

Office of the  
Privacy Commissioner  
of Canada



Commissariat à la  
protection de la vie privée  
du Canada

**Summary of Research Projects  
Funded under the Contributions Program 2004  
to 2007**

**September 2007**

# Table of Contents

Introduction.....	1
<b>Consumer Privacy and Marketplace Compliance</b>	
<b>Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?</b> <i>Canadian Internet Policy and Public Interest Clinic (two separate reports), April 2006.....</i>	2
<b>On the Data Trail: How Detailed Information About You Gets Into the Hands Of Organizations With Whom You Have No Relationship. A Report on the Canadian Data Brokerage Industry</b> <i>Canadian Internet Policy and Public Interest Clinic (two separate reports), April 2006.....</i>	3
<b>Do Consumers Benefit From the Trading of Personal Information?</b> <i>L'Union des consommateurs, April 2007.....</i>	4
<b>Implementing PIPEDA: A Review of Internet Privacy Statements and Online Practices</b> <i>University of Toronto, May 2005.....</i>	5
<b>Privacy Models that Work: A Guide for Canadian Organizations</b> <b>Best Practices in Data Management: A Guide for Marketers</b> <b>Small Business Privacy Compliance – Research Findings</b> <i>Canadian Marketing Association (three separate reports), June 2005.....</i>	6
<b>Securing Compliance, Protecting Privacy: The PIPEDA Enforcement Evaluation Research Project</b> <i>British Columbia Civil Liberties Association, March 2006.....</i>	7
<b>Guidance for Privacy Professionals and Business Organizations</b>	
<b>Professional Certifications Standards Project</b> <i>Canadian Association for Professional Access and Privacy Administrators and Canadian Access and Privacy Association, March 2007.....</i>	8
<b>Strategies for Drafting Privacy Policies Kids Can Understand</b> <i>University of Western Ontario, March 2007.....</i>	9
<b>Health Information</b>	
<b>Pan-Canadian De-Identification Guidelines for Personal Health Information</b> <i>Children's Hospital of Eastern Ontario Research Institute, April 2007.....</i>	10
<b>Electronic Health Records and the <i>Personal Information Protection and Electronic Documents Act</i></b> <i>University of Alberta and University of Victoria, April 2005.....</i>	11
<b>Secondary Uses of Personal Information Held on National Electronic Health Record Systems: Key Developments, Issues and Concerns</b> <i>Centre for Bioethics, Clinical Research Institute of Montreal, June 2007.....</i>	12
<b>Social Uses of DNA in the Policy Making Process: Analysis of Two DNA Identification Bills</b> <i>University of Ottawa, April 2006.....</i>	13

<b>Technology Choices and Privacy Policy in Health Care</b> <i>Memorial University of Newfoundland, April 2007</i> .....	<b>14</b>
<b>Privacy and Technology</b>	
<b>An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies</b> <i>Dalhousie University, April 2005</i> .....	<b>15</b>
<b>The Challenge of Consumer Identification with New Methods of Electronic Payment</b> <i>Option Consommateurs, August 2006</i> .....	<b>16</b>
<b>Digital Rights Management Technologies and Consumer Privacy: A Canadian Market Survey and Privacy Impact Assessment</b> <i>Canadian Internet Policy and Public Interest Clinic, April 2007</i> .....	<b>17</b>
<b>Privacy Rights and Prepaid Communications Services: A survey of prepaid mobile phone regulation and registration policies among OECD member states</b> <i>Simon Fraser University, March 2006</i> .....	<b>18</b>
<b>Vehicle Technology and Consumer Privacy</b> <i>Automobile Consumer Coalition, March 2007</i> .....	<b>19</b>
<b>Surveillance</b>	
<b>Location-Based Service and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada</b> <i>University of Victoria, June 2005</i> .....	<b>20</b>
<b>Location Technologies: Mobility, Surveillance and Privacy</b> <i>Queen's University, March 2005</i> .....	<b>21</b>
<b>The Use of Video Surveillance Cameras in Public Places in Canada</b> <i>Ecole nationale d'administration publique, December 2005</i> .....	<b>22</b>
<b>Workplace Privacy</b>	
<b>A Preliminary Exploration of Workplace Privacy Issues in Canada</b> <i>University of British Columbia, April 2006</i> .....	<b>23</b>
<b>Under the Radar? The Employer Perspective on Workplace Privacy</b> <i>Ryerson University, June 2006</i> .....	<b>24</b>
<b>Other</b>	
<b>PIPEDA and Identity Theft: Solutions for Protecting Canadians</b> <i>B.C. Freedom of Information and Privacy Association, April 2005</i> .....	<b>25</b>
<b>Privacy within the Criminal Justice System: Investigation DNA</b> <i>University of Ottawa, April 2007</i> .....	<b>26</b>
<b>Can ID? Visions for Canada: Identity Policy Projections and Policy Alternatives</b> <i>University of Toronto, April 2007</i> .....	<b>27</b>

## Introduction

The Office of the Privacy Commissioner of Canada is proud to present abstracts of the 25 privacy-related research studies we have funded through our Contributions Program since 2004.

Part of our mandate is to promote understanding and awareness of privacy issues among Canadians. The Contributions Program funds and publishes valuable research by Canadian academics, privacy advocates and the business community – much of it cutting edge, world-class and of global relevance.

The need for such research has never been more pressing. Moreover, there is no shortage of privacy issues to study. Indeed, many privacy experts believe that political, economic and technological trends are placing relentless pressures on our privacy and other rights and freedoms.

During the first three years, researchers funded by the Contributions Program examined implementation of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. They studied medical privacy issues, including genetics and automated health care records. They looked at an array of other new technologies and how they can "creep" into our private lives. And they researched workplace privacy issues from the perspectives of both employees and employers.

In 2007, my Office is focusing Contributions Program research on privacy over the Internet, especially among young people, who seem too willing too often to take risks with their safety and reputations for the sake of convenience. We are paying attention as well to the challenges inherent in securing identification and authentication where, increasingly, we have to give up our once assumed anonymity to simply move about or communicate. A third stream of research will evaluate the intersection of the public and private sectors regarding the collection and use of personal information, such as the increasing availability of our consumer records to government authorities.

We encourage advocates, academics, policy makers and business leaders to both use and build on this existing body of research, to undertake new research and to help develop and share best privacy practices. Privacy is a core value of our society and indeed a fundamental human right. We need to protect it for the sake of all global citizens and future generations.

Jennifer Stoddart  
Privacy Commissioner of Canada  
September 2007

## Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?

*Canadian Internet Policy and Public Interest Clinic, April 2006, 110 pages*

This study was designed to examine to what extent organizations are respecting the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, by assessing the compliance of retailers with certain key provisions of *PIPEDA*.

Sixty-four online retailers were identified in an unbiased selection process and assessed for compliance with *PIPEDA* requirements for openness, accountability and consent. The assessment involved calling the company's main telephone number and asking a few standard questions, reviewing the company's privacy policy and ordering a product or service online. A second group of 72 online and offline retailers were assessed against the *PIPEDA* requirement for individual access. This assessment involved sending a standard letter to companies and reviewing responses.

The results of the study's compliance assessment indicate widespread non-compliance in all four areas, and recommends that alternatives to *PIPEDA*'s current enforcement need to be considered. While almost all companies assessed had a privacy policy and were thus aware of the need to respect customer privacy, many failed to fulfill even basic statutory requirements such as providing contact information for their privacy officers, clearly stating what they do with consumer information and responding to access to information requests. The results strongly suggest that Canadian data protection legislation provides inadequate incentive for companies to give consumers meaningful control over their personal information, and to be open about their data management practices.

Report available at: <http://www.cippic.ca/en/bulletin/>.

## **On the Data Trail: How Detailed Information About You Gets Into the Hands of Organizations With Whom You Have No Relationship. A Report on the Canadian Data Brokerage Industry**

*Canadian Internet Policy and Public Interest Clinic April 2006, 64 pages*

The report describes how detailed personal information about Canadians ends up in the hands of direct marketers and others. Specifically, it examines the data brokerage industry whose activities have significant implications for individual privacy. It is descriptive, relating how Canadian data brokers purport to comply with Canadian privacy laws. However, it does not actually assess data broker compliance with Canadian privacy laws.

Research was conducted using a variety of methods, including literature and website reviews, expert consultations, access to information requests and selective follow-ups with managers and data compilers. Researchers reviewed industry guidelines and privacy policies to better understand how companies trading in personal information approach compliance with privacy laws.

There is a large and vibrant trade in the personal information of Canadian consumers. The driver of this trade is the direct marketing industry. Facilitating this trade is an array of companies that specialize in, among other things, list management and brokerage, geo-demographic population profiling, database analytics, individual consumer profiling, survey-based data-gathering, and multi-source data mining.

While much of the data takes the form of customized lists and group profiling, there is abundant evidence of individual consumer profiling. The increasing accumulation of personal data and consolidation of databases leaves individuals vulnerable to abuses by those with access to the data. It is hoped that this report will provide researchers, consumer advocates, policy makers, and others with useful information on which to design effective laws and policies for protecting personal information in the marketplace.

Report available at: <http://www.cippic.ca/en/bulletin/>

## Do Consumers Benefit From the Trading of Personal Information?

*L'Union des consommateurs, April 2007, 73 pages*

Marie-Eve Rancourt

The heart of this research project is a discussion of whether the trade in personal information by companies is beneficial to consumers.

In addressing this question, the author considered the benefits of the following data practices, arriving at these conclusions:

Profiling: although some consumers may appreciate the personalizing of services and advertising that results from the ability of marketers to create an individually tailored consumer profile, there is nothing to guarantee the accuracy of profiling information that may be used in ways harmful to the person's interests (for example the granting of credit or hiring decisions). Moreover, profiling creates different categories of consumers ("good consumers" and "bad consumers") which opens the door to discriminatory practices – noting that France's Supreme Court had ruled that such consumer characterization was illegal in that jurisdiction. Profiling can also lead to increasingly invasive target marketing which could change the nature of Internet interactions and encourage individuals to over-consume.

Cookies: cookies files facilitate the use of the Internet in helpful ways, but are often installed without consent and collect information about the users without their knowledge or consent. In particular, "persistent cookies" (those that remain on a user hard drive after an Internet session ends) result in a consumer's total loss of control over personal information – with the attendant risks of profiling and identity theft.

Spyware: where commercial companies include spyware in their software, which automatically downloads when the user accepts the licensing agreement, such software collects personal information, most often without explicit consent, consumes RAM and hard drive space, and mobilizes processor resources that could negatively impact on other computer applications. In addition, only the industry benefits from collecting information by spyware, usually in circumstances where it fears that the consumer would refuse to disclose the information if given a choice.

Spam: defended in some quarters as an environmentally friendly and economical form of advertising that is easy to delete or ignore, and that lets small companies compete with larger ones, the author sees no consumer benefit in this form of advertising due to its high annoyance factor and the fact that spam rarely offers products that consumers might find interesting.

Loyalty cards: the report enumerates the privacy concerns such as the impressive quantity of information that can be collected by businesses, the lack of transparency surrounding its collection, and the impossibility of consumers enjoying the advantages of a loyalty card without accepting this information collection.

Period of retention and safeguards: current practices are prejudicial to consumers due to the privacy risks created by prolonged data retention and poor safeguards.

Cross-border data flows: unlike European laws, Canadian laws do not prohibit transborder transmission or subject it to conditions of equivalent protection. The report suggests that exporting the personal data of Canadians allows companies to circumvent Canadian standards and benefit from legislation that is less binding.

This study incorporates new field research, based on a survey and analysis of online privacy policies of 10 companies, particularly with regard to whether companies seek explicit consent to collect and use personal information. The survey conducted between April 10 and April 20, 2007, with a results grid and a discussion of findings highlights.

Report available at: [http://www.consommateur.qc.ca/union/docu/vieprivee/info\\_perso\\_e.pdf](http://www.consommateur.qc.ca/union/docu/vieprivee/info_perso_e.pdf)

## Implementing *PIPEDA*: A Review of Internet Privacy Statements and Online practices

University of Toronto, May 2005, 43 pages.

Rajen Akalu, Barbara Bressolles, Sapna Mahboobani, Aniz Alani, Andrew Clement

These four studies evaluate how well various Canadian telecommunications, airline, banking and retail companies are complying with *PIPEDA*'s openness principle and, in the case of airlines and banks, with the European Commission's Data Protection Working Party Opinion on information notices. The authors reviewed the companies' online privacy policies against these criteria, combining their research with surveys, interviews and online interaction with chief privacy officers and other experts.

The telecommunications study is a summary of a Canadian Federal Court of Appeal case, *Englander v Telus Communications Inc.* Mr. Englander contended that Telus had contravened the knowledge and consent requirements of *PIPEDA* (which should mirror the openness principle); and that charging a fee to obtain an unpublished phone number contravened the spirit if not the letter of the Act. The Court agreed concerning the former, but not the latter. Service fees of telecommunications companies are regulated by another federal agency.

The second paper examines the online privacy statements of four Canadian airlines, Air Canada, WestJet, CanJet and Jetsgo, to determine their compliance with *PIPEDA* and the Working Party Opinion. The latter provides insight into European Commission policy processes seeking to ensure adequate protection of personal information on passengers and crew arriving from Europe. This information is used by the Canada Border Services Agency to identify potential terrorist threats. The Agency's privacy commitments to the Working Party were welcomed and sufficient to conclude that protection was adequate. However, the study notes a lack of uniformity in the airlines' online privacy statements which it suggests the Office of the Privacy Commissioner deal with by audit or education.

The third paper explains more fully the Working Party Opinion on harmonizing privacy notices and evaluates the extent to which two leading Canadian banks (CIBC and Scotiabank) meet identified standards. The author agrees that harmonization is likely to result in greater ease of comparison among statements, including identifying omissions. A three-tier notice system is recommended, the first providing 'core' information and the second and third more relevant information that is required by the Commission and national law. Taken together, these constitute a legal notice. In this light, it is believed both CIBC and Scotiabank privacy statements are deficient, although Scotiabank's notice was found to be more user-friendly through the use of links.

The final paper examines privacy statements within the retail business sector which falls under provincial jurisdiction. It concludes that while this sector is generally following the lead of federal undertakings such as banks and airlines (which were subject to privacy legislation three years in advance of retail businesses), this may not be a good thing. Publication of more detailed information would provide consumers with a proper basis on which to assess companies' privacy practices and hold them to account.

Overall, the authors find *ad hoc* compliance, concluding that companies appear motivated to communicate their privacy policies due to business prudence rather than concerns for privacy. There is room for improvement.

Report available at:

[http://PIPEDAproject.atrc.utoronto.ca/index.php?option=com\\_content&task=view&id=1&Itemid=1](http://PIPEDAproject.atrc.utoronto.ca/index.php?option=com_content&task=view&id=1&Itemid=1)

## **Privacy Models that Work: A Guide for Canadian Organizations Best Practices in Data Management: A Guide for Marketers Small Business Privacy Compliance – Research Findings**

*Canadian Marketing Association (three separate reports) June 2005*

The Canadian Marketing Association produced two guides and conducted a survey in 2005, all dealing with privacy legislation and compliance issues.

**Privacy Models That Work - A Guide for Canadian Organizations** (13 pages) examines privacy management models in Canadian organizations. It starts from the premise that the privacy management function is comparatively young, and that there is no widely accepted or single 'right way' to position, organize and manage the corporate privacy function. Based on interviews with more than a dozen leading Canadian organizations, the report distills the approaches used by these companies into three main models and an alternative model for smaller organizations – models that the report states “work for Canadian organizations.”

Each of the models is briefly described, with first-hand statements by privacy officers on the strengths of their model. The pros and cons of various privacy structures, key roles and responsibilities of privacy officers, privacy compliance management processes and audit processes are all briefly described, with a short bulleted section in each case on “what works.” The report concludes with a short section on incorporating privacy into overall business strategy.

**Best Practices in Data Management – A Guide for Marketers** (12 pages) is a customer-focused set of guidelines addressing four main areas of interest for marketers – collecting information, obtaining consent, safeguarding information and sharing it with partners.

In each of these areas of interest, the document offers specific, detailed and practical advice, based on the CSA Privacy Principles that will help marketers to apply best practices.

The section on consent, for example, explains the different forms of consent and covers nine specific points that marketers should be aware of when obtaining consent. There is similar valuable guidance in each of the other sections. The report concludes with a one-page summary of best practices.

**Small Business Privacy Compliance – Research Findings** (23 pages) is based on an online survey completed by 157 companies (275 companies undertook the survey, but 118 did not complete it, primarily due to the fact that privacy legislation did not apply to their business activities).

The survey posed questions concerning the handling of personal information within businesses, business attitudes towards privacy legislation, the steps taken by businesses to ensure privacy compliance, the ranking of various privacy risk considerations (for example damage to business reputation), what safeguards are in place, what barriers exist to full compliance with privacy legislation, and what additional resources are needed.

Lack of information was considered the leading barrier to privacy compliance (51%), with time taken to implement new laws and/or update processes the second top barrier (43%).

In the need for additional resources, the top three responses were, in order of importance, a need to understand the privacy laws from an industry perspective; a need for more simplified and more accessible information; and a need for better maps to find online information.

The report concluded with recommendations that the Office of the Privacy Commissioner help small businesses achieve privacy compliance (including the need to reach more businesses), start with the basics, recognize industry similarities and differences, provide a dedicated website for privacy compliance, and help businesses build a privacy policy.

Reports available at: <http://www.the-cma.org/?WCE=C=47|K=224334>

## Securing Compliance, Protecting Privacy: The *PIPEDA* Enforcement Evaluation Research Project

British Columbia Civil Liberties Association, March 2006, 91 pages

Principal Researcher, Kirk Tousaw, Barrister & Solicitor

This study examines the enforcement mechanisms in *PIPEDA* vs. alternative models in the provinces of Quebec, Alberta and British Columbia, as well as Australia and New Zealand, and two non-privacy models in Canada regulating human rights and telecommunications.

The research combines literature reviews and interviews with privacy officials, advocates and officers of regulated parties, to analyze the practical effects of different choices in enforcement models. The research highlights which powers have been granted and used, to identify policy and legal mechanisms best enhancing compliance.

The study finds that there is more dissatisfaction than satisfaction with the ombudsman role played by the Office of the Privacy Commissioner under *PIPEDA*, and that the law needs changing to make enforcement more effective. The OPC has strong investigative powers (and audit and education roles) but cannot issue orders and award damages. The only recourse is through the Federal Court, which is viewed as a considerable barrier to access justice. The author states that the ombuds-model may have been appropriate to achieve consensus among regulated parties when *PIPEDA* was first enacted. He recognizes OPC's serious commitment to enhancing enforcement under the existing model. However, the study concludes that, after five years, the OPC requires more tools to move the regulated parties toward more substantial compliance.

Recommendations include several reforms the OPC could implement without amending the law or the ombuds-model. These include:

- 1) improved investigation standards, such as using agreed statements of facts, ensuring each party has a full opportunity to respond and that reports sent to each are substantially identical;
- 2) additional funding to provide legal assistance, make site visits to review privacy policies and make more information available online and in printed form; and
- 3) permanent audit and review processes to measure compliance, with the results being published in the Commissioner's *Annual Report*, including identifying non-compliant businesses.

The study also recommends amendments to *PIPEDA*, concluding that stronger enforcement tools available and used in other privacy jurisdictions will enhance compliance even further while still retaining the dispute resolution focus of the ombuds-model. These new tools include empowering the Commissioner to issue orders that are able to be filed with the Federal Court and made immediately enforceable; allowing the Commissioner to award compensation to complainants and, in egregious cases, to award punitive damages against respondents; allowing representative complaints to the OPC (filed by a third party on behalf of an individual), and allowing complainants to file class action suits in the Federal Court.

Report available at: <http://www.bccla.org/othercontent/FINAL%20REPORT.APRIL06.pdf>

## **Professional Certifications Standards Project**

*Canadian Association for Professional Access and Privacy Administrators and Canadian Access and Privacy Association, March 2007, 65 pages*

This report is the end result of the first phase of an ongoing initiative by the Canadian Access and Privacy Association (CAPA) and the Canadian Association for Professional Access and Privacy Administrators (CAPAPA) to establish standards for information and privacy professionals in Canada.

A working group for this project, chaired by Frank Work, Alberta's Information and Privacy Commissioner, consisted of senior representatives of CAPA, CAPAPA and the Quebec L'Association sur l'accès et la protection de l'information (AAPI), senior officials of the Office of the Information Commissioner of Canada and the Privacy Commissioner of Canada, as well as academics, consultants and industry representatives involved in this field.

The objective of this report was to identify and establish professional standards for information and privacy professionals (IPPs). The standards will constitute a minimum-level-for-practice criteria used to evaluate competence to practice as an IPP seeking certification.

The report advances a strong requirement for professional standards and, in subsequent phases of this work, creation of a certification and oversight body. It stresses that IP professionals can be seen, in some settings, as quasi-judicial officials upholding legal rights of a quasi-constitutional nature. It describes such professionals as "stewards of a public trust that underpins our democratic and economic freedom". It argues that the work of such professionals "requires special qualifications and a high-level of professional comportment".

Described in the report are the three inter-related aspects of IPP work: the Administrator Aspects; the Executor Aspect; and the Advisor Aspects, all of which require a different focus. The report states that the ordering of these aspects is an important consideration in designing and classifying job descriptions, in organizing IPP work groups, and in engineering career structures.

The competencies required in all three aspects are outlined in an IPP Competency Profile which presents the level of proficiency needed to achieve entry into the profession through formal certification. A total of 24 specific competencies are identified under the three aspects, including interpreting legislation, building relationships and trust, developing technological awareness, and providing training and education. The report adds that the structure of the competencies contemplates possible later refinements and customized enhancements to identify more expert levels within each competency. Appendix C of the report contains a list of "attainment indicators" for each of the 24 competencies, making this an extremely useful matrix for any evaluation of IPP qualifications.

The report also contains a proposed six-point Code of Ethics for IPPs, intended to identify their professional obligations, and identify for clients, stakeholders and members of the public the expectations and accountabilities placed on certified IPPs.

The report concludes with criteria for certification that could be applied by a professional certifying body, a listing of target audiences for certification, and an outline of work yet to be completed. The next stages of work include a recommended certification model (delivery in August 2007) and a recommended governance model, to be completed by the end of November 2007.

Report available at: <http://www.capa.ca/Main%20certification.html>

## **Strategies for Drafting Privacy Policies Kids Can Understand**

*University of Western Ontario, March 2007, 119 pages*

Jacquelyn Burkell, Valerie Steeves and Anca Micheti

The goal of this research was to identify guidelines for the drafting of privacy policies that children and teens can interpret accurately and with relative ease. Achieving this goal required a three-pronged strategy. Firstly, the authors analyzed relevant literature on readability and document comprehension within the target age groups. Secondly, focus groups were conducted with children and teens to examine their experiences and practices of looking at and interpreting privacy policies on favourite kids' sites. Based on this, a set of potential guidelines for privacy policies was identified, which was empirically tested in the third phase of the research. The end result is a set of guidelines for the drafting of privacy policies that the authors claim "make a difference, by actively improving the comprehensibility of privacy policies encountered by Canadian children and teens as they surf the net".

Previous research by these and other authors indicates that privacy policies are "hard to find, long and often written at a reading level that is not accessible to most adults". Prior research by the authors found that 49 of the top 50 kids' sites do contain privacy policies. Those policies, however, are typically difficult to find. Furthermore, they tend to be long (1902 words on average), with average reading level scores of grade 11 to grade 12. (Grade 8 is the recommended level for documents directed at adults, according to the Flesch grade level test.)

Although readability formulae are typically used to assess the comprehensibility of privacy policies, the authors warn that writing policies to readability formulae does not, in itself, guarantee comprehension. The bulk of the report focuses on a set of proposed guidelines that address the language of privacy policies, the structure of the text and the overall design of policies. There are 14 specific guidelines under these three categories: for example, one guideline suggests that double negative construction should be avoided. These guidelines are identified based both on reader feedback and on previous research on the factors that influence reading comprehension. The extended description for each guideline cites relevant research findings, identified comments from young people that are relevant to the guideline, and provides practical examples of positive and negative instances of the guideline. To test the effectiveness of the guidelines, the authors compared original and revised versions of actual online policies (with disguised names). Thirty-five participants aged 11 to 17 participated in the testing. Comprehension was improved with the revised policies, and participants were more able to accurately report the information collected by the site. In addition, participants overwhelmingly preferred the rewritten versions. The report includes a useful table summarizing the guidelines.

The authors also found that kids care about privacy. In the focus groups conducted by the authors, it became clear that, while privacy is not a primary goal of online activity (in this respect, the authors consider children to be no different than adults), it was clear that children and teens feel uncomfortable with the pervasiveness of online surveillance, but feel disempowered to do anything about it. As one girl put it, there are doors on the Internet, but "the doors are broken".

The authors also found that a general distrust of organizations that collect personal information on the Internet permeates the expectations of the privacy policies that children and teens encounter online. They expect these policies to make it more difficult to discover what happens to their information and they attribute bad will to the drafters. As one 17 year old boy said, they "take advantage of the kids ... cause they can't read at university level".

Report available at: <http://idtrail.org/content/view/684/42/>

## **Pan-Canadian De-Identification Guidelines for Personal Health Information**

*Children's Hospital of Eastern Ontario Research Institute, April 2007, 83 pages*

Khaled El Emam, Elizabeth Jonker, Scott Sams, Emilio Neri, Angelica Neisa, Tianshan Gao and Sadrul Chowdhury

This study examines the risks of re-identification of anonymized Personal Health Information (PHI) when the data is combined with information from public databases or with inferential data (for example the predicting of gender and year of birth from first names and graduation years). The study found that, in some circumstances, the success rate of a re-identification attack on anonymized health data can be quite high. The study also found that such re-identification risks are not trivial, especially among job seekers who may post sufficient personal information about themselves on publicly accessible web sites to permit some simple re-identification attacks.

Based on the findings, the research team formulated practical guidelines and a concrete data anonymization tool that will allow data health information custodians to manage re-identification risks in their data releases and to protect the privacy of Canadians. The major focus is the anonymization of quasi-identifiers such as gender, data of birth and postal/zip codes.

The report notes U.S. research by Latanya Sweeney that 87 per cent of the U.S. population can be uniquely identified through public data sources, using the three quasi-identifier variables of the ZIP Code, gender and date of birth. Gender, date of birth and city, town or municipality of residence can also uniquely identify 53 per cent of the U.S. population.

The authors set out to determine what the parallel situation might be using quasi-identifiers and databases available in Ontario. To examine what identification databases might be available to a re-identification attacker, the researchers looked into what datasets are available from 29 Ontario Ministries, commercial information brokers, genealogical sources, professional societies, Statistics Canada and Elections Canada. They also tested the ability to link data about individuals through various publicly available sources, resulting in some hard statistical findings about the ability to link lists of Ontario physicians and lawyers to home postal codes and date of birth, and the ability to obtain date of birth, home phone numbers and the gender of home owners in Ottawa and Toronto. The report also examines inference attacks – particularly the accuracy with which gender and year of birth can be inferred using genderizing software and other predictive methods. There is also detailed analysis of the ability to predict a person's home postal code from another postal code – for example a work address or a doctor's address. The researchers considered urban and rural postal codes in Alberta, Ontario and Nova Scotia.

Based on this research, the authors concluded that region (postal code) alone, gender alone, year of birth alone, and the combination of gender and region were quasi-identifiers representing a consistently low risk of re-identification of anonymized data. They warn, however, that this only applies in the specific circumstances of their attack scenario and assumptions about risk threshold. They suggest that further work should consider record level re-identification risk.

The study contains recent research findings on the extent of personal information (name, address, postal code, telephone number and an age indicator) that Canadians were willing to post on the Internet in job resumes, and also what personal information could be recovered from sold-off hard drives. Using a file recovery utility, the researchers were able to recover personal information from 39 of 60 drives they acquired from used computer equipment vendors, despite repartitioning and reformatting. The vast majority of drives with recovered data had personal information on them, which including salary information and tax returns, personal correspondence, information on life insurance policies and inheritances, employee payroll data, police record checks, divorce documents, and personal health information, including one drive with highly sensitive mental health information about a number of individuals.

All of this leads to a recommended decision making process for anonymizing a data set, with some useful and detailed bulleted considerations for different quasi-identifiers.

Report available at: <http://www.ehealthinformation.ca/documents/OPCReportv11.pdf>

## **Electronic Health Records and the *Personal Information Protection and Electronic Documents Act***

*University of Alberta and University of Victoria, April 2005, 100 pages*

Nola Ries, Elizabeth Robertson, Fiona Moore and Jane Steblecki

This report examines the issues of privacy, confidentiality and security in the context of personal health information and electronic health records (EHRs). It notes that “the call for speedy progress [in EHR systems] may be somewhat premature until adequate discussion has occurred in regard to privacy, confidentiality and security issues”.

Part 1 surveys some of the issues surrounding EHR systems, including the challenges of establishing such systems, the concepts of privacy, confidentiality and security within the health care framework, the status of EHR systems in Canada and the complexity of the Canadian privacy landscape. This part ends with a comment by Professor Elaine Gibson that protecting personal information should not be viewed as a barrier to the deployment of a pan-Canadian Health Infostructure, but that “strict privacy and security regimes must be understood as essential to maintaining the trust of members of Canadian society that our personal health information is receiving the highest of protection”.

Part 2 is a detailed review of *PIPEDA*'s rules in the EHR context, as well as rules regarding EHRs in health information-specific laws in Manitoba, Saskatchewan, Alberta and Ontario.

Particular attention is paid to the issue of consent in *PIPEDA* in the EHR environment. The authors explore the challenges of obtaining informed consent from patients for future use or disclosure of information on an EHR, noting the problem that future information uses cannot be foreseen when the individual's personal information is first put into the system. The concept of the “circle of care” and the ability to rely on implied consent for treatment-related uses or disclosures of personal information is also discussed, as is the notion of what, in fact, constitutes “informed consent”. There is also some discussion of secondary research uses, including reference to studies on patients' acceptance of secondary use of EHRs for research.

The review of provincial health privacy laws contains detailed analyses of EHR provisions, including how some of these provisions have changed over time. This section concludes with the observation that health sector entities that are subject to provincial health information statutes may also have to comply with *PIPEDA* if they engage in commercial activities, but there are few situations in which an organization will find it impossible to comply with requirements of both. The authors add that, if such situations arise, the organization should seek further guidance from provincial commissioners or the federal commissioner and, if legislative rules impede delivery of health care to patients, those experiences ought also to be reported to privacy commissioners as well as relevant government departments overseeing the legislation.

Part three is a detailed examination of EHR initiatives in Australia, the United Kingdom and the United States, the legislative environments and the issues to be resolved, including such issues as data linkage and function creep and declining physician support (in the U.K.) for electronic records systems.

There are three appendices: 1) a legislative table of current public sector, private sector and health sector laws and where they apply; 2) case summaries of EHR use by four agencies – BC Cancer Agency, the Alberta Capital Health Region, the Saskatchewan Pharmacy Information Project, and the Nova Scotia Hospital Information System; and 3) a list of best practices in developing an EHR system, based on CSA privacy principles. For health information policymakers, this appendix may be one of the most important components of the report.

Report available at: <http://www.law.ualberta.ca/centres/hli/pdfs/ElectronicHealth.pdf>

## **Secondary Uses of Personal Information Held on National Electronic Health Record Systems: Key Developments, Issues and Concerns**

*Centre for Bioethics, Clinical Research Institute of Montreal, June 2007, 93 pages*

David J. Roy and François Fournier with technical assistance from Thierry Hurlimann

The intent of this study is to draw attention to the perspectives, opportunities and concerns that national Electronic Health Records systems (nEHRs) will raise concerning secondary uses of Personal Health Information (PHI). The research is extremely well-documented and up-to-date, with a thorough analysis of secondary use concerns.

The authors propose that, where PHI is used in ways which have little or nothing to do with direct patient care, patient trust in the therapeutic relationship with health care professionals is at stake. Secondary uses may also threaten patient autonomy—if patients are thwarted in the degree of control that can exercise over their PHI—and the fidelity (integrity) of health care professionals. In addition, such uses may raise broad and critically important social, cultural and democratic issues.

Secondary uses of PHI are generally defined as non-direct care uses, and include both health related purposes (such as health care management, public health, medical research) and non-health purposes (such as law enforcement, immigration). The current boundary between primary and secondary uses is challenged by some secondary users, such as medical researchers, who wish to be recognized as primary users and therefore be exempted, for example, from more stringent consent processes.

The authors describe EHRs as patient-centred records that are derived from Electronic Medical Records (EMRs). EHRs are subsets of EMR information, uploaded to central sites and used for a range of purposes related to patient-oriented services and improvements in health care delivery. While some countries, Quebec and some other provinces of Canada are moving ahead with provincial nEHRs, as yet, no nEHRs are fully deployed and operational on any national basis. Thus the research report is a snapshot of an evolving and fluid situation, reflected on the issues connected to future secondary uses of PHI in a nEHR.

Part 1 of the report considers the pan-Canadian EHR system proposed by Canada Health Infoway and addresses three principal aspects of secondary uses of personal health information within national electronic health records systems: the elements in the design of nEHRs that enhance or limit secondary uses of PHI; the governance framework of nEHRs regarding secondary uses of personal health information, including questions relevant to consent; and thirdly, expectations and concerns raised by various stakeholders on secondary uses of PHI stored in nEHRs.

Part 2 is an extremely detailed and well-documented case study of the U.K. National Health Service (NHS) Summary Care record. Over the past 10 years, this evolving system has been the subject of extensive, often fierce, debate over secondary uses of PHI. The report addresses the legal framework for secondary uses of PHI within this system, the types of secondary uses envisioned, and concerns that have emerged about these uses. It also describes a number of proposed “improvements” and requests for clarification raised by various stakeholders.

Part 3 is a summary and synthesis of in-depth conference call interviews conducted in May 2007 with a dozen well-known Canadian experts (names are listed) on issues related to secondary uses of PHI. This includes a detailed discussion of the widening circle of secondary uses, what issues should be emphasized in discussions about nEHRs (for example, the values of privacy, autonomy and dignity), health research as a secondary use (which raised numerous concerns), the challenge of consent, and governance issues.

Report available at:

[http://www.ircm.qc.ca/bioethique/english/whatsnew/EHR\\_Secondary\\_Use\\_Report.pdf](http://www.ircm.qc.ca/bioethique/english/whatsnew/EHR_Secondary_Use_Report.pdf)

## **Social Uses of DNA Information in the Policy Making Process: Analysis of Two DNA Identification Bills**

*University of Ottawa, April 2006, 74 pages*

Dominique Robert and Martin Dufresne in collaboration with Alain Lachapelle and Marie-Lyne Vachon

This report focuses on the uses of DNA in the criminal justice system, and on an understanding of the social tensions involved, through a comparative analysis of the submissions from various interest groups, tabled before Parliament in the legislative process leading to the promulgation of two DNA bills (C-3 and C-13). The first of these bills allowed for the creation of a national DNA database and the second bill added to the list of offences for which obtaining DNA samples is allowed.

The authors point to the three ways the topic of DNA is broached in the literature concerning its use in the criminal justice system. DNA is treated either as: a chemical substance to be treated forensically; an investigation tool to be used strategically; or as a sociological manifestation of how modern cultures are redefining the relationship between science and the law.

Analysis of the reports submitted by the groups and associations involved in the study of Bill C-3, which led to the creation of Canada's national DNA database, shows that the various political actors are in general agreement when it comes to the usefulness of creating a genetic database. However, they are divided or disagree on at least five major issues: the usefulness of DNA within the criminal justice system; the similarity between fingerprints and genetic prints; the scope of discretionary power a judge should have in ordering the taking of a sample; the retroactivity of samples; and the need to conserve DNA samples.

When Bill C-13 proposed the expansion of the existing genetic print system in 2005, six major issues arose out of the various reports and presentations. Certain issues were already present in past debates while others were new: the expansion of the primary and secondary offences lists and related criteria; the point in time when a DNA sample should be taken; the scope of the law's retroactivity; the discretionary power of judges in ordering the taking of a sample; the treatment of persons found not criminally responsible; and the conservation of samples.

The debates surrounding these bills have led to concrete results. Not only have the debates influenced the legal texts, they have given rise to and feed into powerful symbols. Analysis reveals two inter-related results: 1) offenders are being transformed into criminal monsters; 2) the objectives of the penal system are being altered – the system no longer searches for justice but rather for truth. The combined effect tends to reinforce the notion that procedural guarantees are obstacles to efficient crime fighting.

Finally, the authors feel that debate is required to answer such questions as: What is the efficiency of the penal system? How do you measure its efficiency? Efficiency for whom?

Report available at: <http://www.saea.uottawa.ca/index.php?lang=fr>

Student number: ADN2007; password: ADN2007

## Technology Choices and Privacy Policy in Health Care

*Memorial University, April 2007, 130 pages*

Edward Brown, Todd Wareham, Gerald Farrell, Theodore Hoekman, Rhonda Chaytor, Jennifer Barrigar, Tracy Ann Kosa, Carla Barton, Neil Barrett, Chris Mercer and Andree Thoms

This report critiques privacy and security-related technologies and the assumptions and biases available technologies may have on legislative and policy choices in Canada's health care field. It is based on extensive research and numerous interviews with academics and health care, information technology and privacy professionals.

The authors find a strong bias towards data security technologies or a perimeter model designed to prevent unauthorized access, to the detriment of considering alternative approaches to privacy technologies. Even privacy technologies such as consent management, which reach beyond security as they are designed to restrict the actual purposes for which personal data are used, can be viewed as more sophisticated access controls within the same model. Patients' actual control of their PHI is imperfect at best since their consent can be implied, there are so many exceptions to consent, and they cannot withdraw their personal health information (PHI) from the health care system. They must trust others and rely on oversight and other enforcement mechanisms.

The authors are concerned about over-reliance on the perimeter model for Canada's health care system. Role based access control, consent management and privacy rights management technologies require engineering that are essentially policy choices about information access. These can create a legacy infrastructure that is difficult and expensive to alter when more fluidity in sharing PHI is essential to quality patient care.

The report examines privacy legislation in Canada and, in particular, four provincial health-sector laws and the notion of data protection as a form of privacy. It describes the creation of custodians or trustees of PHI, with rules enabling data sharing, which has led to a patchwork of disclosure provisions, consent exceptions and contractual obligations involving primary care professionals, IT companies, administrators, oversight and other agencies. Also included is a review of regulations under health information privacy laws and the role of privacy impact assessments in the healthcare environment.

The authors recommend more discussion concerning which rules will be enforced or monitored by technology vs. non-technology (human) approaches. Both doctors and patients do not fully understand the infrastructure protecting their information, yet they are required to accept them. Safeguards can create an illusion of protection while simply shifting vulnerability and decision-making from one set of humans to another, and even away from the "circle of care" – those directly involved with patient-care delivery– to service providers and administrators

The report includes interviews with stakeholders, confirming concerns about the risks inherent in automated PHI, the immaturity of some security and privacy technologies, limitations of the role-based conception of access control, and whether there is any really meaningful patient control offered through consent mechanisms (both legislative and technological). It concludes that privacy extends well beyond data protection to issues of dignity and trust, for which technological solutions have yet to be created.

Report available at: <http://cpig.cs.mun.ca/TechnologyChoices.pdf>

## **An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies**

*Dalhousie University, April 2005, 64 pages*

Dr. Teresa Scassa, Dr. Theodore Chiasson, Professor Michael Deturbide, Anne Uteck

Radio Frequency ID tags are poised to replace the UPC barcode as a mechanism for both wholesale and retail inventory control. Yet the tiny chips offer a range of potential uses that go beyond the bar code. What was conceived of as a superior inventory control device has the potential to become a powerful data-matching technology and, ultimately, a technology of surveillance.

Media attention has tended to focus on consumers' concerns about retail uses of RFID technology, especially the ways in which it can be used to feed the ever-increasing demand for personal information in exchange for goods and services in the ordinary retail marketplace. However, privacy concerns extend far beyond the commercial context. RFIDs have virtually limitless applications and are being considered for use (or are already deployed) in a range of contexts from delivering health care, managing library collections and controlling the safety of food supplies, to employee monitoring or government surveillance as a part of national security initiatives.

The authors begin with an exploration of the technology that underlies RFIDs, and an overview of the present use and anticipated deployment of RFID technology. They then examine the privacy implications of the use of RFID technology. Noting that privacy law can either be formative or reactive in addressing the issues raised by new technology, the authors examine various legal initiatives in the U.S. and abroad that attempt to deal with privacy implications of RFID technology, as well as activity by consumer and privacy activists.

Using *PIPEDA* as a focus, the authors consider the extent to which existing private sector privacy legislation in Canada sets norms that are useful or practical in addressing RFID technology, and identify gaps in the legislation.

While this report focuses on private sector use and deployment of RFID technology, the authors also consider the broader public context. Government adoption or use of RFIDs for government programs will support private sector deployment of these technologies, and may play a role in limiting government response. Further, the potential for personal information to migrate with relative ease from the private sector to government adds a public dimension to private sector developments.

The authors conclude with a set of specific recommendations addressing the need for RFID-specific standards and guidelines; consumer awareness that data collected in the private sector may be sought by government departments and agencies, and may be obtained without their knowledge or consent; mandatory privacy impact assessments by government agencies that would apply to new programs or initiatives employing RFIDs, and legislation or regulations that would require manufacturers and retailers to use RFID tags only on removable hang tags or product packaging.

Report available at:

[http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs\\_Report2\(Single\).pdf](http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf)

## The Challenge of Consumer Identification with New Methods of Electronic Payment

*Option Consommateurs, August 2006, 61 pages*

Jacques St-Amant

This report is a review of methods to confirm identity during electronic transactions, the security of the transactions, and the compliance of new biometric identification technologies with legislative frameworks governing the protection of personal information.

After analyzing the current trend towards the use of biometric methods for consumer identification, the author concludes that biometric authentication systems will likely be no more secure than current systems, while posing challenges to consumer privacy.

Biometrics work well only if the system can verify that the biometric came from the person at the time of verification and that the biometric matches the master biometric on file. There are reasons why systems often can't do just that. Also, although biometrics are unique identifiers, they are not secrets and are not failsafe as unique identifiers.

The author concludes that the use of biometric authentication technologies presents greater legal and financial risks than they are worth. He suggests biometrics are complementary to other existing technologies and that no single system is fully reliable.

On the issue of consumer privacy he notes that business is demonstrating an increasing propensity for collecting personal information in an attempt to manage legal and financial risk. The rapid rise of the electronic transaction card and the parallel rise in the use of Personal Identification Numbers (PINs) have led to a redefining of the respective responsibilities of the customer and financial institutions. Although security was historically seen as a shared responsibility, in practice it was a bank's responsibility to ensure that the signature it accepted was indeed the signature of its client. According to the author, banks are making an attempt to place more of the onus on the customer.

The author feels that consumers have little control over what is being done or will be done with the information that is revealed in return for goods and services. Systems designers argue that secrecy is necessary to security thus adopting the *security through obscurity* philosophy. The author offers evidence that this approach has long been discredited and that all stakeholders would benefit from an open discussion of the issues. Authentication systems should be designed so that the risks to banks and their commercial clients are balanced against the risks to consumers. The author fears that this is not the case and that the imbalance favours the banks although they occasionally do a poor job of managing the risks.

Report available at: [http://www.option-consommateurs.org/documents/principal/fr/File/rapports/renseignements\\_personnels/oc\\_rr\\_rens\\_pers\\_biometrie\\_200608.pdf](http://www.option-consommateurs.org/documents/principal/fr/File/rapports/renseignements_personnels/oc_rr_rens_pers_biometrie_200608.pdf)

## Digital Rights Management Technologies and Consumer Privacy: A Canadian Market Survey and Privacy Impact Assessment

*Canadian Internet Policy and Public Interest Clinic, April 2007, full report 213 pages*

David Fewer and Philippe Gauvin and Alex Cameron

Digital Rights Management (DRM), as defined in this study, is “a system comprising technological tools and a usage policy, which is designed to securely manage access to and use of digital information”. This study observes the behaviour of a number of DRM technologies with a view to assessing the impact of these technologies on consumers’ privacy, and assessing the DRM distributors’ compliance with *PIPEDA*.

The researchers divide the DRM technologies analyzed in this study into two categories: autonomous DRM and net-dependent DRM. Autonomous DRM requires no outside interaction for the DRM system to operate (for example, software that requires a CD-key to become useable or that deactivates after a certain number of uses). Net-dependent DRM, in contrast, involves Internet authentication or Internet surveillance of uses, such as web-enabled software validation or online music subscription services that deploy digital licenses to access locked content. All net-dependent DRM communicates with external computers.

The researchers consider how DRM is changing the ways individuals interact with digital content by tracking and controlling individuals’ access and use of copyrighted works, and in the process is eroding privacy rights. The study assesses the use of DRM in the Canadian marketplace and how *PIPEDA* may apply to DRM. They examine the chilling effect that DRM, as a form of surveillance, may have on individuals’ access to controversial or unconventional information and the legal right to speak anonymously or receive information anonymously – instrumental in exercising an effective right of freedom of expression.

Based on a survey of the Canadian marketplace, the researchers undertook a technical assessment of 18 selected DRM applications from different market sectors between January and March 2007. These included Apple *iTunes Music Store* and *iTunes Video Store*, Azureus *Zudeo*, eReader (*The Da Vinci Code*), InterActual (Disney’s *Pirates of the Caribbean*), Intuit *QuickTax*, Microsoft *Office Video*, *Napster*, Symantec *Norton SystemWorks 2006* and Telus *Mobility Spark*.

The assessments were carried out using a controlled test-bed setup consisting of a testing computer and gateway computer configured to emulate a typical user environment. University of Ottawa law students and CIPPIC counsel, acting as ordinary users, carried out the testing.

The report contains detailed research analysis of each DRM application, and a detailed assessment of 12 net-dependent DRM technologies that researchers observed engaging in automatic communications of information through DRM against the requirements of *PIPEDA*. This assessment considered privacy policies, related documentation and organizational responses to access requests. The researchers considered that none of these organizations were compliant with CSA privacy principles.

The research also discovered that several third parties, particularly Akamai Technologies, Omniture and Doubleclick, were frequently involved in the DRM applications tested. These third parties collect considerable user information, including IP addresses, browser type, operating system, ISP, bandwidth and time of day. In the case of at least two of these companies, the researchers state they were never informed of their existence or their role in the DRM system. At least one organization failed to properly secure personal information and communicated the user’s username, password and email over the Internet without encryption.

Report available at: [http://www.cippic.ca/uploads/CIPPIC\\_Report\\_DRM\\_and\\_Privacy.pdf](http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf)

## **Privacy Rights and Prepaid Communication Services: a survey of prepaid mobile phone regulation and registration policies among OECD member states**

*Centre for Policy Research on Science and Technology (CPROST),  
Simon Fraser University, March 2006, 80 pages.*

Gordon Gow and Jennifer Parisi

This research report is a survey of policies regarding the regulation of prepaid mobile phone services in OECD countries. The intent was to contribute to an evidence-based policy deliberation on the issue of privacy rights and prepaid communications services in Canada and elsewhere by examining the policy positions and experiences of the countries surveyed. As the report is intended to provide empirical evidence for informed decision-making on this subject, there are no specific recommendations on how Canada or other countries should proceed on this issue.

Prepaid mobile phone services are typically purchased by a customer who buys a mobile handset and airtime credit and then obtains additional airtime credit vouchers or buys stored value cards with cash, debit or credit card transactions. In some countries individuals can obtain pre-paid services in a completely anonymous manner without having to furnish any user identification. Due to increasing concerns about the use of anonymous prepaid phone services for criminal and terrorist activities, several countries have introduced regulations requiring mobile phone operators to collect customer information for prepaid services:

The report states that, while Canada does not have such regulations in place, the possibility of this occurring in future ought to be a matter of interest to the Privacy Commissioner because the legal and ethical implications remain uncertain. Public debate has been encumbered by a lack of information about what objectives such a requirement might realistically seek to achieve or how it might be implemented and enforced.

The report helps address this question by presenting findings from a survey of OECD countries on questions that include government policy, industry concerns and other evidence on the use and abuse of prepaid services, as well as forums and opportunities for public debate of the issue. Research was conducted between April and October 2005, relying on numerous published sources of information as well as questionnaires sent to data protection authorities and other agencies in OECD countries. Information, at varying levels of detail, was obtained from about 25 of the 30 OECD countries, as well as from South Africa.

The report contains a detailed country-by-country summary of each country's positions on prepaid communications services registration. Among countries surveyed, the profiles on Australia, Canada, Germany, the Netherlands, Norway, the Slovak Republic, Switzerland, the United Kingdom and the United States include the most detailed discussion and analysis of the country's position on the issue, the reasons for and against registration, the specifics of regulation, the marketplace response and logistical issues.

The report includes some summary comments on the justification for and against prepaid registration, the feasibility of implementing and enforcing regulatory measures, and possible uses of alternative measures.

The report suggests a test of "reasonable appropriateness" is required in considering the collection of subscriber information for prepaid mobile communications, and proposes that this question could be settled in one of three ways: by producing empirical evidence to show that registration has a deterrent effect on crime and terrorism; by making a politically and socially acceptable case for prepaid phone registration based on the interpretation of existing legislative authority; or through an efficiency argument that claims that such regulation will improve the efficiency of law enforcement and public safety.

Report available at: <http://www.sfu.ca/cprost/prepaid/>

## Vehicle Technology and Consumer Privacy

*Automobile Consumer Coalition/Car Help Canada, March 2007, 74 pages*

Paul Coninx

This report explores the rapid growth of technologies in North America and Europe that record the actions and locations of private vehicles, their implications for motorists' privacy, and ways of dealing with them. The technologies reviewed include: event data recorders (EDR), global positioning systems (GPS), vehicle telematics (communications devices), radio frequency identification (RFID) and automatic plate number recognition (APNR).

The author concludes that motorists' behaviours will be increasingly tracked, due to road safety, congestion, environmental concerns and the efficiencies and convenience these increasingly inexpensive technologies offer. Interested third parties include transportation departments and the police, automobile manufacturers, service providers and insurance companies.

Motorists have long required drivers and vehicle licenses and, over time, transportation departments have developed vast databases on current and previous owners which are too widely accessible. The author recommends more restricted access due to the risks of personal harm, identify theft, unwanted solicitations and overreaching state agencies.

EDRs assist in crash investigations but are opposed by some car manufacturers as they can result in motorists having their own cars testifying against them. The author disagrees as motorists are on public roads, and recommends that EDR be enhanced and made mandatory and accessible to interested parties, including the motorist. However, the recording time of such devices should be strictly limited to no more than several seconds before and after a crash occurs. He also promotes driver condition monitoring (but not recording), to alert motorists to drowsiness and lane wandering.

The author concludes that GPS and related technologies should be a motorist's choice, based on full information about such privacy implications as possible third party access to their location, direction, speed and even conversations. Motorists should always retain the right to have such devices removed from their vehicles on demand. He recognizes the real and potential opportunities for abuse that automatic cameras and APNR can pose, but also acknowledges their road safety value in some circumstances and that they are no more invasive than being stopped by the police. He recommends several safeguards to preclude abuse, such as not assessing demerit points when the driver is unknown.

The author points out that the right to individual privacy when inside a vehicle has not been held to be a priority in Canadian and American courts, in spite of the *Charter of Rights and Freedoms* and the U.S. constitution. The author also presents the case that increased use of transponders and RFID is inevitable, to control congested roads, collect tolls and parking fees. These technologies pose the greatest threat to privacy if they lead to large, centralized databases shared by different companies and jurisdictions. This threat could be alleviated through the use of prepaid "smart" transponders that would not require the storage of personal data. Such decentralized technology should be put into place before centralized technology becomes the norm.

The author finally makes numerous recommendations regarding protection of the personal data gathering by these new technologies, including encryption, restricted access, avoidance of data matching and full information to motorists.

Report available at: <http://www.carhelpcanada.com>

## **Location-Based Service and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada**

*University of Victoria, June 2005, 44 pages*

Colin J. Bennett and Lori Crowe

This report looks at 'mobile' surveillance and tracking technologies: existing products; the current state of product availability; actual and potential application; and target groups. It discusses ambiguous media coverage of 'mobile' surveillance issues, and poses the following questions: How are tracking devices being used or misused, and by whom? What are the claimed benefits of such devices and are they legitimate? Who is at risk of having their privacy violated and in what way? How can privacy rights be protected? Finally, it aims to get a better purchase on the privacy implications of location-based services that are currently available in the Canadian marketplace, and therefore what specific challenges might face the Office of the Privacy Commissioner of Canada and its provincial counterparts.

The authors provide product information and operational requirements and limitations on various technologies, such as those used for 911 emergency services (wired and wireless); Radio Frequency Identification Devices (RFIDs); Event Data Recorders (EDRs, used as automotive 'black boxes'); and Personal Location Devices (PLDs). More importantly, they examine the pros and the cons of their uses. For instance, while a PLD or RFID device can help parents track their children in an amusement park, it also could be used to locate, stalk and kidnap those same children. EDRs, installed in many new cars (unbeknownst to the vehicle's driver) can help emergency services locate a vehicle if needed. Conversely, EDRs can be used by employers to track their 'mobile' employees (such as delivery drivers) unscrupulously, and have been used successfully by prosecutors in court cases.

Target groups identified include mobile workers; the elderly, disabled, and health care patients and caregivers; children and teenagers; drivers and individuals in professional and recreational activities; and prisoners and offenders. However, these technologies can be used by or against any individual. Locational data can be extraordinarily sensitive in that it can be monitored remotely, without the individual's knowledge and consent. It may be collected continuously and stored indefinitely. The level of consumer education and experience is low, and the potential value of such information for government and business is enormous.

The authors conclude that there are potential challenges to existing privacy regulatory frameworks, and that attempts to apply standard information privacy principles to locational data are few. In Canada, federal and provincial privacy commissioners need to consider ways in which the general public should be educated about the capture, use and disclosure of locational information. They might also consider ways in which they might become involved more closely with the standards setting processes that have such profound and long-term impacts on surveillance practices.

Report available at: <http://web.uvic.ca/polisci/bennett/pdf/LBSFINAL.pdf/>

## Location Technologies: Mobility, Surveillance and Privacy

*The Surveillance Project, c/o Department of Sociology,*

*Queen's University, Kingston, Ontario, March 2005, 74 pages*

David Lyon, Stephen Marmura, Pasha Peroff

This research report examines new privacy concerns created by Location Based Services, their underlying technologies and the advent of real-time tracking. The purpose of the research is to draw attention to current concerns about tracking individuals using such technologies, including what manufacturers and service providers are doing to ensure compliance with privacy legislation in Canada. The report also considers whether corporate strategies resonate with public expectations of such services.

Information sources include interviews that took place in 2005, mainly in Ontario, with industry experts. Secondary information sources included media reports, industry websites, published surveys and company privacy policies.

The report defines location technologies as those that can pinpoint coordinates, continuously and in real time. The principle location technologies considered in the report are cellular telephone location technologies, some of which are network-based and some of which require the use of Global Positioning System (GPS)-equipped handsets. Other GPS enabled technologies such as vehicle navigation systems are also addressed. The report does not include other tracking technologies such as active Radio Frequency Identification (RFID) tags and close-circuit television (CCTV) systems, as they are not capable of generating continuous, real-time, accurate location information about an individual.

The report considers market forecasts, market drivers and impediments to growth of location-based services, and the privacy issues involved in such services. The authors state that major wireless carriers and location-based service providers in Canada will likely be proactive in anticipating and addressing public and legal concerns about the appropriate collection, use and disclosure of customer information but may not invest the resources needed to head off potential problems in the area of data security.

According to the authors, the nature of location information will enable a more comprehensive picture of individual and collective patterns of movement which will invite the creation of new algorithms designed to make inferences about the potential relationships between mobility and identity. The report also notes that location data is being stored for future marketing use to target advertising to consumers and to gather information concerning the mobility of populations, much of which involves the sophisticated use of anonymous, aggregate data to categorize consumers into specific target groups. The authors stress that, while privacy legislation such as *PIPEDA* is clearly necessary to protect the rights of individuals, it is not designed to deal with commercial social sorting practices made possible through use of anonymous aggregate data.

The report includes recommendations for future research into a number of variables that influence privacy attitudes towards location technologies, including the role played by government, industry and the media. It suggests the need for comparative studies of location technologies with other countries having fairly dense urban populations and widespread cell phone use. It also suggests further investigation into the accuracy of predictions made about business and technology developments by marketing research firms; the vulnerabilities of private and public sector data storage and management, including location data; and the issues of media convergence in light of traditional government policy approaches to various mass media and communications media.

Report available at: <http://www.surveillanceproject.org/files/loctech.pdf>

## The Use of Video Surveillance Cameras in Public Places in Canada

*Université du Québec, Ecole nationale d'administration publique, December 2005, 66 pages*

Christian Boudreau and Monica Tremblay in collaboration with Paul-André Comeau

This report is a study of the perceptions, issues, privacy impacts and best practices on the use of video surveillance in Canada. The study is based on a review of 22 video surveillance projects of publicly accessible sites (most targeting downtown streets and commercial areas), seven provincial privacy guideline publications, input from four Québec-based focus groups, media analyses and an overview of the literature.

The authors feel that authorities must consider five principal issues as the use of video surveillance becomes more widespread in Canada.

Firstly, based on their analysis of the Canadian context, the authors conclude that, due to a growing sense of insecurity within the population, the main pressure for increased video surveillance comes from various community groups (business owners, citizens, etc.) rather than from government and public institutions. Although not necessarily the best approach, video surveillance is usually the first solution that comes to mind. The result is often a displacement of the problem (for example drug dealing, prostitution) and a growing threat to the privacy of individuals.

Secondly, the importance given to privacy issues varies according to current events. Terrorist acts are not alone in generating the kind of fear that triggers demand for increased video surveillance. Any criminal or delinquent act can capture the public imagination depending on the victims and circumstances. The danger lies in overreacting to a situation that is limited in scope since the decisions are often hard to reverse.

Thirdly, digital camera technology opens the possibility of generalized biometric identification in public spaces. The authors feel that this further threat to privacy may require closer regulation and monitoring of video surveillance systems by responsible authorities.

Fourthly, although video surveillance is usually seen as a tool for monitoring the criminal element and discouraging crimes against persons or property, certain groups who feel at risk of discrimination by authorities (due to ethnicity, age, gender, etc.) consider it a tool for ensuring transparency and fair treatment. Again the question comes down to balancing the quest for security against the need for privacy.

Finally, although community groups are often the ones requesting increased video surveillance, they are also the ones looking for increased oversight and regulation of these systems. This often puts them at odds with the system administrators who wish to maintain their autonomy. This tension points to the need for clearer governance rules and increased dialogue among stakeholders.

Report available at: <http://archives.enap.ca/bibliotheques/2006/06/24261876.pdf>

## A Preliminary Exploration of Workplace Privacy Issues in Canada

University of British Columbia, April 2006, 60 pages

Vance Lockton, Richard S. Rosenberg

This report explains the importance of workplace privacy, discusses the inadequate legal protections in Canadian and American jurisdictions, reviews specific areas of concern and concludes with five problems that must be addressed to resolve them. It is intended to provide a framework for analysis by employers, employees and policy-makers alike.

The report identifies privacy as an issue of trust and human dignity. Employees generally associate workplace monitoring with enforcement and punishment that can cause anxiety and depression. In turn, employers monitor to reduce employee theft, ensure productivity, protect against workplace litigation, avoid workplace tragedies and prevent electronic attacks and leaks. Employers are increasingly resorting to more thorough pre-employment checks, access controls, surveillance cameras, Internet, e-mail and network monitoring, and tests and searches.

The authors note that workplaces are increasingly extended into homes, public areas and cyberspace, due to company-provided electronic devices which may be used for both business and personal purposes. This has blurred the line between on-duty and off-duty, and increased the prospect of surveillance. Yet some studies find companies that engage in electronic monitoring and drug testing to be more stressful and less productive workplaces than those that do not.

The report identifies several deficiencies in Canadian laws protecting employee privacy. The *Privacy Act* only applies to federal government institutions, while *PIPEDA* does not apply to employee personal information for provincially regulated businesses. The federal Privacy Commissioner, who oversees these two Acts, does not have remedial powers and, under *PIPEDA*, non-compliant institutions are not identified by name. In addition, privacy laws in Alberta and British Columbia have lower standards concerning the collection of employee information as long as notification is given. The majority of collective agreements in Canada provide no additional protection.

In contrast, Quebec's *Civil Code*, *Charter of Rights* and accompanying privacy legislation exceeds the protections found in *PIPEDA*. The report cites New South Wales, Australia, as a jurisdiction where workplace surveillance is properly regulated, including mandatory prior notification, a listing of prohibited surveillance and restrictions on covert surveillance.

The authors review specific complaint investigations and case law, covering closed circuit TV (CCTV), mail openings, keystroke monitoring, off-duty surveillance and drug testing. The report concludes that the power imbalance between employers and employees means privacy will not be protected by default. Specific recommendations include a need for greater understanding that workplace privacy issues need not be adversarial as both employers and employees benefit from workplaces based on trust and mutual respect; a need for legislation to protect employees in provinces and territories not currently covered by employment privacy legislation, and pro-active legislation to specifically address surveillance. Recommendations also include empowering the Privacy Commissioner to publicly identify offending companies, better anticipation of the privacy impacts of new technologies, and greater Canadian research to deal with them.

Report available at: <http://www.cs.ubc.ca/~lockton/workplace.pdf>

## Under the Radar? The Employer Perspective on Workplace Privacy

Ryerson University, June 2006, 22 pages

Avner Levin, Mary Foster, Mary Jo Nicholson and Tony Hernandez

Canadian employers and consumers recognize the need to balance workplace privacy with other interests to ensure a competitive economy. The purpose of this report was to document current practices from the employer perspective and to understand how such a balance is viewed and implemented in a Canadian context.

The project was based on a structured interview and analysis methodology, using a cross-country/cross-industry representative sampling and taking into consideration such factors as union representation and employer size. The interviews centred on key indicators such as employer awareness of workplace privacy; the existence and capabilities of a variety of technologies for monitoring/surveillance; the purposes of surveillance; justification for workplace privacy; and government and industry roles.

Federal and provincial Information protection legislation addresses some aspects of workplace privacy. The report provides a description of the legal terrain in Canada, looking at federal and provincial privacy legislation and the impact these laws have on business practices and outlooks. The conceptual approaches to workplace privacy, however, are based on the fundamental concepts of privacy in general.

The authors provide a framework pertaining to prevailing privacy-in-workplace concepts, one based on *rights* (the European model, based on the right to dignity or a private life) and one based on *property* (the U.S. model, based on the employer's ownership of the workplace). The *rights* model prevails in Quebec and is reflected in its legislation, while the report found that federal and other provincial legislation is often wrongly interpreted by Canadian businesses to reflect the U.S. model when, in fact, it imposes a standard of reasonableness on employers.

Employers' attitudes on the role of government and industry in dealing with workplace privacy issues were explored. Those interviewed acknowledged that legislation related to privacy acted as motivation for companies to take formal steps to comply. However, no employer saw any need for additional federal privacy legislation on privacy in general, and on workplace privacy in particular. They would, however, welcome guidelines that would clarify existing legislation.

The report focuses on the surveillance and monitoring measures reported by employers, and the purposes for which they were introduced to the workplace. The report evaluates these measures and purposes in light of the *rights* and *property* models, and in light of the legislated requirement for such measures to be reasonable.

The report found that Canada appears to be developing a hybrid model of workplace privacy issues management, based on trust. As one employer highlighted, "the interest of the company and the interest of the individual are inseparable.... We feel strongly about building that foundation of trust between the employee and the company". All employers interviewed agreed that some form of workplace privacy is necessary for the "regular and trouble-free functioning" of their business, and that it indeed may result in increased productivity.

The employers interviewed uniformly insisted, however, that their employees "do not perceive workplace privacy as a "real" issue". The report concludes on that basis that Canadian employers view workplace privacy as a non-issue as well – "under the radar" screen of most employers. The report therefore calls for further research into employees' attitudes to workplace privacy.

Report available at: <http://ryerson.ca/faculties/business/news/archive/UnderTheRadar.pdf>

## ***PIPEDA and Identity Theft: Solutions for Protecting Canadians***

*B.C. Freedom of Information and Privacy Association, April 2005, 73 pages*

Stephanie Perrin, Philippa Lawson, Jennifer Manning and Robert Gellman.

Leila Pourtavaf, Research Assistant

This report describes identity theft as the “perfect non-violent yet highly lucrative crime” and sets out to assess its scope both in Canada and the U.S., the methods of identity theft, legal issues in prosecution, legal responses in the U.S. and the protection offered by the *Personal Information Protection and Electronic Documents Act (PIPEDA)* in Canada. The report ends with a series of recommendations to improve protection against identity theft in Canada.

The report highlights statistical data from 2002 and 2004 on incidences of identity theft in both Canada and the United States. The report differentiates identity theft from simple credit card or bankcard fraud where banks have taken steps to limit individual liability. ID theft is defined as situations where an individual takes over the identity of the person to open new accounts, an activity which the report states, “creates real problems for the honest individual to substantiate their own identity”. There are informative descriptions with anecdotal examples of different methods of identity theft techniques.

Three chapters of the report cover the identity theft legal environment in the U.S., including legal issues, legal responses, and an analysis of what is referred to as the “ChoicePoint Scandal”. Reasons for the low prosecution rate for identity theft cases in the U.S. are explored, including a discussion of one benchmark legal case, *Huggins v. Citibank*. There is also a useful selective inventory of U.S. laws addressing identity theft, including both federal and state laws. In the U.S. discussion, the report describes a Model Regime of Privacy Protection, proposed in the wake of the ChoicePoint scandal by two public interest lawyers. The 16 specific proposals contained in this Model Regime are all described, followed by analysis.

From a Canadian perspective, the most useful aspect of the report is the very detailed examination of the protections against identity theft currently available under Canada’s *PIPEDA*, with detailed analysis of specific clauses of the 10 CSA Principles where the law offers specific protections.

This chapter is useful, in fact required, reading for anyone specifically concerned with corporate obligations to prevent identity theft or seeking to understand how *PIPEDA* can be used to protect consumer interests, including filing a complaint under the act.

The report concludes with eight specific recommendations that include the need for further research on company practices and ID theft risk and specific guidance for business, as well as more public education on this issue. The federal Privacy Commissioner should also be encouraged to collaborate with other commissioners and police agencies on investigations, audits and public education, and to take identity theft cases to the Federal Court to seek redress and damages for victims.

Proposed legal changes include mandatory breach notification by businesses where individuals are put at risk of ID theft, and amendment to Canada’s *Criminal Code* to address identity theft. The report also calls for acceleration in establishing mutual assistance arrangements for the prosecution of ID theft, and mutual assistance for the investigation of privacy breaches between Canada and the U.S.

Report available at: [http://fipa.bc.ca/home/hot\\_topics/14](http://fipa.bc.ca/home/hot_topics/14)

## **Privacy in the Criminal Justice System: Investigation DNA**

*University of Ottawa, April 2007, 49 pages*

Martin Dufresne and Dominique Robert in collaboration with Pascal Dominique-Legault, Alain Lachapelle and Marie-Lyne Vachon

This report contextualizes the handling of DNA samples within the broader privacy debate, from the time samples are collected during an investigation to their use in judicial proceedings. The 'CSI effect' has made the use of genetic information in crime investigations as well known as fingerprints, yet there has been no serious public debate (outside of special interest groups) on the use of DNA in the criminal justice system.

The report is composed of five sections, the first of which reviews the growing challenge of maintaining privacy rights in a "private life" and the blurring of distinctions between "private life" and "public life". This results in a new aspect – the "public private life" which arises from both societal needs and the confluence of information technologies. In this context, regarding genetic information, the authors raise the issues of dataveillance, unintended secondary uses, and the value of this data in the information economy.

The second section explores the challenges to the "private life" of identification via genetic technology. DNA information that people leave behind – for example, cells left on a seat at an airport – may be trotted off to China by another passenger while the remainder of our cells move towards Toronto. This dilution of self – in which our detachable DNA information could end up in numerous disparate databases without our knowledge – can also lead to the penal justice system storing, examining and comparing DNA samples, with unique privacy rights implications.

The third section is a description of the methodology used to collect and analyze the data that is the subject of section four. The authors attempted to map the justice system's use of DNA to identify the sequence of collection of DNA evidence in criminal investigations, the key actors in its collection and use in police forces and police labs. They also provide an overview of standards in place and the types of information collected from DNA evidence and how it is used (the data trajectory). The authors conducted eight interviews, ranging from one to three hours, with representatives of two police forces and the National DNA Data Bank, along with a review of relevant documentation.

The fourth section is an extremely detailed and revealing description of the trajectory that DNA will take in a criminal investigation, from the moment a sample is collected at the scene of a crime to its inclusion in one of the two registries of the national DNA database. The authors describe ten discrete stages that break down into two categories. The first category is comprised of the six stages that lead from collecting genetic substance to establishing an individual's identity. The second category includes the four stages leading to an incriminating proof or the "criminal identity". In describing the various stages, the authors raise the possible social and legal ramifications for privacy. The authors point out that DNA can have significant impact on the "private life" of individuals when it can be linked directly to them, or used to profile likely suspects in a crime, or used for bio-monitoring or predictive purposes.

In section 5, the authors present some conclusions, including the view that the creation of a "penal identity" through DNA collection in a crime investigation changes the paradigm of the "private life" and subjects the individual to a new relationship with the criminal justice system in which his actions and the presence of his DNA must be explained. In this milieu, a subject's right to silence is diminished, the burden of proof that he is not a suspect shifts to the individual, and a "tunnel vision" approach to use of DNA evidence may affect his legal rights. This, in sum, marks a whole reorganization of penal justice which challenges our liberal notions of the "private life".

Report available at: <http://www.saea.uottawa.ca/index.php?lang=fr>

Student number: ADN2007; password: ADN2007

## **Can ID? Visions for Canada's Identity Policy: Understanding Identity Policy and Policy Alternatives**

*University of Toronto Faculty of Information Studies and London School of Economics and Political Science, April 2007, 114 pages*

Krista Boa, Andrew Clement, Simon Davies and Gus Hosein

This report maps, analyzes and makes recommendations concerning the current identity policy landscape in Canada, particularly in the context of the U.S. REALID proposal, the Smart Border Agreement, and plans for the Western Hemisphere Travel Initiative. The report also looks at plans for drivers' licences and identity documentation in several Canadian provinces. The report draws upon experiences in other countries and a review of leading cases of identity scheme development in Canada, as well as the results of two research workshops conducted with government officials, academics, civil society organizations and private sector firms.

The ensuing report looks first at the dynamics of identity policy, examining a number of important policy factors. These include the political risks, including the risk of how identity cards in particular can alter the relationship between the citizen and the state and create a source of tension. The authors note that privacy "may yet produce the largest political risk in the Canadian context". Looking next at the drivers for such policies, the authors warn that the driving principles for an identity scheme could shift in midcourse, further raising the political risks. The report also considers the challenges of building an identity scheme that matches stated goals and objectives within realistic timelines and with reasonable technologies, describing the difficulties of doing so in other jurisdictions. The effectiveness of policy choices and the costs of such systems are described at length, and the authors consider the questions of who ultimately pays for such costs, who decides the policy and who "owns the system". In Canada, the report points out, a predominant concern is whether a new policy is "owned" by the federal government or the provinces.

The authors next consider the benefits of a national policy framework, stating that, while establishment of a national identity assurance infrastructure may prove highly beneficial (especially to the needs of business), policy leadership is required to cultivate and nurture identity assurance across the Canadian economy. Looking at recent examples from Sweden, Hong Kong and Malaysia, the authors conclude there are many benefits to beginning a national discussion on the need for effective identity strategies across Canada, but that a centralized solution decided by government may not actually produce these benefits. They stress that more work at the ground level is required, within organizational, commercial, and consumer and citizen-facing environments.

In their analysis, the authors outline the bad public policy risks of vendor-driven choices or adopting "neat technologies" such as biometrics without open and careful dialogue, and express alarm at the lack of clarity and transparency on Canadian identity policies. They outline criteria necessary for strong public consultation, as well as propose several sets of principles and tests to guide such an effort. They conclude that it is feasible to build national identity schemes that simultaneously address the legitimate security and data sharing interests of government and the legitimate privacy and autonomy interests of citizens. The report also summarizes findings from two workshops held in Vancouver and Ottawa where approximately 50 individuals participated, and which included a robust discussion of privacy concerns, and whether any scheme should involve mandatory or voluntary (opt-in) use of identity services. In addition, it includes a detailed discussion of provincial, federal and international identity initiatives in recent years, including recent Canada-U.S. border security initiatives.

Report available at: <http://www3.fis.utoronto.ca/research/iprp/>