IPSI Public Lecture Series 2009

September 28	**Andrew Clement, Professor, University of Toronto** *"Toward Secure, Privacy Sensitive ID/Authentication"* The conventional approach to authenticating an individual for the purposes of authorizing a particular transaction is to require an ID card or similar form of unique personal identifier that links the individual to an organizationally maintained database. In both face to face and on-line settings, this is highly problematic from a privacy point of view - often revealing much more personal information than the minimum required. An alternative approach that is gaining attention in on-line transactions is that of digital credentialing - of securely and reliably establishing that the person is entitled to conduct the transaction without requiring full identification (e.g. Credentica/Microsoft's U-Prove technique). This lecture will introduce this alternative, more user-centric approach to ID/authentication, by showing how credentialing can work in face to face settings while protecting privacy interests. In so doing, it will provide an introduction to the central theme of this fall's lecture series, ID/authentication, as well as the speakers to follow who will address various aspects of this topic. View Presentation (PDF)	Bissell Bldg., 140 St. George Room 728
October 5	**Kostas Plataniotis, Professor, University of Toronto** *"Introduction to Biometrics for ID and Authentication"* Biometric identification, authentication, verification of claimed identity, and prevention of un-authorized access to physical assets and confidential, sensitive information are critical elements of an effective security architecture in several civilian and commercial applications. Biometrics, a measurable physical characteristic or personal behaviour trait that can be used to identify and verify a claimed identity appears to be the obvious choice for large scale authentication, user identification and platform/application attestation. The objective of this presentation is to review the state-of-the-art in biometrics-based research with particular emphasis on solutions for authentication. The presentation will highlight open research questions and present recent technical advances.	Bissell Bldg., 140 St. George Room 728

October 26	**Roger Clarke, Xamax / Visiting Professor The Australian National University / Australian Privacy Foundation (Chair) / Australian Computer Society** *"A Sufficiently Rich Model of (Id)entity, Authentication and Authorization"* Conventional approaches to authentication revolve around identities and identity management. This presentation introduces a model and a coherent set of terms. These enable organisations to judge what infrastructure and business processes are appropriate to support particular eBusiness and eGovernment systems. Application of the model demonstrates that the precepts on which the current 'identity management' industry is based are deeply flawed. The model is applicable to many different categories of entities, including goods, motor vehicles, computing devices, human beings, and artefacts as proxies for human beings. The importance of the distinction between an entity and an identity is drawn out by considering mobile phones.	Bissell Bldg., 140 St. George Room 728
November 2	**David Lyon, Professor, Queen's Research Chair, Queens University, Sociology** *"Identifying Citizens: ID Cards as Surveillance"* New IDs, proliferating around the world, portend a new social and political condition. Not merely a response to post 9/11 anxieties about national security, new IDs are a novel means of governance in a world where surveillance is the dominant organizational mode. Showing a token of legitimate ID is now a basic condition for the exercise of freedom. Now that IDs depend on large-scale databases, biometrics and sometimes RFID, what does the "new social and political condition" mean for surveillance, security and citizenship?	Bissell Bldg., 140 St. George Room 728
November 16	**Carlisle Adams, Professor, University of Ottawa** *"Credential Systems: Promise, Risks and Possible Mitigations"* Concerns about the degradation of privacy in our increasingly digital world has led a number of researchers to explore the creation of Privacy Enhancing Technologies (PETs). One such PET is the	Bissell Bldg., 140 St. George Room 728

	concept of a credential system, which allows the construction of privacy-preserving access control infrastructures in online environments. Credential systems hold much promise for those interested in retaining some control over their personal information but, as with any technology, there can be risks associated with widespread deployment. This talk will give a brief introduction to credential systems and some of the associated risks, and discuss recent research into possible mitigation techniques for these risks.	
November 23	**Lorrie Cranor, Program Director Carnegie Mellon University, CyLab / Engineering and Public Policy / Institute for Software Research / School of Computer Science** *"Usable Privacy and Security"* Many secure systems rely on a "human in the loop" to perform security-critical functions. However, humans often fail in their security roles. Whenever possible, secure system designers should find ways of keeping humans out of the loop. However, there are some tasks for which feasible or cost effective alternatives to humans are not available. In these cases secure system designers should engineer their systems to support the humans in the loop and maximize their chances of performing their security critical functions successfully. I will introduce some high- level approaches to usable security and discuss a proposed framework for reasoning about the human in the loop that provides a systematic approach to identifying potential causes for human failure. This framework can be used by system designers to identify problem areas before a system is built and proactively address deficiencies. System operators can also use this framework to analyze the root cause of security failures that have been attributed to "human error."	Bissell Bldg., 140 St. George Room 728
November 30	**Dmitry O. Gorodnichy , Senior Research Scientist Group Leader, Video Surveillance and Biometrics Technologies / Applied Research and Development Division / Laboratory and Scientific Services Directorate / Canada Border Services Agency** *"Recognition in Video"* Video has become the main information media of our age. Thousands of video cameras are installed in public places. Thousands of hours of video data are being	Bissell Bldg., 140 St. George Room 728

	recorded, transmitted and archived daily. As a result, automated recognition of individuals in video has become one of the most frequently contemplated uses of biometrics. It is however also one of the most challenging. This talk presents an overview of the problems and solutions related to video-based recognition. Among the questions considered are: • What makes video-based biometrics so different from conventional image-based biometrics such as fingerprint, iris and passport faces? • Why is conventional error-tradeoff-based evaluation not sufficient for evaluation of face recognition in video? • Why is the human brain so efficient in performing video recognition tasks, while computers are not? • What is the state of the art, and what is the future of recognition in video - for academia and for industry?	
December 7	**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"* U.S. novelist Jonathan Franzen once characterized privacy as the "Cheshire cat of values." One wonders whether current legal and ethical norms aimed at protecting privacy and anonymity will suffer the same fate as Lewis Carroll's enigmatic feline—all smile and no cat. While privacy law's "consent" requirements are easily understood and applied in coercive or surreptitious surveillance systems, their application is murkier in the context of social networks, ubiquitous computing and other forms of lateral surveillance where participants seem to eagerly and voluntarily disclose private information without regard to the consequences. In this lecture, Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology, considers the future (regulation) of privacy and anonymity through an exploration of the aims and effects of ubiquitous computing and the broader social shift from traditional to "softer" forms of surveillance.	Bissell Bldg., 140 St. George Room 728