the democratic Commitment

JOURNAL OF THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION NOVEMBER 2006 / VOLUME 40 NUMBER 3

fighting for freedom since 1962

INSIDE

Focus on Privacy & Access Issues

THE LAW FOUNDATION OF BRITISH COLUMBIA

The BCCLA acknowledges the generous support of the Law Foundation of BC

WE CAN HANDLE THE TRUTH

Campaign for Open Government and the *Access Denied* Report

THE BCCLA IS PART OF A BROAD-BASED coalition that has launched a campaign for open government. The campaign is focused on improving the Province's record on Freedom of Information (FOI) requests.

The Campaign is calling for the government to implement its own Special Committee's recommendations to improve FOI and to address a culture of governmental secrecy.

The BCCLA advocates for a strong access to information culture to provide a real safeguard against governments using their vast resources of information selectively to shape public opinion to serve its own purposes and not those of citizens. Freedom of information is fundamental to democracy.

The Campaign for Open Government was launched with the release of a report titled *ACCESS DENIED: An analysis of the B.C. Government's response to freedom of information requests, 2000-2005*. The report is an analysis of data from the Province's Corporate Requests Tracking System (CRTS) which is used to track information requests from the public and flag requests that are considered politically sensitive. The following excerpts are from the report: An analysis of CRTS data provided to the Freedom of Information and Privacy Association by the B.C. government suggests many shortcomings in the administration of the *Freedom of Information and Protection of Privacy Act*. Results indicate that response times for information requests are often in excess of legal timelines; that the CRTS is used to flag the requests of particular user groups, based on political sensitivity; that these distinctions can lead to longer response times; and that this discrimination affects the outcomes of requests.

Public use of the Act has declined over a five-year period, in particular requests made by individual users.

continued on page 3

TO THE CONVERTED / A message from our president Jason Gratl

"Marshall Macluhan said that in the sixteenth century the printing press created "La Publique". In his tradition, I have three disorganized and speculative thoughts about the recent cultural implications of the internet.

...the first implication is to a deepening sense of humour. We live an age of political parody – what happens when the chasm between public communication and reality is wide and deep. Prominent government and corporate messaging is ripe for reduction to absurdity: the rise within the mainstream of Stephen Colbert and South Park and mockumentaries in the past two or three years is a symptom of these faultlines.

A good laugh fills the lungs of a skeptical democracy. And laughter will drive absurdity to the wings.

The second implication is a thinning of the veneer of human civility. Contributions to the web can be made anonymously, in persona, in another's name, as a collective – all modes of expression involving limited personal accountability and limited social restraint. The lack of restraint has lifted the sluice on expressions of racism, sexism, homophobia, religious and ideological fanaticism, anti-social desires and generalized misanthropy.

There are those who would sanitize the internet against hate speech and other improprieties. These enthusiasts, though often well-meaning, operate with the mistaken premise that anonymous anti-social speech is virulent. In fact, anonymous speech is of attenuated persuasive force. And when more ambitious anonymous voices attempt to meet each other in person to plot the ascension of chaos and disorder, they will, I suspect, quickly find themselves in the company of at least one anonymous undercover investigator. In any event, we should acknowledge the internet as a very good place for people who write only in all-caps.

The third implication is the creation of a private refuge for contemplation and personal development. Like Borges' Library of Babel, almost every page of every book ever written is within reach of our cubicle. We can read, watch and listen to almost anything, or add something of ourselves to the soft white glow. The concatenation of this private give and take is our best representation of a new collective free mind. This space is worth protecting.

In this vein, it is of concern that the Ministry of Public Safety is working to pass the *Modernization of Investigative Techniques Act* which would allow the government to obtain IP addresses on demand from service providers. It is worrying that service providers are so gently accommodating. South of the border there is a battle for control over the flow of internet traffic. The trouble on the horizon is that industry consolidation may permit hardware owners to distort unfettered access to obtain political and economic leverage.

As this issue of the *Democratic Commitment* makes clear, the BCCLA is committed to the difficult task of monitoring and ameliorating the interface between technology and civil liberties. We are committed to equality of access, non-censorship, and internet privacy. I thank all the volunteers and staff who contribute to this ongoing effort (especially the contributors to this issue) and I urge our readers to support our Association to allow this work to continue.

The main reason for this decline is growing disenchantment of FOI requesters with a process that is increasingly fraught with government resistance, evasion and delay.

Cutbacks to the [Office of the Information and Privacy Commissioner] are all the more troubling in light of recent increases by the B.C. government on expenditures for paid advertising. This type of illustration is often used by advocates of freedom of information to contrast what a government spends to get its favoured message out, versus what it spends to give citizens the specific information they request under FOI.

In February of 2006, the annual provincial budget included an allocation of $21.8 million for government advertising. This represents a funding increase of over 100% over the previous year, including increased advertising spending for frontline ministries that have been the subject of recent scandals.

Reliable figures dealing with the costs of administrating FOI in BC are not readily available. However there are some interesting comparisons which can be made. For instance, the Public Affairs Bureau of the B.C. government now employs 216 staff – up from 2002 in the previous year. This figure is over 12 times the number of staff employed by OIPC.

To access the full report: www.opengovernment.ca

PRIVACY AND PENSION TRIBUNAL DECISIONS

In the old days, privacy was protected almost inadvertently. Before personal information was stored electronically, posted on the Internet and databases linked, disclosures of personal information were apt to be somewhat contained. No more. In this context the Association has responded to a complaint about the amount of personal information made publicly available in the published decisions of the Canada Pensions Appeal Board, which are widely available to anyone with an Internet connection.

We are urging the Pension Appeals Board to reconsider its policy about what nominal information should be published and released in these decisions. We are concerned about the vast amount of extremely personal and confidential information of appellants that is disclosed in a published appeal decision and that these disclosures can be a disincentive for someone to launch an appeal.

There is a tension in this issue. Like other judicial or tribunal decisions, we need openness and transparency and the release of decisions is obviously a key aspect of that.

However, our position is that these objectives can be achieved along side upheld privacy rights by simply removing the names of the appellants from the postings and keeping the substantive reasoning for the decisions. We are looking forward to following up our written submission on this issue with the new Chair of the Pension Appeals Board sometime in the new year.

fighting for freedoms since 1962

British Columbia Civil Liberties Association
550 – 1188 West Georgia Street
Vancouver, British Columbia
Canada V6E 4A2
Tel: 604.687.2919
E-mail: info@ bccla.org
Web: www.bccla.org

The Democratic Commitment is a publication of the British Columbia Civil Liberties Association. The Association was established in 1962, and is the oldest continuously active civil liberties association in Canada. It's mandate is to preserve, defend, maintain, and extend civil liberties and human rights in British Columbia across Canada through public education, complainant assistance, law reform and litigations.

Publications mail agreement 40045354

Post 9/11
Traveling to the U.S. Is Not Easy

by Richard S. Rosenberg

VISITING THE UNITED STATES IS BECOMING INCREASINGLY DIFFICULT AS IDENTIFICATION REQUIREMENTS FOR FOREIGNERS ARE BEING RAMPED UP.

Three areas of particular interest are documents necessary to enter the U.S. and their relation to the possible introduction of National ID cards in Canada; the status of the Canadian no-fly list and its overall effectiveness, and finally, the problems associated with the sharing of information about airline passengers, from the European Union, with the U.S.

Terrorist threats, and of course actions, have led to a series of preventative procedures at the world's airports and on the world's airlines, particularly those based in the U.S. The U.S. government has been warning Canadians that very soon they would require new border identification to enter the U.S. It was feared that Canadians would need a passport, or equivalent, to cross their rather long border into the U.S. American merchants at the populous border crossings worried about the impact of reduced Canadian traffic because of the high cost of passports. After much negotiation, a somewhat reduced biometric-based document was agreed upon and initially scheduled for implementation in 2008. Subsequently, this date was extended to mid-2009 because of concerns by the Canadian government about the difficulty of meeting given technical specifications.

In Canada, early debate turned upon whether or not a new form of identification, a National ID card, would satisfy border requirements as well as internal Canadian security needs. The federal Standing Committee on Citizenship and Immigration held hearings during February of 2003. On November 22, 2002, the then Immigration Minister, Denis Coderre, made the following remarks: (CBC, 2002)

"Let's have a national debate for policy-making purposes. Do Canadian people feel that we should have a national ID card?"… Coderre said the card would be based on the Maple Leaf card now issued to landed immigrants in Canada. The Maple Leaf cards contain biometric information such as fingerprints. He said the cards would make it easier for Canadians to travel, especially to the U.S.

It is interesting to note that even after the events of September 11, 2001, the U.S. has not opted for a National ID card, probably because of the general antipathy of most Americans towards the idea of being required to carry so-called "papers," for identification. As a vice-president of the Electronic Frontier Canada, I made a presentation to the federal Standing Committee on Citizenship and Immigration, on February 19, 2003 in Vancouver. The following is a representative comment: (Rosenberg, 2003)

It is inevitable that in the aftermath of crises such as September 11, concern for the security of the nation will (seem to) overweigh individual privacy rights. This government has introduced a number of bills that raise serious privacy issues and in the context of such legislation as well as the Canada Customs and Revenue Agency (CCRA) database on foreign travel activities and the Lawful Access Discussion Paper, the current proposal for an ID card strikes many that the government is clearly over-reacting.

Another action taken by the Canadian government (as well as the U.S.), in 2002, as part of its anti-terrorism response was the no-fly list, a collection of individuals deemed to be threats, whose access to airplanes was restricted. How this list was compiled is unknown as is the means by which one can have one's name removed. Transport Canada officials say that "they plan to incorporate an appeals process so that passengers blacklisted by mistake can get their names removed from the list." (Salot and Freeze, 2006) Furthermore, for any flights from Canada to or over the U.S., Canadian airlines must check all passenger names against the American no-fly list.

As part of its attempt to deal with international terrorism, the U.S. government required "all airlines flying to the United States to share passenger data, such as name, address and credit card information, with Customs and Border Protection." (Nakashima, 2006) The European government agreed to this requirement even though it violated the privacy protection guaranteed individuals in the European Union under the *Data Protection Act* of 1995. In May of this year, the European Court of Justice, "annulled the deal on a technicality but gave the E.U. and the United States Sept 30, 2006 to replace it" (Nakashima, 2006). One more quotation describes the scope of this post 9/11 agreement:

> Under the post-Sept. 11 data-sharing agreement, Europe allowed the United States to keep the data for up to 3 1/2 years, but the United States wants to be able to hold onto the information longer. Europe also allowed the United States to share the data, part of a database called the Passenger Name Record, with other U.S. counter-terror agencies on a restricted, case-by-case basis. The United States wants to be able to share the data more liberally.

So the deadline has been passed and no solution is on the horizon but the U.S. government maintains its right to take serious steps if the desired data is not turned over as a matter of course.

One can expect more lists, more delays, more hassles as new lists are developed and applied in ways that defeat reason and empower bureaucrats and law enforcement officials.

Richard Rosenberg is Chair of BCCLA's Privacy and Access Committee and has been a member of BCCLA's Board of Directors for the past year.

Richard is a Professor Emeritus of computer science at the University of B.C. As personal computers became a reality, he became interested in how computers could be programmed to interpret and use natural language commands. However, rather than placing all of his attention on semantics and mathematics, as some computer scientists may be inclined to do, his research explores the social impacts of computing.

In fact, Richard's most recent book, *The Social Impact of Computers*, addresses these concerns. In particular, he notes that we "need to give some thought to the impact of technology down the road and really think about the good but also the bad." For example, the internet is typically viewed in a positive light because it facilitates access to

vast amounts of information; but, it also creates new problems. When individuals access websites, the potential to leave a trail of identifiable information is huge. "The privacy implications [of the internet] are out of control"; and there are few legislative protections for privacy while on the internet. In many jurisdictions outside of Canada internet privacy policies are voluntary and should be considered little more than a goodwill gesture. Oftentimes, there is nothing stopping these websites from using or misusing your personal information.

In addition to privacy concerns, computers and the internet have created a new environment for freedom of speech restrictions as governments lobby service providers to restrict content or log private information. File sharing and music downloading have created questions about intellectual privacy rights on an international scale.

Richard is active in community organizations that share a belief in the importance of social responsibility. He is the president of not one, but two groups: the Freedom of Information and Privacy Association (FIPA), which complements the privacy work of the BCCLA, and the Vancouver Peretz Institute, which promotes Jewish culture in Vancouver. He is also a member of the board of the Vancouver Community Network, a non-profit organization specializing in free web hosting and computer education.

Arar Vindicated

Government Pressured to Implement Inquiry's Recommendations

On September 18, 2006, Justice Dennis O'Connor, Commissioner of the Arar Inquiry released his interim report into the actions of Canadian officials in relation to Maher Arar. Mr. Arar is the Syrian-born Canadian who was captured by U.S. authorities when in transit through a New York airport and sent to Syria where he was subsequently tortured.

The Inquiry found Mr. Arar completely innocent of ties to terrorist organizations. Instead, the Inquiry found considerable fault with the conduct of the RCMP and other government agencies that contributed to Mr. Arar's rendition to torture in Syria.

The former Liberal federal government established the Arar Commission of Inquiry in February 2005 to investigate and report on the detention, deportation, torture and return to Canada of Mr. Arar as well as give policy advice to government on the best mechanism for accountability of Canada's national security agencies.

The Inquiry's voluminous account of the actions of Canadian officials in relation to Mr. Arar includes a 376 page report with findings and recommendations as well as two large volumes of Factual Background some of which has been excerpted due to national security confidentiality claims of government. The BCCLA has been very critical of the government's expansive claims to confidentiality on national security grounds. The Arar Commission expects to have to go to court to force the government to release further details.

The BCCLA has been significantly involved in the Arar case. After Mr. Arar's return to Canada in October 2003, the BCCLA was a prominent voice in calling for a public inquiry into the matter. The Association purchased ad space in the Globe and Mail to write an open letter to then Prime Minister Paul Martin in December 2003 and held a rally for Mr. Arar in early 2004. The BCCLA has been an Intervenor in both the Factual Inquiry and the Policy Review. Since the release of the report, the Association has been outspoken in the media calling for the government to agree to implement the Inquiry's recommendations.

The Inquiry is expected to release its report on recommendations for an independent civilian review agency for the RCMP's national security activities very soon.

The BCCLA's efforts are now focused on meeting with the government and opposition to press for a speedy implementation of the Inquiry's recommendations. We encourage anyone who would like to advocate for the speedy implementation of the Inquiry's recommendations to email:

The Right Honourable Stephen Harper, Prime Minister of Canada (pm@pm.gc.ca)

The Honourable Stockwell Day, Minister for Public Safety (day.s@parl.gc.ca)

The Honourable Vic Toews, Minister of Justice (toews.v@parl.gc.ca).

The Inquiry report can be viewed at http://www.ararcommission.ca/eng/26.htm

Some of the Inquiry's conclusions:

- The RCMP provided inaccurate and misleading information to American authorities without warnings about the appropriate use of such information. This misinformation indicated that Mr. Arar was suspected of being linked to the Al Qaeda terrorist group although the RCMP had no factual basis for this assertion.

- It is very likely that, in making the decisions to detain and remove Mr. Arar, American authorities relied on information provided by the RCMP.

- The Department of Foreign Affairs and International Trade sent the RCMP and CSIS information about Mr. Arar confessing to terrorist involvement without informing them

that the confession was likely extracted under torture.

- The RCMP failed to cooperate in an earlier effort at a joint letter to reassure Syrian authorities that Mr. Arar was not considered a terrorist risk.

- The RCMP did nothing to set the record straight regarding the allegations of Al Quaeda membership that continued to dog Mr. Arar when he was returned to Canada.

- The RCMP were not forthright in briefing Canadian officials about Mr. Arar and suppressed important details favourable to Mr. Arar.

Some of the Inquiry's recommendations:

- The RCMP must only share information after appropriate screening for relevance, reliability and accuracy and with the inclusion of appropriate caveats.

- There must be an appropriate and independent civilian body to review the national security activities of the RCMP.

- There must be appropriate training of the RCMP and other agencies regarding profiling of Muslim and Arab communities and citizens.

- The Government of Canada should register a formal objection with the United States and Syria regarding the treatment of Maher Arar.

- The Government of Canada should assess Mr. Arar's claims for compensation and respond accordingly.

BCCLA Spearheads Prevention of Torture Act

After the Arar Inquiry's first report, the same questions were on everyone's minds: how could we let this happen? And how can we prevent it from happening again?

The vast majority of Canadians are steadfastly opposed to torture. What the Arar Inquiry revealed was that in order to bring the actions of our government officials into line with this widely-held belief, we need to renew and reinforce Canada's legal commitment to preventing torture.

In response to this need, the BCCLA has drafted a Bill called the *Prevention of Torture Act*. If passed tomorrow, the legislation would be the first of its kind in the world. If passed five years ago, the legislation could have prevented the torture of Mahar Arar and others.

You can find a link to the latest version of the draft Bill on the front page of our website (www.bcccla.org). Here are some highlights of what this legislation would do if enacted:

1. make it a criminal offence to use information known to be derived from torture,
2. prohibit Canadian officials, including the Armed Forces, from handing over prisoners to be tortured at home or abroad,
3. create a government watchlist of countries which are known to engage in torture and providing for those countries to be treated accordingly when it comes to information sharing, deportation, and extradition from Canada,
4. make sure that information sharing with foreign governments includes clear communication of Canada's stance against the use of torture, and
5. establish diplomatic protocols to bring home any Canadian citizen at risk of torture abroad, without undermining our ability to investigate and prosecute those citizens at home under our laws, free of torture.

National and international non-governmental organizations, such as the Association for the Prevention of Torture and the Canadian Arab Federation, have already endorsed the Bill. In Ottawa, the BCCLA's lobbying efforts appear to have the support of the majority of members of the Public Safety Committee. This support may result in the Bill being introduced into Parliament.

WHAT CAN I DO TO HELP?

Send an e-mail to The Honourable Stockwell Day, Minister for Public Safety and Emergency Preparedness, at this address: day.s@parl.gc.ca; and to the Prime Minister's Office: pm@pm.gc.ca; urging them to support the BCCLA Prevention of Torture Act. Include these links to the draft and backgrounder: www.bccla.org/tortureact.pdf and www.bccla.org/tortureactbackgrounder.pdf. Finally, cc your email to christina@bccla.org so we can send you our thanks.

Confidentiality
...at the Crossroads

The BCCLA is very concerned about the state of patients' rights and medical privacy as the government moves quickly to bring in a system of electronic medical records ("eHealth strategies").

On August 1st 2006, the B.C. Persons With AIDS Society released a report analyzing the potential effects of the new eHealth strategies agreed to by the B.C. government and the B.C. Medical Association. In that report, the Society notes that there are significant problems with the proposed system of electronic health records, from the threatening of the 'full-disclosure' relationship between doctors and patients, to turning 'knowledge' about individuals into 'data' about individuals, to a great potential for abuse due to a lack of consultation with one of the most interested parties: the patient. The following is an excerpt from that report:

On March 11, 2006, it was announced that the B.C. Medical Association and the provincial Government had reached an Agreement for physician compensation and related matters for the period April 1, 2006 through March 31, 2012. Ratification of this Agreement by the BCMA's membership was announced on May 4, 2006.

The March 11 BCMA news release announcing the Agreement noted it "provides funding for the use of information technology in the delivery of care by physicians." The May 4 news release issued jointly by the BCMA and the provincial ministries of Finance and Health noted the ratified Agreement would provide "more resources to support full service family practice," and that "the BCMA elected to reinvest part of the incentive into information technology to enhance patient care." Fairly innocuous stuff. The references cited are apparently the only public notice given of the provisions of the Agreement's "Schedule C", the provisions governing the new IT initiatives.

Why is this important? As noted on page 23 of eHealth Strategic Framework, "Within 10 years of eHealth implementation, the majority of patient health information is expected to be maintained in a standardized, shareable electronic form. This will include medication histories, immunization records, laboratory test results, and other relevant patient information. The full patient record or a suitable subset will be easily transmitted to authorized care providers in other locations, and the results of specialist consultations will be electronically transmitted back to the primary care physician."

Further, through the implementation of the envisaged "Interoperable Electronic Health Record" (iHER), patients' hospital, home care, public health, laboratory, pharmacy and diagnostic imaging records will all be incorporated into one grand electronic record that can be viewed by any of the broad health care system's various operatives – all of it done over the internet, and all of it stored in facilities and by organizations completely independent of the individual patient's doctors' offices.

Finally, one small additional element of the whole eHealth project is a public health initiative that would, in unspecified ways, use the eHealth system (including the EHR) to develop "a client and population-centred information system to improve access, delivery and integration of health care services for managing communicable diseases." Among the benefits anticipated are "Enhanced ability to recognize and manage potential communicable disease outbreaks" and "Faster response to public health issues".

With the exception of the document's section "Safeguard Privacy and Security"... you will search through eHealth Strategic Framework in vain for a discussion of health care consumers' legitimate concerns for the maintenance of doctor/patient confidentiality in particular, and for the overall confidentiality of their health care records in general.

The Two Problems

1 According to B.C.'s Information and Privacy Commissioner's website, the [*Freedom of Information and Protection of Privacy Act* (FOIPPA)] provides that any person may request access to records held by public bodies (including records of their own personal information) and may request the correction of their personal information, including their own personal information in records held by public bodies.

This at least ensures that individuals should be able to have access to their own EMRs and EHRs (although this has not been tested), and be able to secure corrections to incorrect information contained in them.

But it doesn't guarantee – indeed, it is has nothing to do with – physician-generated EMRs being "uploaded" to central servers, and with core data sets being extracted from those EMRs, for access and use by a host of players throughout the health care system. (This is because, as far as the FOIPPA is concerned, all of this information is collected legitimately for the purpose of giving the individual concerned timely access to appropriate health care. All of the envisaged uses are consistent with the reasons for which the information was collected originally. Indeed, substantial elements of the core data set are already "in the system", having been collected by BCMSP or FairPharmacare, among other players.)

This leaves individual health care consumers with one defence: withholding consent at the source. At any time you are free to decline to provide any information requested by your physician or to ask that any particular element of your record in your doctor's office be expunged.

But imagine for a moment the consequences of declining to give your doctor various aspects of your personal and personal health information. It could defeat the whole purpose of consulting a physician. Indeed, this operational requirement for "full disclosure" is what lies at the heart of the time-honoured doctrine of doctor/patient confidentiality. It is widely recognized – including at law – that doctors secure information from their patients for vital medical and related purposes, and that such information ought not to be divulged to anyone else for any other purpose, ever. If such complete and dependable confidentiality were not dependable, it could have an intolerable "chilling" effect on the doctor/patient relationship, causing the withholding of occasionally crucial information and so reducing seriously the very effectiveness of that relationship. Further, access to sensitive but filtered-and-organized information by others in addition to the doctor who originally secured that information necessarily deprives those others of the context in which that information was supplied. That kind of knowledge and understanding can only come from a long-term relationship between patient and physician. As one physician deeply alarmed by and opposed to the current development of the EHR system in B.C. has put it, "Having all the information about a patient is not the same things as knowing all the information, and neither is the same thing as knowing the patient."

It is widely recognized – including at law – that doctors secure information from their patients for vital medical and related purposes, and that such information ought not to be divulged to anyone else for any other purpose, ever.

2 There is another problem that has run like a ghost through the entire evolution of the EHR paradigm. Throughout all of this planning and movement towards implementation, "patients" (aka "clients" and "consumers") are viewed simply as occasional seekers of generalized low- to mid-level health and medical information at best, and as passive suppliers of information with no other legitimate interest in the eHealth system's activities at worst. The concept that patients might have a legitimate – indeed, a vital – interest in the design and functions of the eHealth system seems never to have occurred to its proponents and architects.

No one would argue that the potential benefits of such a system as that envisaged in the overall eHealth package could be substantial. But – as AIDS activists will recognize better than most – the scope for error, abuse, and accidental or deliberate unauthorized disclosure of personal information is enormous. Given such alarming potential for harm, it is absolutely imperative that individual and organized health care consumers be decisively involved in the development of the system and remain in control of their personal sets of information.

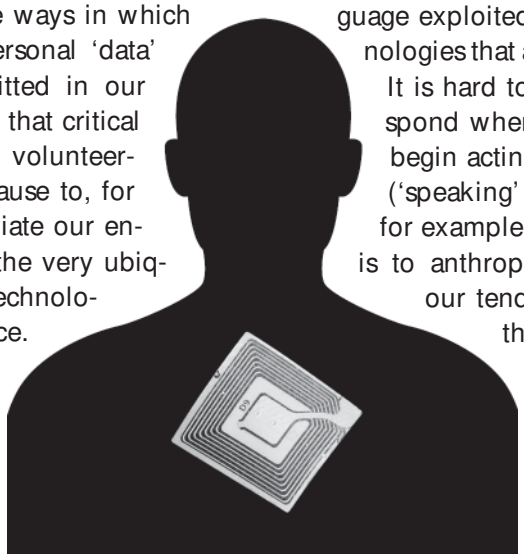
RFID and Intelligent Objects
A Limited Case Study

Vance Lockton and Wendy Foster, Ph.D.

For the vast majority of Canadians, surveillance technologies exist in one of two conceptual realms: that of dystopic science fiction or, perhaps more uneasily, as naturalized elements of our everyday. So inured are we to the ways in which our activities, movements and personal 'data' are collected, stored and transmitted in our routine negotiations with daily life that critical reflection upon our 'rights-release' volunteerism is rarely engaged. If we do pause to, for a minute, denaturalize and unmediate our environments, we are paralyzed by the very ubiquity that works to render 'smart' technologies invisible in the very first place.

In this article, we focus our discussion on Radio Frequency Identification (RFID). RFID, as a pervasive tool in the burgeoning surveillance application industry, is rarely popularly registered as such. Many do not consider that identifying data is collected each time an RFID-enabled key fob is used to open an office door, or in the instance that an EZ-Pass style RFID payment system is employed on toll roads or at gas stations. Further, the deployment of RFID is forecasted to increase proportionally to the decline in cost of tag technology to cent and sub-cent levels. (PolyIC, a venture founded in part by conglomerate Siemens, hopes to create 1.3 cent chips by 2008 through the conversion of tags from silicon to printed plastics.)

Contemporary objections to the introduction and proliferation of RFID-enabled technologies has centered on hypothetical formulations of privacy-invasive scenarios, which, although valuable considerations, suffer from an elevated abstraction. What is required, as a corollary, is a critical approach anchored in present issues associated with current and pre-deployment RFID, such as an industry romance with the metaphorization and marketing of RFID as an 'intelligent' attribute of the objects to which they are attached. As 'signifying' animals, we are particularly vulnerable to the powerful, metaphorical language exploited to describe and normalize technologies that are introduced into our daily lives. It is hard to predict how individuals will respond when the objects that surround them begin acting in ways that seem autonomous ('speaking' to each other via radio waves, for example). One common reaction, though, is to anthropomorphize the object – that is, our tendency, when the workings of the things around us are unclear, is to see the world as alive, with human characteristics that bring the unknown into alignment with the known, ourselves. Mike Kuniavsky of Adaptive Path states that "In its broadest definition, animism is the belief that all objects have will, intelligence and memory and that they interact with and affect our lives in a deliberate, intelligent and (in a sense) conscious way." [1] With RFID as our example, we see that when a tag is applied to an object, an animistic process takes place wherein the object is now referred to as 'smart' (for instance, in the case of smart cards, or smart passports), has memory, and is believed to be interactive with its environment. The object is now an agentic subject, and as such, it not only becomes a much more valuable commodity, but the rules of ethics can now be seen apply to it. It seems intuitive that it is much easier to change or limit a potentially privacy-invasive 'communication protocol' than a privacy-invasive 'intelligent-object,' which is accorded a higher 'value' by both the producer and the consumer of the technology.



Radio Frequency IDentification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is an object that can be attached to or incorporated into a product, animal, or person for the purpose of identification using radio waves. Chip-based RFID tags contain silicon chips and antennas. Passive tags require no internal power source, whereas active tags require a power source.

Why engage in such a debate? Isn't 'data', after all, meaningless in and of itself? For all intents and purposes, 'data' is merely a string of symbols, unencumbered by the nefarious transformation into organized information, and the subsequent and more dangerous identity of interpreted knowledge. The 'data' of our existences, as it resides in closed circuit video archives, as visit traces logged by tracker cookies on the Internet, or as readable bits and bytes on the microchip systems that found smartcard technologies, is, by virtue of its specialized abstraction, more comfortably absorbed into the realm of the non-critical – as unexamined as the microwave and the television

We bother because the attribution of the 'human' onto the 'technology' involves the problem of agency. This in turn has powerful implications for the laws that govern and regulate behaviours and legal subjects, as well as for the ways in which we position ourselves in relation to our technologies more generally. An agent, by definition, effects its environment, it enacts a change upon its real context; it is the subject of its world. When we produce technologies that profoundly interact with and alter environments (such as 'smart shelves', which register not only their inventory states but record and transmit customer behaviours), we need to begin to understand, perhaps differently, the ethical imperatives attached to such intelligences. When our objects become 'smart,' when our technologies become 'facilitators,' and the 'human,' within this developing and novel relationship, becomes increasingly marginalized – reduced to a mere operator of a privileged interpretive device – we are then required to consider the consequences that such a reduction might produce economically, socially, and culturally.

1] http://adaptivepath.org/publications/essays/archives/000272.php

Membership has its perks!

Join the BCCLA today and become a part of an organization that is actively involved in bettering your community and making it safer for you, your friends and family. If you are not already a member, please sign up today. With your membership you will receive the following benefits:

- *Civil Liberties Update* – our popular monthly e-newsletter
- *The Democratic Commitment* – newsletter published three times a year, which includes our Annual Report
- Invitations to events throughout the year, such as our lecture hosting Chief Justice Beverly McLachlin, Stephen Ward, Associate Professor of Journalist Ethics of UBC School of Journalism or his Excellency John Ralston Saul.
- Invitation to and voting rights at our AGM in March

Sign up online at www.bccla.org or call Lil Woywitka, our Membership Secretary at 604-687-2919 or email lil@bccla.org and join today!

How *you* can have an impact on civil liberties from the comfort of your own home...

Hosting a Third Party Event is how! Having friends over for dinner or planning to throw a party?Include the BCCLA in your plans. Donations don't always have to come from you alone.

Think about having some friends over for dinner and ask them for a donation to support the BCCLA. Include a short speech outlining the importance of the Association so your friends and family can become informed. We are always happy to provide materials and speaking notes.

You can hold an annual event such as a golf or darts tournament and make the BCCLA your charity of choice. Instead of collecting a registration fee, ask that a portion go to support the BCCLA and our important work.

Even if it's just having friends over for a cup of coffee, you can make a difference. Simply send a cheque of the proceeds made payable to the B.C. Civil Liberties Association and record any names and addresses of those wishing to be tax receipted.

We would also appreciate it if you could include your story. Tell us the creative and special way you raised the funds so that we can put it on our website and in our upcoming newsletters.

With your help and donations, making a gift to the Association ensures that together we are keeping our communities safe and secure from abuses of our rights.

For more information and options on holding a Third Party Event to benefit the B.C. Civil Liberties Association please contact Sarah Frew, Director of Development at 604-687-2919 or email sarah@bccla.org.

Helping the BCCLA help the Community!

Our greatest challenge is not the cases we work on but funding our increased work demand. Please consider making a monthly gift to the BCCLA. It is a hassle free way to support the Association and help us plan ahead.

Are you interested in making a planned gift to the Association?With the Federal Government's announcement of the elimination of capital gains tax on gifts of securities this is fast becoming a popular option for donors across the country. It is a gift that gives to both the Association and to your estate. For more information please contact Sarah Frew, Director of Development at 604-687-2919.

UNITED WAY DONATIONS

United Way of the Lower Mainland

Don't forget that you can designate the BCCLA as a specific recipient of your United Way donation!

The B.C. Civil Liberties Association wishes to thank the Law Foundation of B.C. and our other funders for their financial support.

The Law Foundation of British Columbia · Vancouver Foundation · VBA Vancouver Bar Association · British Columbia · BC Gaming Policy and Enforcement Branch of the Ministry of Public Safety and Solicitor General