SPEAKING NOTES

STRATEGIES FOR PUBLIC SAFETY TRANSFORMATION
TERRORISM AND TECHNOLOGY:
PREVENTION, PROTECTION AND PURSUIT

by Greg Wright
Executive Director
Integrated Justice Information Secretariat
Solicitor General Canada

(Check Against Delivery)
Bal Harbour, Florida
March 10, 2003

The protection of personal information is essential to building public confidence and trust as we improve interoperability, and enhance sharing of criminal justice information in an increasingly electronic environment. It's essential because there's a good chance that society in general, and specifically those most directly affected by crime – witnesses, victims and practitioners – might otherwise not come forward or participate in the criminal justice process. Victims or witnesses would be reluctant to come forward if they felt their personal information was not properly protected in an electronic environment, and officers might be concerned that their personal or family information information was accessible if issues such as disclosure, access and security were not addressed. Such an outcome would eventually result in less public security and less faith in government.

I'm here today to give you a Canadian perspective on privacy as it relates to the theme of this conference– the common goal of creating a safer national and international community through enhanced communication and information sharing in our public safety sphere. The terror visited upon the United States, and indeed the world on 9/11 has led us to re-frame our core beliefs as well as our understanding of the extent to which terrorists can and will wreak havoc, which raises in turn the measures we would be willing to undertake to avert another such tragedy. In fact Canadian polling data shortly after those events clearly showed that Canadians were willing to sacrifice some level for privacy for increased security. Two-thirds of Canadians indicated that protection from terrorist threats outweighed expectations of personal privacy. However, as the public's sense of imminent danger lessens over time, so may the willingness to accept incursions into privacy. Ultimately, in considering these measures, we must ensure that we don't end up sacrificing those same liberties that we strive to protect.

Information, and the sharing of it, is a pivotal factor in mounting an effective defence against terrorism, and indeed, any crime. In a perfect world, public safety officials have in their hands all the information they need, when they need it, to deal with prospective offenders. And ideally, this information would prevent a criminal event from ever taking place.

Creating a criminal justice environment that effectively allows for electronic information sharing is pioneering work, not just for Canada, but worldwide. Simply put, there is no country in the world that has achieved such interoperability. In Canada, we have focused our efforts to date towards achieving interoperability on enhancing our ability to share critical information at key points throughout the criminal justice system and beyond. This includes the federal, provincial/territorial, and municipal levels, as well as international partners such as the United States.

The appetite for quick technological fixes (if that's not an oxymoron) to reach that goal is understandable. However, it must be tempered by an appreciation of the non-technical complexities of the task, in particular those that relate to privacy concerns.

As North Americans, we take great pride in our recognition of privacy as a distinct value. But what is this thing we call privacy? How do we define it? Well, a very basic definition, one favoured by the Privacy Commissioner of Canada, is that privacy is the right of every individual to control the access to information about him or herself. In the context of information systems and information sharing, it could be defined as the right to exert a measure of control over the collection, use and disclosure of one's personal information.

In Canada, two key pieces of legislation set out the principles through which we maintain our privacy. Nationally, the *Privacy Act* governs the information handling practices of federal government institutions, while the *Personal Information Protection and Electronic Documents Act* or *PIPEDA* covers privacy protection when dealing with the private sector. As well, all provinces and territories in Canada have their own legislation to protect personal information.

In addition, the Canadian *Charter of Rights and Freedoms* protects "a reasonable expectation of privacy".

Finally, the enabling legislation of individual government departments affords protections for the information collected by each department. Interwoven with these important pieces of legislation are key government policy directives that impose strict conditions on data sharing, data matching, and the use of key identifiers. As of last May, new directives require a privacy impact assessment as a condition for project or program funding.

Canada has a federal Privacy Commissioner, who has a measure of oversight regarding national legislation. He is not a government official, rather he reports directly to Parliament. His chief role is champion and overseer of the privacy rights of all Canadians. Although the government of the day is not obliged to follow his recommendations, he can publicize his views widely to all Canadians. Provinces and territories also each have their own privacy commissioners who exercise similar local responsibilities.

I'd like to spend a few minutes now to elaborate on some of the key passages within our legislation. As mentioned earlier, the *Privacy Act* provides some of the key protections for an individual's personal information held under the control of the Canadian government.

The *Privacy Act* includes a set of fair information practices regarding the collection, use, disclosure, retention, and disposal of personal information collected by government departments. These practices emulate the international standards that form the basis of the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, drafted in the 1980's with the agreement of some 20-odd member nations, including Canada and the United States. In fact, the U.S. Department of Justice crafted privacy legislation based on those same standards, cooincidentally with the assistance of one of Canada's provincial privacy commissioners. (Anne Cavoukian)

In the context of the criminal justice system in Canada, the regulations, rules, and policies were designed to carefully balance democratic and individual privacy rights with the need to support the government's public safety mandate. Sections 4 to 8 of the *Privacy Act* set out the core principles of the fair information practices. Let's look at a few key points.

1- Collection

Under Section 4 of our Act, information collected by a government institution must relate directly to an operating program or activity of that institution. Further provisions mandate that the information, wherever possible, be collected directly from the individual, who should be informed of the purpose for the collection.

2- Consistent use

Section 7 of the Act holds that information collected for one purpose should not be used for another purpose without the consent of the individual, unless that use is consistent with the original purpose for the collection of the information.

3- Disclosure

Information is generally protected from disclosure to others without the consent of the individual under Section 8 of the Act.

Other sections of the Act deal with issues such as the length of time information may be retained, the manner in which it should be protected while held in government custody, and the manner of disposal.

However, there are always exceptions. In the case of the *Privacy Act*, one of the key exceptions from the point of view of public safety involves information required or used for law enforcement purposes. Society as a whole recognizes and accepts that a

balance must exist between the rights of the one, and the potential safety and well being of the many. Where demonstrably required, certain privacy encroachments are tolerated in the knowledge that the broader goal of public safety is being served.

This kind of balancing, in the quest for increased public safety, was a prime consideration in the crafting of Bill C-17 introduced last fall in the Canadian legislature. Also, known as *The Public Safety Act,* it is a package of initiatives that will increase Canada's capacity to prevent terrorist attacks, protect Canadians, and respond swiftly should a significant threat arise. However, some of its most important clauses are also its most contentious in terms of their potential impact on privacy.

For instance, a previous version of the bill allowed designated officers of the Royal Canadian Mounted Police to access airline passenger information for the primary purpose of identifying individuals with an outstanding **warrant** for their arrest. This caused a strong reaction from privacy advocates, since the breadth of the authority – the ability to check all passengers for warrants - was not, in their view, demonstrably linked to the actual need--- that is, the protection of air travelers from terrorist attack. As now drafted, designated RCMP officers may now only access passenger information for the purpose of transportation security**.** This would support the RCMP's effective management of the Air Carrier Protective Program. Once this Bill is passed, Aircraft Protective Officers will be able to use air passenger information to assist them in determining which flights to cover and when selected, to screen passengers' backgrounds for potential risks**.**

We are also in the process of reviewing legislation governing lawful access to information and communications by law enforcement and national security agencies. Just to be clear, let me briefly outline what we mean by "lawful access". It is the lawful interception of communications and the search and seizure of information, which law enforcement and national security agencies need to conduct their investigations.

Lawful access is well entrenched and Charter-tested within our legal system. It is sanctioned by legal authorization such as a warrant, after a sufficient demonstration of

need has been provided. This means that only a judge can decide when, under specific circumstances, the need to ensure public safety outweighs the need to ensure someone's privacy. By contrast, the intentional and unlawful interception of private communications is an offence under the *Criminal Code*.

The protection of privacy is of fundamental concern to the Government of Canada. For this reason, lawful access is a tool reserved for serious offences and incorporates strict safeguards and accountability measures, including public complaint mechanisms.

The existing lawful access legislation was designed for rotary and analog technologies, not e-mail or the Internet. Today's criminals and terrorists change cell phones frequently and send e-mail through different Internet service providers around the world in an attempt to shield their activities from detection. Advanced communications technologies are preventing law enforcement and national security agencies from receiving the information that the judge has decided they should have access to. As a result, terrorists and criminals can operate in "intercept-safe havens".

With more than a decade since the last reform, lawful access legislation does not reflect evolving information and communications technologies. For example, the procedure by which law enforcement officers obtain court authorizations to obtain e-mail data is presently the subject of some uncertainty. On some occasions, interception authorizations have been used to collect e-mail information, while in other cases, a standard search warrant has been used for this purpose. Thirty years ago, legal drafters certainly could not have foreseen the need to develop a judicial procedure dedicated to the lawful acquisition of e-mails.

The proposed *Criminal Code* amendments under development aim to provide the agencies with investigative tools tailored to the digital age in accordance with the Council of Europe *Convention on Cyber-Crime*. Agencies would be able to use these tools in the course of their investigative and national security activities to obtain information – but

only about specific, court-identified suspects.

Criminal and terrorist networks are constantly trying to keep a step ahead of law enforcement techniques, especially in the realm of new technology, and unfortunately, they seem to have the resources to do so. To address these concerns, the government is proposing that all service providers ensure that their systems have the technical capability to enable lawful access by law enforcement and national security agencies.

With respect to privacy then, we are faced with the ongoing challenge of defining the appropriate balance between our responsibilities as government custodians of individuals' personal information, and our need to make that information available to those we have entrusted with making critical public safety decisions – often front-line officers in policing, customs, and immigration. And although the horrific events of 9/11 are forcing us to reconsider exactly where that balancing point should be, we still want to be able to find effective, workable solutions within Canada's existing privacy regime, and public expectations.

Having worked to establish a reasonable balance by respecting existing laws, or introducing carefully balanced new legislation, we then work to mitigate the risks of inadvertent or unauthorized use or disclosure of personal information. That's where secure processes and new technologies come into the picture. With the proper command and control mechanisms, new technologies can heighten the security of transactions, and can better safeguard the personal information held by government. After all, in order to maintain public confidence, government must ensure that the highest standards of security and confidentiality apply to its personal information holdings.

Secure processes include message and document encryption as well as role-based access systems, which limit the authority or ability to access sensitive information to those whose role in the organization clearly requires them to access the information. Technology plays a role in further enhancing privacy because of the capability to maintain electronic audit trails of all information queries – something that would never

have been possible in a paper world. Public Key Infrastructure (PKI) and other solutions are being broadly implemented.

We are also beginning to expand the use of biometrics beyond fingerprinting for identification purposes, using retinal-scanning technology for example. None of these issues have easy answers, and they will all be the subject of open debate and discussion.

Our government is committed to maintaining public safety and national security, while protecting the rights and privacy of all people in Canada. We are constantly working to balance the preservation of important individual rights and freedoms with the real and ongoing threat of terrorism. Privacy is a value we will not surrender.

Thank you (+ concluding remarks).
