FIPA
BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

FIPA Newsletter of the BC Freedom of Information and Privacy Association

BULLETIN

DECEMBER 2012
FIPA.BC.CA

THIS EDITION: YEAR IN REVIEW, UNIVERSITY SUBSIDIARIES, LICENSE PLATE SCANNERS + MORE

BIG WINS, NEW CHALLENGES:

2012 IN TRANSPARENCY

In B.C. and across Canada, the past twelve months have seen information rights making headlines on a regular basis. And usually not in a good way.

At the B.C. Freedom of Information and Privacy Association, much of our year was spent (once again) in sparring matches with the provincial government over access, transparency, and privacy issues. At the top of the list was finally winning the long-delayed release of the government's full $300-million Workplace Services Agreement with IBM, held back for eight years by stall tactics and failed legal challenges (all charged to the B.C. taxpayer, by the way). Credit, however, is due to the government for finally obeying the order of the B.C. Supreme Court and releasing a full, un-redacted copy of the contract.

The disclosure was a major victory for FIPA, but more importantly, for the people of British Columbia. The Court's decision, and the government's response to it, establishes a new standard for transparency around government contracting and will hopefully lead to more proactive disclosure of documents pertaining to the disbursement of public funds. Of course, we're still waiting to see just how the government will make much such records available, but the precedent has been set.

But while the release of the IBM contract was a long overdue step forward for the government, they also took some major steps backward. For example, in the last week of the spring sitting of the legislature (which would turn out to be the last sitting of the year), the government jammed some seriously damaging amendments to information and privacy law into four pieces of otherwise innocuous legislation. These bills dealt with generic drug pricing, animal disease outbreaks, medical first responders, and coastal ferries administration, not information and privacy rights.

> In the last week of the spring sitting othe legislature...the government jammed some **SERIOUSLY DAMAGING AMENDMENTS** to information and privacy law into four pieces of otherwise innoculous legislation

Despite an unprecedented four letters from Information and Privacy Commissioner Elizabeth Denham, each strongly criticizing the bills, they went ahead all the same, putting huge amounts of public information under the lock and key of ministerial and cabinet secrecy, and opening sensitive personal data to new threats. FIPA wrote to Premier Christy Clark, protesting this piecemeal repeal of the *Freedom of Information and Protection of Privacy Act*. The response, sent by then Minister of Citizen Services, Labour, and Open Government Margaret MacDiarmid, did little more than offer talking points.

To these access rollbacks, the government also added a couple of privacy horror shows. First came the disastrous rollout of the leaky, dysfunctional Integrated Case Management system, and then the mysterious data breach at the Ministry of Health. At least the government's plans to introduce a poorly-documented province wide ID card were put on hold because of a labour dispute at ICBC. Will the BC Liberals risk the data disaster trifecta by bringing it in just before the provincial election?

We also found ourselves in the midst of a couple of other troubling issues, which are now under investigation by the Information and Privacy Commissioner. First, we complained about the fact that about two thirds of completed FOI requests are not being posted on the government's website, contrary to their promise to do so. We then revealed that almost a quarter of general FOI requests come back from the B.C. Government with no documents whatsoever, while more than a third of requests filed by the media come back empty handed. We look forward to the results of the Commissioner's investigations in the new year.

We are also looking forward to the results of an investigation into the failure by public bodies across the province to release information about dangers to health safety and the environment. This investigation was based on a complaint filed by the Environmental Law Clinic at the University of Victoria on behalf of FIPA, and was the culmination of two years of research into the public sector's failure to disclose.

So while 2012 may have brought plenty of grim news on the information rights front, our fingers are crossed for a brighter 2013.

A NEW YEAR MEANS NEW WAYS TO SUPPORT FIPA

Without question, it's been a busy year at FIPA. But as we've scrambled to keep up with rollbacks to citizen privacy and access rights, we've also been fortunate enough to work with many new allies, colleagues, collaborators, and community members who are passionate about information rights. Heading into the New Year, we wanted to think of a way to keep that momentum up and bring lots of new faces into one of the most successful and resilient civil society communities in British Columbia.

That's why we're excited to introduce **monthly donations**. For a minimum donation of $5.00 per month (automatically charged to your credit card through our secure online payment system), you can help keep FIPA running and contribute to develop a number of exciting initiatives, including…

- **A brand new website**, boasting updated help topics, more accessible research, and links to all kinds of information rights resources
- A **new guidebook** that will help instructors, students, and researchers make the most of FOI and ATI in the classroom
- Expanded **education programming**, including a new series of privacy law crash courses designed for those in the social mission and start-up sector
- **Ongoing advocacy** to increase transparency and accountability among government departments, public bodies, and the private sector alike

Becoming a monthly donor is a low-cost, low-maintenance way to support these projects and much more. With governments in B.C. and across Canada aggressively pursuing data sharing practices, expanding surveillance efforts, and rolling back privacy protections, that support is more important than ever before.

Signing up is simple, secure, and fast. Just visit fipa.bc.ca, click "Donate" and select "Monthly" from the Frequency drop-down menu.

We hope that as you plan your holiday giving, you consider supporting FIPA as a monthly donor. Your contributions will help us gear up for another busy year of fighting for citizens' information rights--and winning.

FOLLOW FIPA ONLINE: **Twitter:** @BCFIPA | **News Updates:** fipa.bc.ca/updates

PRIVACY ADVOCATES RAISE RED FLAGS OVER C-12 SURVEILLANCE MEASURES

While the federal government may have been forced to temporarily shelve C-30--its proposed warrantless online spying legislation--following massive public outcry last spring, they show no signs of slowing down when it comes to the expansion of state surveillance efforts. Privacy advocates across the country have now turned their attention to C-30's companion bill, *An Act to Amend the Personal Information Protection and Electronic Documents Act (C-12)*.

The bill proposes a vast swath of amendments to *PIPEDA*, which governs privacy and information practices in Canada's private sector. Tamir Israel, Staff Lawyer at the Canadian Internet Policy and Public Interest Clinic has written that, taken together, these amendments impose a "voluntary sharing regime" on private companies across the country that would undermine the privacy rights of citizens.

Specifically, C-12 creates incentives that encourage telecom companies and ISPs to disclose user data to vaguely defined "lawful authorities" who request that data to carry out equally ambiguous "policing services." Beyond failing to define these contentious terms, in effect broadening them to include such bodies as private security companies, C-12 also "immunizes organizations from any obligation whatsoever to even verify the validity of any lawful authority offered" (in Israel's words).

While the bill does offer up some minimal privacy protections, they are far outweighed by the significant expansion of police, legal, and state powers to access sensitive private information.

As Israel has put it, C-12 is a bill that erodes privacy in the name of privacy itself.

In short, C-12 sets the stage for C-30. By undercutting statutory privacy protections and expanding the number and type of organizations allowed to carry out policing services, it paves the way for the implementation of warrantless access to Canadians' private information. That's why, despite major grassroots victories against Lawful Access itself, it's important that we remain as vigilant as ever. With C-12 in place, a resurrected C-30 will be that much more difficult to stop. FIPA will continue to track C-12 and work with our allies to challenge its privacy rollbacks wherever possible.

TAKE A STAND:

OpenMedia.ca's Stop Online Spying petition now sends a message to your MP letting them know that you oppose C-12, as well.

Visit OPENMEDIA.CA/STAND and tell your MP to take a stand against surveillance.

NEW PARLIAMENTARY STUDY TACKLES BIG DATA, SOCIAL MEDIA AND PRIVACY

Over the past ten years, social media networking technologies have exploded in scope and popularity. Millions of Canadians are now connected to their peers, colleagues, and corporations through networks like Facebook, Twitter, LinkedIn, Instagram, Tumblr, and dozens of other social media platforms.

But with such growth have come a number of privacy threats and breaches, many of which have become major public scandals in recent years. In this environment, with more citizen data snaking its way through global social networks than ever before, it's crucial that Canadian privacy legislation adapt to the new world of social media and big data.

Charmaine Borg, MP, Terrebonne-Blainville

That's why FIPA is pleased to see the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) taking action. Rookie Québec MP Charmaine Borg, who sits on ETHI, has initiated a study into the privacy implications of social media, and how Canadian policymakers might address our changing technological landscape.

FIPA's submission, *Social Media, Big Data, and Privacy: Protecting Citizen Rights in the Age of Connection* can be read in full on our website, and will also be posted to the study's webpage once it has been translated. Drawing on the innovative work of privacy experts like Valerie Steeves, we consider how the rapid growth of metadata and the plummeting cost of data storage challenge us to think about privacy in new ways, and to ground new privacy policy directions in a protection of our sociability and relationships.

The Committee's study, which began in June of this year, is expected to wrap up next year. We hope it compels policy makers across the country to think seriously about the implications of social media on the

> "If the information used to breach our privacy rights increasingly comes from our encounters in digital space, and NOT SIMPLY OUR INDIVIDUAL PATTERNS OF DISCLOSURE, then any policy framework that would defend privacy must take seriously the concepts of interaction and sociality."
>
> (EXCERPT FROM FIPA SUBMISSION)

QUESTIONS?

FIPA provides assistance, referrals, and support to the public on information rights issues free of charge. If you have FOI or privacy concerns, get in touch.

#103-1093 West Broadway
Vancouver BC, V6H 1E2
P: 604-739-9788
F: 604-739-9148
E: fipa@fipa.bc.ca
W: fipa.bc.ca/help

INFORMATION COMMISSIONER LOOKS TO OVERHAUL ACCESS TO INFORMATION ACT

Canada's *Access to Information Act* is showing serious signs of wear and tear. Anyone who has attempted to access government records under the *Act* will no doubt be familiar with the long delays, suspicious loopholes, and sweeping exceptions often applied to what should be routine disclosures.

It should come as little surprise, then, that in the most recent transparency rankings released by the Centre for Law and Democracy in Halifax, Canada ranked 55th of 93 nations when it comes to the accessibility of government records, edging out Angola, tying with Malta, and falling behind Mongolia.

In response to this grim situation, Canada's Information Commissioner Suzanne Legault has convened a nation-wide consultation on the status of the *ATIA*. Since September, Commissioner Legault has been collecting ideas on how this critical but woefully out-of-date piece of legislation can better serve Canadians. This is an important opportunity for citizens all across the country to speak up for their information rights.

Anyone, whether acting as an individual or as a representative of an organization, can contribute. Submitting is simple: just visit the Commissioner's website, follow the links to the consultation page, download the form, and email it to the address provided when you're finished. You can complete as many or as few questions as you like, and your thoughts will be sent directly to the Office of the Information Commissioner. Submissions close Friday, December 21st.

FIPA has prepared an extensive submission for this consultation, available in full through our own library and on the Commissioner's website at www.oic-ci.gc.ca. Throughout this document we stress the importance of such measures as eliminating access fees, expanding the number and type of government bodies covered by the Act, instituting harms tests to justify denials, giving the Commissioner full order-making powers, and creating a single override provision that would enforce the release of records if they are in the public interest.

We also drew extensively on the campaign platform laid out by the Harper Conservatives during the 2006 federal election, which made several excellent suggestions for reforming the *ATIA*, including…

- Giving the Information Commissioner the power to order the release of information.
- Letting the Information Commissioner review the exclusion of cabinet confidences from records released to the public.
- Requiring public officials to create records that document their actions and decisions.
- Providing a general public interest override for all exemptions, so that the public interest is put before the secrecy of the government.
- Making the non-disclosure of government information justifiable only in cases where disclosure would result in harm or injury.
- Ensuring that the disclosure requirements laid out in the *ATIA* are not undermined by the secrecy provisions in other federal acts.

Since taking office, however, the Conservatives have been all-too-keen to forget these promises and let the access rights of Canadians crumble under the weight of an outdated and inadequate piece of legislation. It's high time this trend was reversed.

Though the federal government has a less-than-stellar track record when it comes to acting on the recommendations of Information Commissioners (such as when the Conservatives turned their noses up at former Commissioner Marleau's 2009 *ATIA* reform recommendations, endorsed unanimously by the Commons Standing Committee on Access to Information, Privacy, and Ethics), we remain hopeful that, backed by substantial citizen engagement, Legault's consultation will be a much-needed step towards improving government accountability in Canada.

> "In the most recent transparency rankings released by the Centre for Law and Democracy in Halifax, CANADA RANKED 55TH OF 93 NATIONS when it comes to the accessibility of government records, edging out Angola, tying with Malta, and falling behind Mongolia."

BC COMMISH TRIES TO LIMIT LICENSE PLATE SURVEILLANCE SYSTEM

In a report released in mid-November, Information and Privacy Commissioner Elizabeth Denham put limits on the Victoria PD's use of Automatic License Plate Recognition (ALPR) technology. The system was developed by and remains in the control of the RCMP, and Victoria and other police departments use the system under an agreement with the Mounties. The ALPR system uses cameras and computers to log about 500 license plates per unit per day, then checks the recorded plate numbers against various lists for things like stolen cars, unlicensed or uninsured drivers, and other types of wrongdoing.

If a scanned plate matches any of the entries on these lists, it registers in the system as a "hit" and is stored on an encrypted flash drive. At the end of the day, the local officer turns that drive over to the RCMP. The problem is that flash drive *also* includes all the other plates that were scanned during the shift. This is called "non-hit" data and includes such things as the location of a vehicle at the time of scanning.

The RCMP says it 'de-identifies' the non-hit information within 30 minutes of getting the drives back, and Victoria PD says it is not able to delete the data directly. But in recent months, the Mounties have indicated that they want to keep that data for a much longer period of time, claiming that it might be useful for some other purpose in the future.

Denham was not impressed, at least not favourably. In her report, she writes, "In my view, the use and disclosure of this information for unspecified purposes would not be justifiable under *FIPPA*. Collecting personal information for law enforcement purposes does not extend to retaining information on the suspicionless activities of citizens just in case it may be useful in the future."

Although she says the use of the ALPR system to collect information specifically and clearly connected to law enforcement efforts *can* be justified under this province's privacy law, non-hit data is not related to law enforcement in any sense, and so its collection can't be justified under *FIPPA*.

But even the hits are questionable, since the ALPR system doesn't just flag things like stolen cars or uninsured motorists. It also includes as hit data anything that falls into a broad category titled "other pointer." This is an exhaustive list and includes everything from people out on parole to those who have threatened or attempted suicide. Denham questioned the relevance of this kind of data to law enforcement efforts, and said this category should be cut back considerably to include only what the police actually need.

Finally, she said the system should be reconfigured so that all of the information not related to law enforcement would be deleted immediately, rather than sending all of it to the RCMP.

As Denham points out, though, the RCMP is not under her jurisdiction, so she can't bring them into line. FIPA will be watching to see what federal Privacy commissioner Jennifer Stoddart has to say about this.

FIPA JOINS COALITION AGAINST SECRETIVE TRADE DEAL

This fall, FIPA joined more than twenty civil society organizations from around the globe to voice its opposition to the **Trans-Pacific Partnership (TPP)**. The TPP is a highly secretive trade deal among Pacific Rim countries, currently being hammered out behind closed doors by national governments and corporate lobbyists.

By pushing for changes to intellectual property laws and increasing data sharing between Pacific Rim countries, the TPP threatens to undermine Canadian privacy protections and clamp down on free speech by criminalizing several everyday uses of the Internet.

To learn more about the TPP and to add your voice to the fight against secrecy, visit stopthetrap.net.

UPCOMING EVENT

WHEN: Tuesday, January 22, 2012
8:30 AM-10:00 AM

WHERE: The People's Law School
900 Howe Street, Vancouver

HOW MUCH: By donation;
No one turned away for lack of funds

COFFEE AND BREAKFAST SNACKS PROVIDED

TO REGISTER:
Email the following information to Tyler Morgenstern at tyler@fipa.bc.ca **no later than January 18th at noon**.

Name:
Organization (If Applicable):
Email:
Phone Number:

This event is free, but seating is limited, so book early. Registrants are limited to three seats per organization, including their own.

If for whatever reason you need to cancel, please let Tyler know by email at your earliest convenience so we that we can release your seat to another another registrant.

PROTECTING CONSTITUENT PRIVACY: WHERE TO START?

Those in the social mission, start up, and non-profit sector probably know it better than most: in environments where resources are thin, time is tight, and deadlines are looming, a new information management tool can be a huge boon for efficiency and productivity. But as helpful as third-party email services, list management clients, and cloud hosting services can be, they also come with serious privacy risks that could land you and your organization in hot water.

On January 22nd, join two of Vancouver's oldest and most established advocacy groups--the BC Civil Liberties Association and the BC Freedom of Information and Privacy Association--for breakfast and conversation on the topic of privacy issues facing small organizations today. Over complimentary coffee and light snacks, reps from the BCCLA and FIPA will lead a casual discussion that considers:

- Your duties as data administrators under provincial and federal law
- The challenges that small organizations now face in fulfilling these duties
- New trends like BYO-Device environments and cloud hosting, and what they mean for your in-house privacy practices
- What can happen when your clients' privacy isn't protected
- The resources, services, and support available to you through FIPA and the BCCLA

PROTECT YOUR INFORMATION RIGHTS

Your support of FIPA is essential in the fight for democratic FOI and privacy policy. **Here's how you can help:**

> BECOME A MEMBER
> MAKE A DONATION
> BECOME A MONTHLY DONOR
> SPREAD THE WORD: TWEET US AT @BCFIPA

join + donate:
fipa.bc.ca
for more information:
fipa@fipa.bc.ca