Protecting Privacy for Canadians in the 21st Century

ST. JOHN'S, Nfld. – Privacy Commissioners and Ombudspersons from across Canada issued two joint resolutions today at their meeting here, including one urging MPs to use caution as they move to expand the investigative powers available to law enforcement and national security agencies to acquire digital evidence.

The second resolution focuses on personal health records.

The resolution dealing with digital evidence addresses the concern of Canada's Privacy Commissioners over federal Bills C-46 and C-47.

CONTEXT

1. The federal government tabled two pieces of legislation in June 2009 aimed at giving Canadian law enforcement, national security agencies and others (hereafter referred to as "authorities") broader powers to acquire digital evidence to support their investigations.

2. Bill C-46, the *Investigative Powers for the 21st Century Act* (IP21C), would allow authorities to order telecommunications providers to preserve and turn over the details of their subscribers' communications. Authorities would also have the power to apply for special orders to trace mobile communications devices and, by extension, their owners.

3. Bill C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act* (TALEA), would give authorities access to information about subscribers and their mobile devices, even without a warrant. The bill would also oblige all telecommunications companies to build in a capability allowing authorities to intercept communications on their networks.

4. The provisions of the proposed Acts raise privacy concerns. For instance, without a warrant, authorities could gain access to personal information such as unlisted telephone numbers, and e-mail and IP addresses.

5. Canadians consider much of this personal information to be sensitive and expect it to be kept confidential.

6. Canadians also expect their use of computers and mobile devices to remain private.

7. The legislation as currently drafted is not limited only to investigations of serious criminal offences, but also could be used to target even minor infractions and non-criminal matters.

WHEREAS

1. Privacy is a fundamental human right that enables the freedom of association, thought and expression.

2. Canadian courts have consistently affirmed the importance of these rights.

3. Canada has a legal regime governing the use of surveillance that protects individual rights while also giving authorities access to communications when authorized. This framework has been carefully refined over decades by Parliament and the courts.

4. To date, the federal government has presented no compelling evidence that new powers are needed.

THEREFORE

The Federal, Provincial and Territorial Privacy Commissioners of Canada urge Parliament to ensure that the proposed legislation to create an expanded surveillance regime strikes the right balance between individual privacy and the legitimate needs of the authorities by:

1. Approaching IP21C and TALEA with caution because they alter a carefully constructed and workable framework;

2. Obliging the government to demonstrate that the expanded surveillance powers they contain are essential and that each of the new investigative powers is justified;

3. Exploring the alternative that, should these powers be granted, they be limited to dealing with specific, serious crimes and life-threatening emergencies;

4. Ensuring that any legislative proposals on surveillance:
   a. Be minimally intrusive;
   b. Impose limits on the use of new powers and ensure appropriate legal thresholds remain in place for
   c. court authorization;
   d. Require that draft regulations be reviewed publicly before coming into force;
   e. Include effective oversight;
   f. Provide for regular public reporting on the use of powers; and include a five-year parliamentary review.

The second resolution passed by the Commissioners focuses on ensuring privacy protection is built into online health record systems.

CONTEXT

Personal health records (PHRs) have started to attract attention in Canada with recently announced services from the public and private sectors that will offer online health records for consumers. This has major implications for the development of the pan-Canadian electronic health infostructure. In this context, a PHR is generally an online health record that is initiated and maintained by an individual patient but there are a variety of other models and terms (such as "patient portal").[1]

Whether or not PHRs are developed by the private or the public sector, Canada's Privacy Commissioners want to ensure that they encompass the highest privacy standards. Now is the time to build components of PHRs that enhance patient privacy and control.

The Commissioners recognize that PHR services will be appealing to many people who may want to store their medical records online. If a large majority (84%) of Canadians consistently respond[2] in favour of being able to access their own health information summary, including medical treatments they have received, they will no doubt be even more interested in the opportunities online PHRs may be able to deliver, as well as the potential for more robust control over their own personal health information.

Privacy Commissioners note that Canada Health Infoway has launched a pre-certification service for "Consumer Health Platforms,[3] to define standards and architecture. Regardless of such initiatives, PHRs must conform to applicable Canadian privacy laws.

Developing privacy-enhancing PHRs should be consistent with the original vision for the electronic health infostructure. A decade ago, the landmark Final Report of the Advisory Council on Health Infostructure took a strong position in favour of patient control when it set out its strategic direction on electronic health records. Among other key recommendations, such as logging of all access to a patient's record, the authors called on ministers of health to develop electronic health records systems that operate "on a need-to-know basis and under the control of patients."[4]

Canada's Privacy Commissioners see the development of PHRs as an opportunity for the patient empowerment envisioned by the authors of the Final Report. If governments and industry make the right choices now, PHRs could be a key privacy-enhancing technology to improve patients' control over their own health information. PHRs may be the method patients have been waiting for to engage with their health care providers and to be informed about their options in controlling how the health system makes use of their electronic health record (EHR).

IN THIS CONTEXT, CANADA'S PRIVACY COMMISIONERS AND PRIVACY ENFORCEMENT OFFICIALS ("COMMISSIONERS") RESOLVE AS FOLLOWS:

Whether PHRs are developed by the private or public sector, the Commissioners call on all developers to ensure that the applications meet the relevant laws and reflect privacy best practices.

1. The Commissioners encourage the government of Canada, and provincial and territorial governments, to accelerate the integration of PHR services that would allow patients to:
    a. access to their own health information,
    b. set rules for who should or should not be allowed to see their own personal health information,[5]
    c. express their wishes for how their health information is used by health researchers and others,[6]
    d. receive privacy and security breach notification alerts,
    e. see who has accessed their records,
    f. request that errors in their record be corrected, and
    g. gain access to resources and contacts in the health ministries and the privacy oversight offices to better address their privacy concerns.

2. The Commissioners call on Ministries of Health to keep Commissioners and the public informed of their progress toward developing and implementing PHRs.

Notes

[1] There are patient portals and other forms of online access where a patient's information is maintained under the control of a provincial health system, physician, hospital or insurance company.

[2] EKOS survey, Final Report, "Electronic Health Information and Privacy Survey: What Canadians Think — 2007," August 2007, pp.56-57, Online: http://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_EN.pdf

[3] Canada Health Infoway Press Release, "Infoway launches new certification service for health information technology vendors," February 12, 2009, Online: http://www.infoway-inforoute.ca/lang-en/about-infoway/news/news-releases/396-infoway-launches-new-certification-

[4] Recommendation 3.4, Advisory Council on Health Infostructure, Final Report, *Paths to Better Health*, February 1999, p.3-10, Online: http://www.hc-sc.gc.ca/hcs-sss/alt_formats/pacrb-dgapcr/pdf/pubs/ehealth-esante/1999-paths-voies-fin/1999-paths-voies-fin-eng.pdf

[5] The health-specific privacy legislation in some jurisdictions includes masking and locking provisions which permit some patient control.

[6] D. Willison, "Use of Data from the Electronic Health Record for Health Research – current governance challenges and potential approaches," March 2009, Online: http://www.priv.gc.ca/information/pub/ehr_200903_e.cfm