SPEAKING NOTES FOR

MARK BORNAIS

FOR THE CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM

OVERCOMING BARRIERS TO SHARING INFORMATION AMONGST POLICE SERVICES AND LAW ENFORCEMENT

Ottawa, ON.

April 26, 2004

Check against Delivery

Good morning everyone. Bonjour à tous.

Let me begin by saying that I feel honoured to have this opportunity to speak with you today and equally privileged to be up here on this panel with two such very distinguished gentlemen.

My intent this morning is to build on some of the areas outlined by my Deputy, Margaret Bloodworth in her address from this morning

When the Department of Public Safety and Emergency Preparedness was created, the Government of Canada clearly indicated that public safety and security are one of our top priorities. And without any doubt, information sharing barriers are going to be some of the major hurdles will we have to overcome.

As Director of the newly created Interoperability Project, which is an 18 month, $8.5M million dollar initiative, one important part of my job is going to be helping the government overcome these barriers.

We all know, access to the right information at the right time and may I add, by the right people, is vital in our efforts to foster a safer and a more secure world. The Interop Project goes beyond just criminal justice and law enforcement and will look within and across the domains of Intelligence, National Security and Public Health. I'll have a little bit more to say about this later.

One of our Government's first efforts at eliminating barriers to information sharing in the criminal justice and law enforcement community came about in 1999 with the creation of the Integrated Justice Information Secretariat. Thus began the efforts for the long-term migration from paper-based environments to the digital world. The strategy focused on providing a sound foundation for information sharing by laying the appropriate building blocks for the future.

The Integrated Justice Information mandate is about the sharing of information electronically on crime and criminals through to the events and outcomes to support public safety.

It is a national program that looks to achieving end-to-end electronic processing of an information lifecycle that begins with that call to 9-1-1 and which can lead to an arrest, a charge, a conviction, a sentence, a parole, and a pardon.

While this sounds fairly straightforward, in all there are some 200 discrete types of transactions that can take place daily between law enforcement agencies at the various levels. Much of this sharing involves personal information. The challenge of operating in a coherent and harmonized manner is daunting given that we have multiple user organisations, different regulatory frameworks, various user perspectives, differing resource capabilities, varying privacy rules, multiple legacy systems, different technology environments. I think you get the idea.

Remember that in Canada we have a “marble cake” of justice responsibilities, where an individual accused of murder in, say Duncan, British Columbia would be arrested by a national police force working under provincial contract and charged with a federal offence. This same individual would be tried in a provincial court, by a provincial crown attorney and likely before a federally appointed judge.

If found guilty, the sentence would likely be served in a federal correctional facility. This simple example only begins to scratch the surface of the complexity of our justice system and the need for effective and efficient sharing of data.

More recently, the tragic events of September 11th motivated a worldwide response to terrorist threats and reinforced the need for Canada's public safety and security agencies to act locally, but think globally. Police, for example, must prevent crime in local communities, while being aware of those threats that transcend jurisdictions and geography.

Two aspects of public attitudes were prominent in our public policy setting. The first was a continued fear of crime, despite declining crime rates in Canada. Fear of crime is fed in part by public awareness of perceived justice system failures, both here and abroad. Examples such as the Paul Bernardo case in Ontario, the arrest of Ahmad Ressam at the Canada-US border, or some of the information sharing issues described by Richard Clarke --- have all served as catalysts for both our image in the mind of the public and a need for doing a better job of working together.

Our work is about connecting the dots between and among the many jurisdictions and hundreds of municipalities, each with vast amounts of information, (largely paper-based) over 10 privacy acts and a patchwork quilt of security schemes.

As we move to an increasingly electronic environment - protecting personal information is essential for building public confidence. There's a good chance that society in general, and specifically those most directly affected by crime – witnesses and victims – might not otherwise come forward or participate in the process.

At the same time, information is the pivotal factor in mounting an effective defense and response to crime and terrorism. In a more perfect world, officials would have all the accurate and up-to-date information needed in order to deal with prospective offenders. And in such a perfect world, this information would prevent a criminal or terrorist event from ever taking place at all.

Creating such an environment is difficult work; no country in the world has achieved such a level of interoperability.

While the efficient use of technology is an important tool in the information sharing process, it is not a panacea. It is but one of the multifaceted challenges to information sharing. The appetite for silver bullets based in technology must be tempered by an appreciation of other complexities, be they rooted in culture, business practices or the legal issues stemming from privacy rights. Of these many issues, it is the latter which seems to be garnering the most recent attention, and it is where I would now like to spend a minute or two.

Polling data taken shortly after 9/11 showed that this event affected the lives of many Canadians and changed our perspectives regarding privacy issues. Canadians were willing to sacrifice a significant level of privacy for increased security. Two-thirds of Canadians indicated that protection from terrorist threats outweighed expectations of personal privacy.

But I ask you, is the pendulum swinging back? In February, for example, the Globe and Mail reported that almost half of Canadians now believe that from a privacy perspective, security forces are going too far in their efforts to fight terrorism.

As Canadians, we take pride in our recognition of privacy as a cherished value. We have various legislation which sets out the principles through which we maintain our privacy.

You already know that 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. In the context of criminal justice, our regulatory framework was designed to balance democratic and individual privacy rights with the need to address public safety.

Society as a whole, seems to be willing to accept that where there are clear and pressing needs, levels of increased disclosure and sharing of personal information is tolerated in the knowledge that the broader goal of public safety is being served.

This kind of balancing was a prime consideration in the crafting of Bill C-7 currently before our Senate. Also, known as *The Public Safety Act*, it is a set of initiatives intended to increase Canada's capacity to prevent terrorist attacks and protect Canadians should a 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 the RCMP to access airline passenger information in order to identify individuals with outstanding warrants for their arrest. This caused a strong backlash from both privacy advocates and our own privacy commissioner

This is a classic issue of balance – where would you draw the line in terms of passenger screening? A person wanted for murder or person on a terrorist watch list is one thing. A habitual traffic violator or jaywalker is at the other end of the spectrum. What about all the offences in-between? What about serious offences that occurred decades ago? Reaching consensus on these matters is difficult at best.

This brings me back to the Integrated Justice Information initiative aimed at enhancing officer and public safety by enabling electronic sharing of information.

Our strategic plan sets forth a 'made in Canada" approach which respects the law, jurisdictional responsibilities, and Canadian values. The Plan sets a course for progress based on partnership, standards, systems modernization, and policy development designed to build consistency.

As one example of an enabler, we have published national data standards, which have been endorsed by federal and provincial ministers of justice and the Canadian Association of Chiefs of Police. This will go a long way towards resolving issues related to inconsistent data, and the potential misidentification of individuals.

In addition, the *Canada Public Safety Information Network* supports federal endeavors, and complements initiatives under way in the provinces, territories, and municipalities, such as BC's JUSTIN and PRIME initiatives.

Proper handling of personal information will be reinforced by standards that strengthen the overall effectiveness of information management:

- Safeguarding of information;
- Records management / data integrity; and
- Governance, accountability and stewardship.

INTEROP

As you have heard from our Deputy Minister, the newly launched Interoperability Project is a high priority for the department. I'd like to spend just a few minutes putting this project in context and to explain what it is that we hope to accomplish.

This nation, the United States and most other countries recognize that information sharing is not only key to solving crimes and bringing criminals and terrorists to justice but, it is also absolutely vital to our ability to proactively deter and prevent events which impact our safety and security. Almost daily, we read about events occurring here and around the world where higher degrees of interoperability might have prevented or at least diminished criminal and terrorist acts.

Interoperability is not just about removing barriers or connecting systems and processes, it is about ensuring the right information is available at the right time. The University of Hull in England describes Interoperability as "***a dynamic process to ensure that systems, processes and culture of an organization are managed to maximize opportunities for the exchange and re-use of information***" and, let me reinforce that this project is geared to go beyond the criminal justice and law enforcement community.

It will additionally and inclusively address interoperability issues within the Intelligence Domain, the National Security Domain and the Public Health & First Responders Domain.

Achieving a fully interoperable public safety and security environment is no small task. Such an endeavour has never before been achieved on a large scale by any one nation. We recognize the challenge before us - yet we are fully committed to moving the yardstick forward. How do we propose to accomplish this?

The Interop Project has a number of specific deliverables which are critical to resolving information sharing issues. First of all, we need to understand and address the urgent and pressing requirements that face the public safety and security community.

As such, the Interop Project will by the fall of this year, provide our government with a clearer picture of not only the state of interoperability as it exists today, but also of the critical needs within and between organizations responsible for our protection. We will continue our work to identify gaps in areas such as technology, process, and policy and make the appropriate recommendations for closing these gaps.

Secondly, if we are to make significant and sustained progress, we need to have a plan. Therefore, the Project will develop a strategy and a vision for information sharing across government. This will form the foundation for a framework by which government will assess, approve and implement initiatives that advance information sharing in the public safety and security community.

This will not be done in isolation and will involve significant input from partners and stakeholders. Together, we will build on the excellent work that has been accomplished to-date and continue to ensure that the safety and security of Canada, its citizens and our partners are realized.

All levels of government in Canada are committed to maintaining public safety and security, while protecting the rights and privacy of all people in Canada. They are constantly working to find a balance between the preservation of important individual rights and freedoms with the need for improved information sharing.

This conference could not have been more relevant to our work.

Thank you.