotis and Dimitrios Hatzinakos (contract with Ontario Lottery and Gaming Corporation [OLG])

The objective of this work was to research, provide software implementations and comparatively evaluate Biometrics Encryption (BE) solutions that can be utilized as part of the overall OLG initiative to evaluate facial recognition for its self exclusion gaming initiative. The work was part of a study for a system that attempts to solve the problem of identifying subjects in a self-exclusion program using facial recognition, while protecting the privacy of stored personal information. In such a case, the personal information is considered to be the facial image itself, as well as application-specific meta-data related to the subject's identity.

Selected publications and presentations:

Y. Wang, D. Hatzinakos, "On random transformations for changeable face verification", Submitted to IEEE Transactions on Systems, Man and Cybernetics, Part B.

Y. Wang, D. Hatzinakos. "Cancelable face recognition using random multiplicative transform", The 20th International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, Aug. 2010.

Y. Wang, K. N. Plataniotis. "An analysis of random projection for changeable and privacy preserving biometric verification", IEEE Transactions on Systems, Man and Cybernetics, Part B (online Dec. 2009).

K. Martin, H. Lu, F. Bui, K.N. Plataniotis, and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition", IEEE Systems Journal: Special Issue on Biometrics Systems, vol. 3, no. 4, pp. 440-450, Dec. 2009.

FOOD4HEALTH PROJECT: YOUTH VOICES RESEARCH GROUP (completed)

Researchers: Cameron D. Norman, Rob McLaughlin, Alex Jadad, Dalla Lana School of Public Health (Ontario Ministry of Health Promotion)

The Food4Health project sought to test a systemic intervention strategy connecting programs together through evaluation and social media and evaluating the impact on collaboration and knowledge translation (KT). Future project work will explore the privacy and security concerns and issues of participants.

The initial project included a multi-sectoral, participatory strategy for issue identification, exploration and solution generation through face-to-face and social software platforms and it engaged youth in food systems issues using social media (e.g., Facebook, Twitter) integrating a feedback generation system that linked data through a central repository that supported rapid, coordinated KT across programs. Food4Health demonstrated that social media create knowledge exchange opportunities and vastly increase the speed of KT across programs, allowing evidence to be mobilized immediately resulting in an action research process that becomes more responsive to knowledge users.

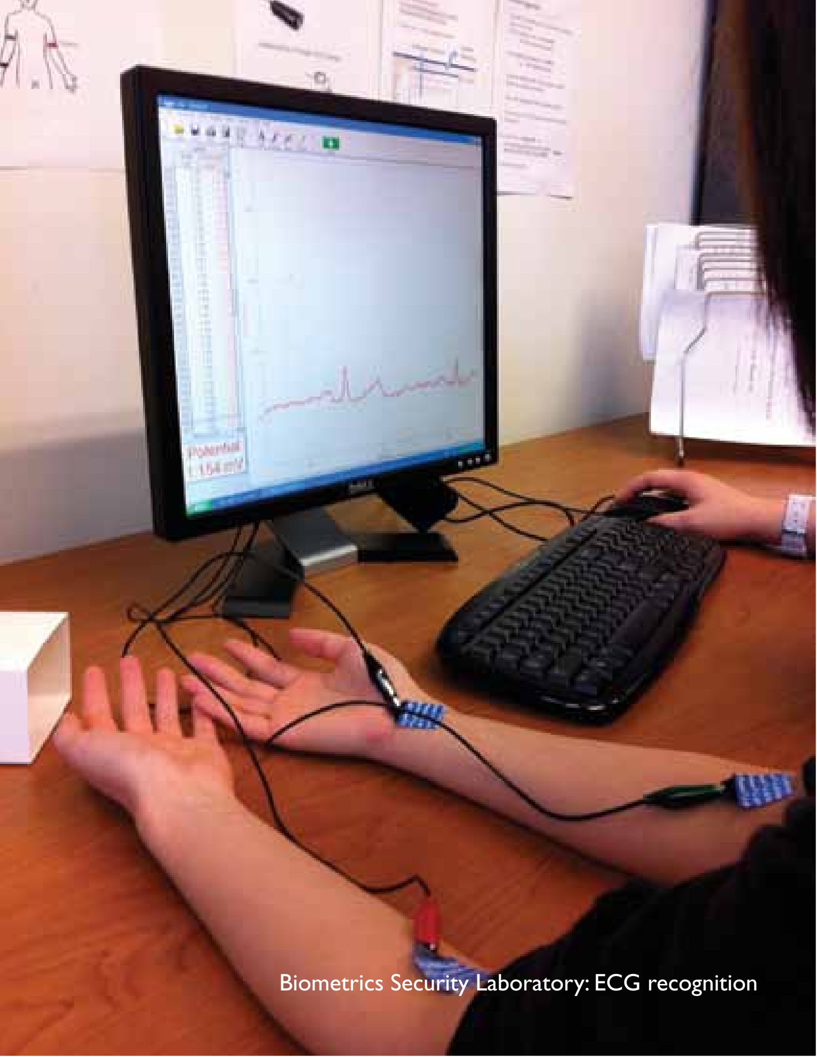
Selected publications and presentations:

C.D. Norman, J. Charnaw-Burger, A. Yip, S. Saad, and C. Lombardo (in press), "Designing health innovation networks using complexity science and systems thinking: The CoNEKTR Model", Journal of Evaluation in Clinical Practice.

C.D. Norman (in press), "Bridging online and offline social networks to promote health innovation: The CoNEKTR Model", in Biswas, R., & Martin, C. (Eds.). Utilizing Collaborative Social Networks and Technologies. IGI Books.

C.D. Norman, J. Charnaw-Burger, C. Lombardo, S. Saad, and A. Yip, "Creating capacity for collaboration in food systems and public health practice: The Food4Health Project", Poster presentation at the annual meeting of the Canadian Public Health Association, Toronto, ON. June 17, 2010.

*Video encryption technology developed by U of T researchers **Karl Martin** and **Kostas Plataniotis** was showcased at "Privacy by Design: The Gold Standard", an event hosted by the Ontario Privacy Commissioner in January 2010. This technology masks the images of individuals captured on video surveillance but allows authorized staff to unmask the images for security or safety purposes. The technology has completed the research phase and nears commercialization. One of its first customers is likely to be the Toronto Transit Commission (TTC), as Ontario Privacy Commissioner Ann Cavoukian has recommended that the TTC use this surveillance technique.*



Biometrics Security Laboratory: ECG recognition

Biometrics Security Laboratory: ECG recognition

Biometrics Security Laboratory: ECG recognition

Face recognition

Face recognition

BIOMETRICS SECURITY LABORATORY (BIOSECLAB)

This University of Toronto laboratory conducts research on biometrics systems, including signal processing methods for reliable feature extraction and robust classification. The laboratory also investigates the feasibility of biometrics for practical applications in a wide range of domains, most notably privacy and security, mobile communications and pervasive health monitoring.

Research projects are focused on several biometric modalities: face, gait and medical biometrics.

The laboratory is currently funded by IPSI and the Natural Sciences and Engineering Research Council of Canada (NSERC) and is affiliated with Bell Canada and Defence Research and Development Canada (DRDC).

RESEARCHERS

Dimitrios Hatzinakos
Konstantinos N. Plataniotis
Andrew Clement
Joseph Ferenbok
Francis Bui
Foteini Agrafioti
Liang Song
Yongjin Wang
N. Hoda Mohammadzade
Haiyan Xu
Ali Tawfiq
Zhengyao Bai

SELECTED PUBLICATIONS AND PRESENTATIONS

Y. Wang, D. Hatzinakos, "Cancelable face recognition using random multiplicative transform", The 20th International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, Aug. 2010.

K. Martin, H. Lu, F. Bui, K.N. Plataniotis, and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition", IEEE Systems Journal: Special Issue on Biometrics Systems, 3:4, pp. 440-450, 2009.

Y. Wang, K. N. Plataniotis, "An analysis of random projection for changeable and privacy preserving biometric verification", IEEE Transactions on Systems, Man and Cybernetics, Part B (online Dec. 2009).

F. Bui, F. Agrafioti, and D. Hatzinakos, "Electrocardiogram (ECG) biometric for robust identification and secure communication", Biometrics: Theory, Methods and Applications, Eds: N. Boulgouris, E. Micheli-Tzanakou, and K. Plataniotis. Wiley/IEEE, 2009.

F. Agrafioti and D. Hatzinakos, "ECG biometric analysis in cardiac irregularity conditions", Signal, Image and Video Processing, Springer, pp 1863-1703, September 2008.

F.M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling", EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, Volume 2008, Article ID 529879, pp. 1-16, 2008.

For more information on BIOSECLAB, please visit http://www.comm.utoronto.ca/~biometrics

RESEARCH ASSOCIATES - ACADEMIC

J. Stewart Aitchison, B.Sc., Ph.D.
Vice Dean (Research)
Faculty of Applied Science and Engineering, University of Toronto

Lisa Austin, B.A., LL.B., Ph.D.
Associate Professor, Centre for Innovation Law and Policy
Faculty of Law, University of Toronto

Ron M. Baecker, B.S., M.S., Ph.D.
Professor, Department of Computer Science, Faculty of Arts and Science
Director, Knowledge Media Design Institute, University of Toronto

Nadia Caidi, M.ST., M.LIS., Ph.D.
Associate Professor, Faculty of Information, University of Toronto

Ron Deibert, B.A., M.A., Ph.D.
Associate Professor, Department of Political Science, Faculty of Arts and Science
Director, Citizen Lab, Munk Centre for International Studies, University of Toronto

Lorraine E. Ferris, Ph.D., C.Psych., LL.M.
Professor, Social and Behavioural Sciences, Dalla Lana School of Public Health
Associate Vice Provost, Relations with Health Care Institutions, University of Toronto

Ashish Khisti, B.A.Sc., M.S., Ph.D.
Assistant Professor, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

David Lie, B.A.Sc., M.S., Ph.D.
Associate Professor, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

Hoi-Kwong Lo, B.A., M.S., Ph.D.
Associate Professor, Department of Physics, Faculty of Arts and Science
Associate Professor, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

Maria Athina Martimianakis, M.A., M.Ed., Ph.D.
Lecturer, Department of Paediatrics
Fellow, Department of Psychiatry and Wilson Centre for Research in Education, University of Toronto

Karl Martin, B.A.Sc., M.A.Sc., Ph.D.
Researcher, Multimedia Lab, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

Cameron Norman, B.A., M.A., Ph.D.
Assistant Professor, Social and Behavioral Sciences, Dalla Lana School of Public Health
Director of Evaluation, Peter A. Silverman Global eHealth Program, University of Toronto

Peter Pennefather, B.A.Sc., Ph.D.
Associate Professor, Leslie Dan Faculty of Pharmacy
Academic Director of the Laboratory for Collaborative Diagnostics, University of Toronto

David Phillips, M.A., M.S.E., Ph.D.
Associate Professor, Faculty of Information, University of Toronto

Matt Ratto, B.A., M.A., Ph.D.
Assistant Professor, Faculty of Information
Director, Critical Making Lab, University of Toronto

Greg Steffan, B.A.Sc., M.A.Sc., Ph.D.
Associate Professor, Department of Electrical and Computer Engineering, Faculty of Applied Science and Engineering, University of Toronto

Eric Yu, B.A.Sc., M.A., Ph.D.
Associate Professor, Faculty of Information, University of Toronto

RESEARCH ASSOCIATES – INDUSTRY & GOVERNMENT

Mike Gurski
Director, Bell Privacy Centre of Excellence
National Privacy Strategist, Bell Canada

Guy Herriges
Manager, Access, Discovery and Business Recordkeeping
Office of the Chief Information and Privacy Officer, Ministry of Government Services, Government of Ontario

Catherine Johnston
President and CEO, ACT Canada

Reza Kopaee
Associate Partner, Deloitte Canada

Yves Lostanlen, M.Sc., Ph.D.
Vice-President and Wireless CTO, Director, Radio Business Unit, SIRADEL, France
Adjunct Professor, University of Toronto

Prabir Neogi
Special Advisor, Electronic Commerce Branch, Department of Industry, Government of Canada

Ruth Vale
Senior Analyst, Privacy
eHealth Ontario/Smart Systems for Health Agency

IPSI

CONTACT INFORMATION

40 St. George Street Room 4145
Toronto, Ontario M5S 2E4
Tel: 416 946-3398
Fax: 416 978-4425
Email: ipsi@utoronto.ca
www.ipsi.utoronto.ca

UNIVERSITY OF
TORONTO