Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics Study: Privacy and Social Media June 7, 2012

INTRODUCTION

Mr. Chair and Honourable Members, thank you for the opportunity to speak to you today. With me today are Caitlin Lemiski and Helen Morrison, Senior Policy Analysts. I first appeared before this Committee in my previous role as Assistant Privacy Commissioner of Canada. And in February of 2012, I appeared before you in my capacity as Registrar of Lobbyists for British Columbia.

As Assistant Privacy Commissioner of Canada, I led the first investigation by a data protection authority of a social media platform. And as Information and Privacy Commissioner for British Columbia, I conducted the first investigation in Canada of the use of a social media site by a political party. Following that investigation, we issued guidelines on social media background checks.

Today I would like to provide you with an overview of British Columbia's privacy oversight model, followed by a review of some of our recent investigative work related to social media. I will then offer my views on the ways in which Canada's privacy laws are meeting the challenges posed by this new media, and how governments could strengthen enforcement of our laws.

PROVINCIAL PRIVACY OVERSIGHT

In terms of regulating the private sector, the Office of the Information and Privacy Commissioner monitors and enforces BC's *Personal Information Protection Act* (known as PIPA). PIPA determines how organizations may collect, use and disclose personal information. We share the regulatory space with the Federal Privacy Commissioner as BC's PIPA has been declared substantially similar to PIPEDA. PIPA has wide application, including coverage of non-profits; it also applies to employee personal information.

PIPA provides the Commissioner with order-making powers. For example, I can order an organization to stop collecting, using or disclosing personal information. I can also require an organization to destroy personal information collected in contravention of the law.

In my experience, order making power provides me with the authority necessary to ensure that organizations are meeting their statutory obligations.

The purpose of PIPA is to govern the personal information practices of organizations in a manner that recognizes both the privacy rights of individuals and the need of organizations to collect, use and disclose personal data for reasonable purposes. Recognizing this balanced approach, privacy laws do not, and should not, prevent organizations from developing and using technologies that benefit our digital economy.

BENEFITS OF SOCIAL MEDIA

I fully appreciate the innovation and value of social media. It allows human expression to manifest in new and exciting ways, and facilitates public participation. Social media also allows people to connect with family and friends, follow the latest news and build online communities. That said, I share the Privacy Commissioner of Canada's concerns that social media companies may not be giving Canada's privacy laws adequate attention.

All organizations, including social media companies, must follow rules regarding knowledge and consent, and limiting collection, use, and retention of personal data. These rules are particularly significant given the speed with which information on social networks can move and replicate.

I acknowledge that the international context in which these companies operate can be a complicating factor. Canada has a very different statutory framework for privacy than in the United States, where many of the world's most popular sites are based.

However, this does not absolve social media companies from complying with Canada's privacy laws. All organizations doing business within our borders are accountable for their information management practices and must follow the law.

Some of the recent investigative work undertaken by Canadian Commissioners demonstrates that Canada is able to address some concerns about social media and privacy; however, it has been an uphill battle.

RECENT INVESTIGATIVE WORK RELATED TO SOCIAL MEDIA

In British Columbia, my Office recently investigated the collection of Facebook passwords and profile information by a political party that used this information to vet prospective leadership candidates.

What we found was that although the political party obtained consent from the leadership candidates, the collection of passwords and profile information contravened the Act.

Under PIPA, an organization must only collect personal information for a purpose that a reasonable person would consider appropriate in the circumstances. We also found that in viewing the candidates' social media profiles, the political party collected information about third parties without their knowledge or consent. As a result of our investigation, the party agreed to stop collecting passwords, and adopted the guidelines issued by our Office on social media background checks.

In another investigation, we examined the Insurance Corporation of British Columbia's offer to the Vancouver Police Department of use of its facial recognition database to identify possible suspects from the 2011 Stanley Cup riot.

The relationship between social media companies and facial recognition technology is significant, as many of these companies integrate this technology into their products.

For example, last year Facebook integrated facial recognition into its photo services, allowing for the automatic tagging of persons in uploaded photos. Facebook chose not to roll out this functionality for its Canadian users.

Indeed, ICBC's offer to the Vancouver Police highlighted our awareness of the power of facial recognition technology and how attractive it may be for law enforcement.

Law enforcement's use of social media is a particular concern, because social media companies possess some of the largest corporate collections of photographs of individuals. There are important questions about whether individuals have provided meaningful/informed consent for the collection of their biometric information for facial recognition. If social media companies collect this information without proper authority,

then any subsequent use of that information by law enforcement may not be authorized. Moreover, tests have called into question the reliability of this technology. For example, at one US airport, a facial recognition pilot project correctly identified volunteers just 61 percent of the time. Based on this low success rate, the airport abandoned plans to use facial recognition. Yet the issues remain because technology will improve and law enforcement will want to use it.

The relationship between law enforcement and social media, particularly in relation to facial recognition software, is an area that would benefit from greater attention and study.

FACILITATING COMPLIANCE

Statutory requirements, regardless of their content, can have little effect unless organizations follow them. In my view, the greatest challenge to privacy and social media is a lack of awareness by businesses of their obligations to limit the amount of personal information they collect. For example, in British Columbia, many organizations do not understand, and are surprised to learn, that PIPA does not permit them to collect personal information just because it may be publicly available on the internet.

In the context of pre-employment screening, an organization's casual approach to collecting personal information online can lead to unsettling results. For example, although it would normally be inappropriate and illegal for an employer to collect information about a prospective employee's age, sexual orientation, or whether or not they have children, an employer may learn these details by accessing a social media profile.

Personal information on these sites is also prone to inaccuracies. Individuals can set up credible-looking imposter profiles. In addition, like a dragnet, organizations may catch far more than they intended when collecting personal information from their websites.

Some counter that individuals must take responsibility for what they post online. While it is true that we should think before we post, this doesn't mean that we should refrain from reasonable opportunities to express ourselves. In the end, it is all about context, and Canada's privacy laws recognize this by limiting collection and use to what is reasonable in the circumstances.

As Canadians' views about communication and expression evolve, the challenge for Commissioners and governments is to help organizations understand these new distinctions. Mothers should not refrain from posting information about their parenting experiences for fear of repercussions from their employers, and friends should be free to make comments about products and services to each other without unreasonable market surveillance and profiling.

These observations are consistent with a 2010 report by the Office of the Privacy Commissioner of Canada, which states “traditional notions of public and private spaces are changing. Canadians continue to consider privacy to be important, but they also want to engage in the online world.”

Sustained public education and engagement will be necessary to promote awareness and compliance with Canada’s privacy laws in the world of social media.

CONCLUSION

In conclusion, social media companies should use the innovations that have made them so popular to uphold the values of privacy important to Canadians. Protecting privacy is about more than obtaining individuals’ informed consent; it is about what is appropriate in context.

Although the principle-based, technology-neutral laws adapt to new technology, in my view, strong enforcement tools, such as order-making powers and mandatory breach reporting are critical for the federal Privacy Commissioner to regulate this space.

Thank you for the opportunity to appear before you today. I would be pleased to respond to your questions.