INFORMATION AND PRIVACY COMMISSIONER/ONTARIO

As part of International Privacy Day, the EFF is interviewing data protection authorities and activists across the globe to gain insights into various aspects of privacy and related legislation in your country. The answers to the questions below will be collated into a post on their website.

QUESTIONS & PROPOSED ANSWERS:

In your opinion, which will be the major threats to privacy in 2012?

Threat #1 - Greater surveillance, tracking and monitoring capabilities

The application of new technologies that facilitate collecting detailed information about people's lives continue to create unique challenges and threats to individual privacy rights.

Business and, by consequence, law enforcement, will be attracted to the capability of these new technologies to provide faster and better data on which to make decisions; but this is not an "either – or" situation – privacy needs to be at the forefront.

Businesses must think beyond security – while security is essential to privacy, it does not equal privacy ~ ideally, they should adopt a Privacy by Design approach.

Biometric-based facial-recognition technology

There are significant privacy and security threats to the use of biometrics and in particular to the use facial recognition technology. Facial images and identities are personal information. Being unique in nature, biometric identifiers can represent a person in the digital world, and may be misused, lost or stolen, leading to potential matching, tracking, impersonation and other deceptive practices.

Sophisticated, high-resolution cameras found in surveillance systems – and now conveniently embedded in mobile devices – are allowing for the frequent capture of high-quality facial images, "on the move." Second, software is now available that is capable of indexing vast numbers of photos, allowing for the creation of biometric databases. All of the photos put on the Internet and social media, as well as other information about people that allows for the tagging of these photos, may now be accessible. Taken together, this greatly increases the likelihood of becoming automatically recognized, and far more accurately than before.

The linkage of one's biometric "template" (a digital representation of your biometric) across multiple databases can result in secondary uses that were never intended. One's identity may now be routinely shared online by others, as well as one's personal profile and geo-location data. When facial recognition becomes widespread, a biometric template could be used to identify an individual in multiple databases.

Privacy is all about retaining control - freedom of choice and personal control. We need to realize that the same technology that serves to threaten privacy may also be enlisted to its protection. I believe this entails the use of *Privacy by Design* – embedding privacy directly into technologies and business practices, resulting in privacy **and** functionality.

But video surveillance and facial recognition need not be privacy-invasive. A system using Biometric Encryption is highly privacy protective, yet accurate and secure, leaving no digital trail of biometric templates behind. It's a solution that doesn't store the biometric template itself but rather a "private" template in which the biometric is irreversibly bound to a cryptographic key. It is currently being used in 27 casinos by the Ontario Lottery and Gaming Corp. in my jurisdiction of Ontario, Canada, based on a joint project between OLG and my office.

Thanks to careful *Privacy by Design* planning, innovative use of advances in Biometric Encryption, and effective data stewardship, Ontario has a privacy-enhanced facial recognition system that can serve as a model for others around the world. Not only is it possible to have facial recognition *and* privacy, it is now a reality – and it represents a win/win solution.

Continued misconceptions abound!

The most serious threats to privacy arise from *misconceptions* about privacy in the popular press and are spreading like wildfire.

- Misconception #1 – Privacy is dead or obsolete;
- Misconception #2 – Privacy stops us from performing our jobs;
- Misconception #3 – With the massive growth of new information technologies, you cannot have both widespread connectivity *and* privacy – wrong!

Not only do these misconceptions contradict one an other, they are dead wrong!

Privacy is alive and well, and more relevant than ever. Consider, for example, that the same technologies that serve to threaten privacy may also be enlisted to its support. Properly understood, privacy is becoming increasingly critical to achieving success in the new economy.

In this environment, *Privacy by Design* offers a principled, flexible, and technology-neutral vehicle for engaging with privacy issues, and for resolving them in ways that support multiple outcomes in a full functionality, positive-sum, win-win scenario.

In the consumer privacy and data protection realm, which is the most important legislative and/or policy effort for 2012 that will affect citizen's privacy rights in your country?

In Canada, an important legislative effort in 2012 that will affect the privacy of all Canadians is the anticipated re-introduction of federal "lawful access" bills (discussed further below under question #3).

Another important legislative effort in Canada is the re-introduction of the federal Bill C-12, the proposed *Safeguarding Canadians' Personal Information Act*. If passed, Bill C-12 will include

defining what constitutes "valid consent" in the *Personal Information and Electronic Documents Act* with regard to the collection, use and disclosure of personal information. The bill will also likely expand the number of circumstances where personal information may be collected, used and disclosed without an individual's knowledge or consent. Finally, the bill may implement mandatory reporting of "material breaches of security safeguards" to the Privacy Commissioner of Canada.

Internationally, the European Union intends to harmonize its data protection laws to allow companies to operate across the 27-country bloc under one data protection regulation. This proposed regulation would enhance the privacy rights of all individuals whose personal information is processed in Europe (*i.e.*, not just Europeans' personal information) and may also require companies to take a *Privacy by Design* approach to protecting personal information, including implementing *Privacy by Design* default settings for their business practices and IT systems.

In the U.S., it is unlikely that Congress will pass privacy legislation this year. However, both the Commerce Department and the Federal Trade Commission ("FTC") are set to release separate final reports with recommendations on how to improve online privacy. It is expected that the FTC report will include support for a system that would give consumers a choice on whether they want to be tracked online. The Commerce Department's report will likely advocate privacy legislation that includes providing consumers with notice about the information being collected about them, choice, access to the information, and security to ensure that data is protected.

In your opinion, which is the most important legislative or policy effort impacting citizen's privacy vis-a-vis the government in 2012?

In Canada, a worrisome legislative proposal likely to affect the privacy of all Canadians in 2012 is the anticipated re-introduction of federal "lawful access" bills. If passed in their original form, these bills will provide the police with a much greater ability to access and track information, via the communications technologies that Canadians now take for granted, including in some circumstances, without a warrant or any judicial oversight.

In view, this represents a looming system of "Surveillance by Design," that should concern everyone in a free and democratic society. In this day and age of 24/7 online expanded connectivity and immediate access to digitized information, new analytic tools and algorithms now make it possible not only to link a number with an identifiable individual, but also to combine information from multiple sources, ultimately creating a detailed personal profile of a personally-identifiable individual.

Bill C-50 would make it easier for the police to obtain judicial approval of multiple tracking warrants and production orders, to access and track e-communications.

Bill C-51 would give the police new powers to obtain court orders for remote live tracking, as well as weaker suspicion-based orders (rather than based on a "reasonableness" standard) requiring telecommunication service providers and other companies to preserve and turn over data of interest to the police.

Bill C-52 would require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and would give the police warrantless power to access subscriber information – including IP addresses and personally-identifiable information that goes far beyond address and phone number.

My office holds the various police services in the highest regard and have a deep appreciation for the critical functions performed by law enforcement. However, I oppose legislation that lacks proper judicial oversight, or is deficient in transparency and openness; these elements are vital in a free and democratic society.

We must be vigilant in not allowing the admitted investigative needs of police forces to interfere with our constitutional right to be secure from unreasonable state surveillance. The proposed surveillance powers would come at the expense of the necessary privacy safeguards guaranteed under the *Canadian Charter of Rights and Freedoms*.

Properly supervised, surveillance powers can be invaluable to law enforcement. However, it is equally true that where individuals are subject to unwarranted suspicions, or evidence is poorly handled, or erroneous conclusions are hastily drawn, the consequences for innocent individuals can be devastating. Recent national security-related investigations make this all too clear (*e.g.*, Maher Arar).

I have no doubt that, collectively, the legislation will substantially diminish the privacy rights of Ontarians and Canadians as a whole. We can, and must, have both security and privacy, in unison. It should not be one at the expense of the other. The true value of privacy must be recognized – and ideally enhanced, not diminished – in any effort to modernize law enforcement powers.

Like other Canadian provincial, territorial and federal privacy commissioners, I have been strongly urging the federal government to re-draft these bills, in recognition of the sensitivity of the data being collected. At a minimum, the proposed legislation should not proceed unless it contains adequate judicial authorization and accountability provisions, in order to preserve the vital elements of openness and transparency that are fundamental to Canada's free and democratic society.

Public Parliamentary hearings must also be scheduled to ensure that civil society, as well as the telecommunications industry, has a full opportunity to provide their input.

Which is the most important privacy case either heard by the Supreme Court in the past year, and/or anticipated to come before it in the coming year? Any major case-law victories on privacy last year?

Several Canadian cases strike me as having significant privacy implications:

(1) ***Emms et al. v. R.:*** In March of 2012, the Supreme Court of Canada will hear five related cases from persons who are appealing criminal convictions following jury trials where the Crown and police conducted background checks on prospective jurors. These

appeals are part of a larger problem of 'jury vetting' that was uncovered in 2009 and investigated by my office (see report entitled *Excessive Background Checks Conducted on Prospective Jurors: A Special Investigation Report* http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=8303). The decision of the Court is likely to provide important guidance about the limits of government intrusion into the personal lives of prospective jurors. I have asked the Court for leave to intervene in the case as an *Amicus Curiae*.

(2) ***A.B. v. Bragg:*** In this appeal, likely to be heard later in 2012, the Supreme Court of Canada will consider the right to privacy under the "Open Court Principle" – which presumes that Canadian courts should be open to the public and the media. The case concerns a fifteen year old girl who had been victimized by an individual who had impersonated her in creating and posting a Facebook account as if it were authored by the teenage girl herself. The fake Facebook account included scandalous comments of a sexual nature. The teenager is asking for (i) the ability to proceed with her lawsuit anonymously, and (ii) a partial publication ban concerning the details of the fake Facebook account.

(3) ***Jones v. Tsige:*** One of the most significant Canadian privacy cases in the past twelve months was last week's decision of the Ontario Court of Appeal in my jurisdiction that recognized a new common law tort for persons who have had their personal privacy violated. In order to establish this new tort of "intrusion of seclusion", a plaintiff must show that: (a) the defendant's conduct was intentional or reckless; (b) the defendant invaded, without lawful justification, the plaintiff's private affairs or concerns; and (c) a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish. While it is unclear as to whether any of the parties will seek leave to have this case heard by the Supreme Court of Canada, given the significance of the legal issues, there is a strong chance that the Court would agree to hear the case if leave was sought.

(4) ***Information and Privacy Commissioner of Alberta v. Leon's Furniture Limited:*** In declining leave to appeal in this case, the Supreme Court of Canada missed an excellent opportunity to provide guidance as to the relationship between unique identifiers and "personal information". In this case, the Alberta Court of Appeal ruled that Leon's was permitted to collect the licence plate numbers of customers picking up their purchases, since, in the Appeal Court's reasoning, licence plate numbers are not "personal information" on the basis that they lack a direct connection to a specific individual. In contrast, the law in many other provinces (including my own - Ontario) is the exact opposite – licence plate numbers are indeed considered to be personal information, as they may readily be linked to an identifiable individual. In my view, the Supreme Court of Canada made a mistake in refusing to hear this case and address this important issue.