JGM Privacy Speech
(Bal Harbour, Florida - March 10, 2003)

Introduction

Earlier I had the opportunity to address the important topic of domestic and international information sharing policies. I am glad to now speak about a closely related topic: the privacy issues and challenges raised by robust information sharing practices.

In the course of building our domestic information sharing efforts, our respective governments have no doubt encountered similar challenges. One of these challenges is ensuring that privacy rights are not needlessly infringed upon in our effort to counter the threat of terrorism through improved information sharing. At the same time, a second challenge is ensuring that we safeguard privacy rights without chilling the spirit of cooperation that we want to instill in the government agencies and entities that must share their information to ensure our national security. Striking this balance is not simple. It is a delicate balance that must be constantly re-calibrated.

The debate over how to strike the proper balance between cherished privacy rights and the legitimate needs of the law enforcement and intelligence communities is not a new one. This debate has, however, grown more vigorous and vociferous, and increasingly important, since the shocking and unprovoked attacks on the World Trade Center and the Pentagon on September 11th. Although it is vitally important to do everything we can to pursue and apprehend terrorists and other criminals, I believe that law enforcement must be ever mindful that we must do so without unnecessarily abridging our citizens' right to privacy. In the United States, privacy is valued much as it is in Canada. Just as Justice La Forest of the Supreme Court of Canada has said so eloquently, we believe that privacy is "at the heart of liberty in a modern state."

I would like to begin my presentation with a brief description of United States privacy laws, highlighting some similarities between U.S. and Canadian privacy regimes. Next, I will share a few thoughts on the evolving perception of privacy in the United States and how we are balancing privacy rights with law enforcement's need to combat future terrorist attacks. Lastly, I will describe some of the measures that we have instituted to protect information from unwarranted disclosure while simultaneously encouraging more active dissemination of information among government agencies.

Privacy Rights in the United States

In considering the topic of this panel (that is, "privacy issues and challenges"), I asked myself, "what do we mean by 'privacy'?" The concept of "privacy" has varying definitions under the law. Furthermore, if you ask two different people for a definition of privacy you are likely to end up with at least two different answers.

One model places privacy rights into four different categories:

- "territorial privacy" or the right to control entry into one's personal space;
- "bodily or personal privacy" or the right to be free from interference with one's person;
- "information privacy" or the right to control the conditions under which information about oneself is communicated to others; and
- "surveillance or communications privacy" or the right to be free from surveillance or interception of one's communications.

The topic of today's panel falls squarely in the third category, that of "information privacy." Law enforcement's sharing of information about citizens implicates the right of those citizens to control how their personal information is disseminated. In the United States, information privacy, as well as the whole panoply of these other privacy rights, are protected either by our Constitution or by statute.

Constitutional privacy rights only protect against intrusion by the government. For example, courts interpret the Fourth Amendment to apply only to searches and seizures by the government and not by private parties or companies. However, more recently privacy protections against private parties have been created by statute. For example, the disclosure of medical and certain financial information is governed by statute.

U.S. and Canadian Privacy Protections

U.S. and Canadian privacy protections share much in common. For example, the U.S. Privacy Act, enacted in 1974, establishes special requirements for the Executive Branch of the U.S. government when collecting, creating, maintaining, and distributing records that can be retrieved by name of an individual, or other identifier. **The Canadian Privacy Act, which took effect in 1983, also imposes obligations on the Canadian federal government department and agencies to respect the privacy rights of Canadians by placing limits on the collection, use, and disclosure of personal information. It also, much like the U.S. Freedom of Information Act (or "FOIA"), gives Canadians the right to access and correct personal information about them held by these federal government organizations.**

However, there are significant differences between our countries' approaches to enforcing privacy rights. Unlike Canada, the United States does not have a "Commissioner of Privacy" to oversee the government's compliance with its own privacy laws. We have opted for other means of ensuring that the government complies with privacy laws. First, legislation such as the Privacy Act and FOIA confer on the public the right to sue the government for violating these statutes. So our courts can be used by the public to vindicate privacy rights. Second, there are some criminal statutes that exist to punish those who misuse or unlawfully disseminate private information. Third, almost all government agencies have Inspector Generals' Offices that are responsible for ensuring that agencies do not engage in fraud, waste, or abuse, which includes abuse of privacy laws. Lastly, multiple congressional committees have oversight authority over federal government agencies, which they exercise to ensure that the Executive Branch complies with its many obligations

to the public, including adherence to privacy rights.

The Mutable Nature of Privacy and the War on Terrorism

While a right to privacy is deeply ingrained in our legal traditions, the legal analysis of privacy rights can shift over time. For example, as Justice Antonin Scalia stated in a 2001 Supreme Court opinion, the analysis of searches under the Fourth Amendment long ago lost its moorings in common law understandings of property rights and trespass. Today, the touchstone of privacy is reasonableness and expectations. It is important to note, however, that privacy is not a static concept. Rather, the nature of privacy rights evolve and are shaped by historical events and societal context.

Under U.S. law, our subjective expectations are critical to the formulation of privacy rights. The Fourth Amendment's protection against unreasonable searches and seizures takes into account the privacy expectations of society and of the subject of a search. In an oft-cited legal opinion, Justice John Marshall Harlan explained that "reasonableness" of a search entails a two-part, expectation-driven test. First, the defendant must have an actual or subjective expectation of privacy. Second, the expectation must be "one that society is prepared to recognize as 'reasonable.'"

The fact that societal norms have a role in shaping the reasonableness of searches means that privacy rights may change when major events occur that alter those norms. For example, the September 11th terrorist attacks have undeniably altered our expectations of privacy in connection with air travel. However, the extent to which September 11th should be allowed to change our general societal expectation of privacy is still being debated in the United States.

There are those who believe that following September 11th the pendulum has already swung too far by subverting privacy rights at the expense of law enforcement and intelligence gathering authority. Others believe that the government ought to be given even greater tools to protect the public from further harm. It is certainly true that the public expects us to use in an appropriate manner whatever tools are in our arsenal to prevent additional attacks and to bring to justice those who were and are responsible for plotting against us, and, speaking from the perspective of the Department of Justice, we are doing just that, and are unapologetic about it.

We recognize, though, that, while desirous of feeling safe and secure, Americans are extremely reluctant, as they should be, to give up their privacy, and many are understandably on guard against what they perceive as governmental overreaching in this time of crisis. This backdrop frames much of the ongoing debate about security versus freedom and helps explain much of the controversy that continues to surround legislation such as the USA PATRIOT Act. This is an important debate that is healthy for a free society which is governed by the Rule of Law.

USA PATRIOT Act and Privacy

I believe that there has been much misinformation and hyperbole about the scope of change brought about by the USA PATRIOT Act. In addition, provisions of the PATRIOT Act which protect civil liberties – including increasing civil penalties for improper disclosure of surveillance information and new reporting requirements when the government installs its own pen/trap device (such as DCS1000, the Internet-based investigative tool formerly knows as "Carnivore") on a network – have largely been ignored. While there are those who contend that the USA PATRIOT Act has dramatically expanded the powers of law enforcement, I would contend that USA PATRIOT Act is actually a very measured piece of legislation.

Two fundamental objectives animated the USA PATRIOT Act's provisions – increasing our surveillance capacities with respect to criminal and terrorist networks and enhancing our ability to swiftly track down and apprehend criminals and terrorists, hopefully before they can act. Regarding the Internet and other electronic communications, the Act has expanded existing provisions that permit law enforcement, with appropriate judicial oversight, to intercept or access communications.

Obviously such objectives – along with a new, more aggressive approach to law enforcement prompted by September 11th – have great privacy implications. As I described at length in the previous panel, we are witnessing a fundamental change in U.S. law enforcement's mission following September 11th. Law enforcement can no longer be primarily reactive. We must prevent, protect, and deter, as well as respond, react, and punish.

Preventing future terrorist attacks may well depend upon our ability to expand our intelligence gathering capabilities through aggressive use of electronic surveillance. Not surprisingly, this raises concerns about undue infringement of privacy rights. Notwithstanding such concerns, our practices under the USA PATRIOT Act do not upset the delicate balance between privacy rights and law enforcement's investigative needs.

The USA PATRIOT Act accomplishes many of its objectives merely by updating surveillance laws to take account of technological changes that have occurred over the intervening years, such as the increased usage of e-mail, the Internet, and cellular phones by terrorists and cyber-criminals, and by making the law technology neutral. Just because new technologies have emerged should not mean that criminals should be provided with new ways to thwart legitimate law enforcement activities.

There is little doubt that our laws must react to technology. For example, the Supreme Court must occasionally interpret our privacy laws in the face of technological advances. The Court has had to reinterpret the Fourth Amendment in light of electronic tracking devices, enhanced visual surveillance techniques, and most recently, thermal imaging devices. Similarly, our laws must keep pace with technology, and the USA PATRIOT has done just that.

Protecting Information from Unwarranted Disclosure

We are using several strategies to ensure that more aggressive use of surveillance authorities and the greater dissemination of investigative information do not result in unwarranted abuses of privacy. First and foremost, we are being as careful as we can be to ensure compliance with the legal standards required under the law before employing a surveillance technique. Practically all of the amendments to surveillance authorities made by the USA PATRIOT Act require that we obtain legal process of some sort before using them. For example, we cannot obtain addressing information for Internet communications without first obtaining legal process from a judge or otherwise complying with the Pen Register/Trap and Trace Device Statute. And we cannot obtain a nationwide search warrant without a court's authorization. By assiduously following the requirements of law, we ensure that we are not running afoul of privacy protections.

Furthermore, shortly after the USA PATRIOT Act was enacted, the Department of Justice held an extensive training session on the new law that was broadcast to each of the 94 U.S. Attorneys' Offices across the country. This training was intended to acquaint prosecutors with the new law so that we could reduce the possibility of abuses. In addition, the FBI held its own training on the new law to ensure that its agents were also familiar with the new capabilities under the statute, as well as its limitations.

Congress has also created safeguards to accompany the new legal authorities it provided for under the USA PATRIOT Act to reduce the likelihood of government overreach . First, some of the USA PATRIOT Act provisions, such as the provision authorizing the use of DCS1000, require that Congress receive periodic reports concerning its use. Furthermore, many of the new authorities are subject to a sunset provision. That is, unless Congress re-authorizes them before December 2004, they will cease to exist. The potential expiration of these authorities was intended to ensure that the government uses them judiciously or else risks losing them.

The newfound emphasis on information sharing within the law enforcement and intelligence communities that I discussed earlier has also bred concerns about protecting the privacy of the individuals about whom information is being disseminated. The USA PATRIOT Act directed the Director of Central Intelligence and the Attorney General to create guidelines for information sharing, but it did not prescribe the content of such guidelines. Yet the Act did require that special regulations be promulgated for the handling of information regarding U.S. persons to guard against improper disclosure.

Last year, the Department issued such regulations, which require that information about U.S. persons that is disseminated by law enforcement be marked to identify it for special handling. The departmental regulations also provide for tight controls on how such information is transmitted and stored to minimize that likelihood that it will be disclosed for anything other than an official purpose. Much of the dissemination of that type of information is done centrally, from headquarters to headquarters. This means that it is easier to ensure that proper procedures are

being followed because a centralized, trained cadre of personnel is conducting the information sharing.

Conclusion

In conclusion, I think it is entirely appropriate following September 11th to question the balances our laws strike between privacy, law enforcement, and security, and to ask whether the balance is properly responding to new technologies and to new threats. I submit, however, that Congress updated U.S. law through the USA PATRIOT Act to accommodate new technologies and new situations, but it did so in a manner which remained faithful to old principles and long-standing constitutional doctrine. Furthermore, I believe that the Department of Justice is carefully prosecuting its battle against terrorism in a manner that is wholly consistent with safeguarding our vital privacy rights.

The debate about privacy versus security is not likely to end anytime soon. These are difficult times we face and there are no easy answers to these difficult questions. Nobody should claim to have all the right answers because none of us is omniscient. While such questions are being raised, however, it is still our responsibility to protect our nations from the lingering threat of unprovoked terrorist attacks. And we will do so aggressively, but within the bounds of the law.

I would like to thank you for inviting me here today and look forward to answering your questions.