

Remarks of Nuala O'Connor Kelly, Chief Privacy Officer, Before the 25th International Conference of Data Protection and Privacy Commissioners

For Immediate Release
Office of the Press Secretary
September 11, 2003

Sydney, Australia - Good morning. It is a great honor to be with all of you at this gathering of distinguished colleagues and leaders in the international privacy community. First let me thank Commissioner Malcolm Crompton, our host at this gathering, who kindly extended the invitation for me to address this group. I would also like to recognize Monsieur Michel Gentot of the Commission Nationale de l'Informatique et des Libertés, our guide for this session.

It is my great pleasure to also recognize my many distinguished friends and colleagues from the United States of America, from both the public and private sector, who have traveled to be part of the important dialogues taking place at this conference. In particular, I would like to recognize Commissioners Orson Swindle and Mozelle Thompson of our Federal Trade Commission, who have been leaders in the United States' participation in the international data protection dialogue. I'd also like to take a moment to recognize the professional staff of the Federal Trade Commission, so many of whom have become my colleagues and friends in my time in Washington-some of whom are here today, like Maureen Cooney, and others who are back home working while we are all here enjoying the glory of this beautiful country. And of course our many private-sector colleagues, like Marty Abrams of the Center for Information Policy Leadership, who constantly challenge all of us in the privacy community in the United States to do better.

September 11: Remembering Our Fallen Patriots

And it is impossible to speak on this date, without recognizing the tragic events of just two years ago, and honoring the memories of the more than 3,000 people who lost their lives on this day. As many of you know, while I am a native of Belfast, Northern Ireland, I have spent most of my life in and around New York City, and I will probably forever, no matter where I live, consider myself a New Yorker. My family was personally affected by these events, and I also had many friends in and around the World Trade Center.

Citizens of more than eighty countries died on September 11, 2001 in New York, Washington, and Pennsylvania. [Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Bangladesh, Barbados, Belgium, Belarus, Belize, Bolivia, Brazil, Cambodia, Canada, Chile, China, Colombia, Costa Rica, Czech Republic, Dominica, the Dominican Republic, Ecuador, Egypt, El Salvador, France, Germany, Ghana, Greece, Guatemala, Guyana, Haiti, Honduras, Hong Kong, India, Indonesia, Iran, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kenya, Lebanon, Luxembourg, Malaysia, Mexico, Morocco, the Netherlands, New Zealand, Nicaragua, Norway, Pakistan, Panama, Paraguay, Peru, the Philippines, Poland, Portugal, Romania, Russia, Slovakia, South Africa, South Korea, Spain, Sri Lanka, St. Kitts & Nevis, St. Lucia, Sweden, Switzerland, Taiwan, Thailand, Trinidad & Tobago, Turkey, the Ukraine, the United Kingdom, the United States of America, Uruguay, Uzbekistan, Venezuela, Yemen, and

Zimbabwe.] To put that number in context, almost every country represented in this room, plus an additional 58 countries, lost a citizen on September 11.

For the victims of these attacks, and for the victims of the more recent attacks in Bali and Jakarta, and for the victims of terrorism around the world, I ask you to join me in a brief moment of silence.

The 17th century English poet, John Donne, wrote that: "Any man's death diminishes me, because I am involved in mankind." The deaths that occurred on September 11, 2001 diminish all of us because their killers sought to end not only their lives, but to quash the very safe and open society that is the title of our discussion today. This, the largest single terrorist act in modern history, requires us to face those who would seek to diminish a free and welcoming society--one where, on a given day in September, the name of those buildings--the World Trade Center--had real meaning. We--as individuals, as people--must face those who would end freedom of speech, freedom of association, freedom of religion, freedom of commerce, and we must stand for this free and complex society in which we believe.

I know and have heard that many of you are concerned that the United States' reaction to these events has put privacy and civil liberties to the test in our country. But you must know as well that the foundations of privacy and the love of civil liberties run far and deep into the bedrock of our country. I'd like to share with you today both a historical perspective on the underpinnings of our free and open society, and to also tell you about our more modern approaches to government respect for individual privacy.

Foundations of American Freedom: The Primacy of the Individual over the State

From our very Declaration of Independence in 1776, the American psyche has been one which values the rights of the individual over government control. This country has been described as one of "rugged individualists," and our Declaration complained of, and sought emancipation from, "a long train of abuses and usurpations" by the government. This seminal document states of the individual that it is "their right, it is their duty, to throw off such Government, and to provide new Guards for their future security." Interestingly, while most Americans speak of "life, liberty, and the pursuit of happiness" as their individual rights under the Declaration, it is as a "new guard for their future security"--in the so many senses of that word--that is the anticipated, and limited role of a free and just government described by the Declaration. That in this limited role, government is not above laws and man, but rather a creation of law and man, and thus subject to them, is a fundamental underpinning of this document. The first of the litany of offenses against the King in the Declaration were that "He has refused his Assent to Laws, the most wholesome and necessary for the public good." It is not required then, by our Declaration, that government be ineffective, but rather, that it promotes a greater good, and that it be a "new guard for [our] future security," while at all times realizing and respecting the primacy of the individual's rights.

Some thirteen years later, the United States Constitution and the amendments thereto formalized the structure for what the federal government would become. And for those of us working in the government, it is a healthy thing to refer back frequently to the document that created these structures. On a more personal

note, I keep, as has been now reported in the US press, a copy of the section of the Homeland Security Act that created the Privacy Office taped to the wall in my office so I can refer to it constantly. It's a good reminder of what the Congress intended for my job and my office to be about. But I digress.

In the preamble to the Constitution, the purpose for this document is articulated: "We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America." It is a fascinating thing, at a time when our friends in the European Union are in the process of drafting a Constitution themselves, to reflect upon the values that are the foundation of this document. The Bill of Rights, contained in the Amendments to the Constitution, further articulates the rights of the people to freely exercise their religion, to freedom of speech, to freedom of the press; to peaceably assemble, to petition the government for a redress of grievances. to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." However, the Ninth Amendment also states that "the enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."

There is no stated right to privacy in the United States Constitution. But it is an underpinning, a theme, a universal recognition, that has led scholars to describe privacy as a "penumbral" right within the constitution.

American Jurisprudence on Privacy

There is a long, rich, and complex history of judicial pronouncements on privacy in the United States. Author Sheldon Richman wrote in 1993 that "no question in jurisprudence is as muddled as that of privacy." Richman argues for privacy as a property right, a popular viewpoint-or at least a popular analogy--in the United States. However, an even more prevalent viewpoint than the propertarian one in American jurisprudence, and one that continues to be expounded on by our own Supreme Court, is privacy as "the right to be left alone," a standard first articulated in 1890 in an article in the Harvard Law Review written by esteemed jurists Louis Brandeis and Samuel D. Warren. In that article, Justices Brandeis and Warren argue not for "the principle of private property, but that of an inviolate personality."

To have an inviolate personality, or rather, the ability to create a personality or persona for the outside world, is again, I believe, a part of a uniquely American psyche. The power to invent and reinvent one's self can be seen in our cultural icons from F. Scott Fitzgerald's *The Great Gatsby* to present-day pop icons like Madonna. One's choice to reveal or not reveal, and the power to control not only one's personal life and public career, but also to control the information that surrounds one's life, perhaps is not so uniquely American, but rather, is universal. But the power to be unmoored and unshackled from one's social, cultural, economic, or class stratification, and to create an entirely new and different persona, however, does seem to me, at least, a fairly American phenomena--certainly one that is caught up in the American fascination with all things new, with our power to invent, and our power to control our own destiny. And to do that, to create a persona without regard to traditional signposts of family or

background or history, rests definitively on a certain measure of personal control over one's defining information and choices. Justice Brandeis later wrote, in 1928, in *Olmstead v. United States*, that the Constitution "conferred, as against the government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized men."

Much later in this century, a string of Supreme Court cases on privacy again tested our concept of the right to be let alone. Beginning in the 1960s, the Supreme Court considered a number of cases and alternately struck down and upheld various personal choices having to do with that most private act--of sexual intercourse. In 1965, the U.S. Supreme Court struck down a law from the State of Connecticut which prohibited the use of contraceptives by married couples. The Court cited the "preeminence" of the home as the "seat of family life" as entitling a "zone of privacy," as its rationale for permitting the use of contraception. Following that decision, in 1973, in one of perhaps the Supreme Court's most well-known privacy cases, *Roe v. Wade*, the Court recognized a limited right to abortion. And in two recent cases, the court first upheld, and then struck down, state laws prohibiting sodomy, first in *Bowers v. Hardwick* (1986) and then *Lawrence v. Texas* (2003), redefining, most recently, a right of privacy in one's romantic, sexual, and familial matters, regardless of sexual orientation.

It was in the *Griswold* case, I believe, that the concept of a penumbral right of privacy--one that surrounds and is created at the intersection of various articulated rights--was created or articulated. In this articulation, privacy, though not expressly addressed in the Constitution or Bill of Rights, is an essential element necessary to achieving the rights articulated in our constitution. It is almost as if the framers thought it was so obvious that it didn't need to be written down.

Legislative Thought on Privacy

At around the same time *Roe v. Wade* was being decided by the United States Supreme Court, concepts of fair information principles were being explored in Europe and throughout the world. Just a year after this landmark court case, the United States' federal Privacy Act of 1974 was passed. Growing out of universal concerns about the growing aggregation of personal information--partly due to new technologies like mainframe computers--and perhaps also out of the Watergate scandal and other governmental issues of the day--this law provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, through detailed "system of records" notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.

Under the Freedom of Information Act, the principle that persons have a profound and fundamental right to know what their government is doing is upheld--almost in the extreme. Any person at any time has the right to query a federal agency about documents and records. A modest fee may be assessed for the time and effort in compiling those records, and in some instances, that fee is waived. While this right is quite frequently exercised by non-U.S. persons, or citizens of other

countries, it is most frequently exercised by members of the press. The U.S. federal government will spend tens of millions of dollars processing and responding to FOIA requests next year, and thousands of federal workers will spend all or part of their day compiling responses to those requests.

A third pillar of the privacy framework at the federal level reflects, once again, a growing reliance on technology to move data--both in government spaces and on the Internet. The E-Government Act of 2002 contained a landmark requirement for privacy impact assessments by federal government agencies.

The provisions of the E-government act set forth a comprehensive framework for considering privacy in the ordinary course of business of government--serving our citizens. The Act and underlying guidance synthesize a myriad of prior guidance on privacy practices and notices, and will assist privacy practitioners in prioritizing their efforts. In particular, the guidance provides helpful information on the content of privacy notices and topics for required disclosure.

Further, the act requires the parameters for privacy impact assessments. Although in use by some agencies already, generally privacy impact assessments are a new and important tool in the toolbelt of privacy practitioners across the federal government. These new requirements formalize an important principle: that data collection by the government should be scrutinized for its impact on the individual and that individual's data...and ideally before that data collection is ever implemented. The process, the very exercise of such scrutiny, is a crucial step towards narrowly tailoring and focusing data collection towards the core missions of government. This practice should provide even greater awareness, both by those seeking to collect the data and those whose data is collected, of the impact on the individual and the purpose of the collection.

I am pleased to have been a small part of the discussions towards the development of guidance on privacy impact assessments. These new requirements set the bar high for privacy practitioners. These requirements also reflect, I believe, a growing sensitivity and awareness on the part of our citizens regarding personal data flows in the public and private sectors. I believe that this guidance will allow federal agencies to respond to citizens' concerns about these activities and also to be current with, or perhaps even slightly ahead of, the evolution of privacy practices in the private sector.

Under the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them.

Administrative/Enforcement Efforts on Privacy

The United States has, I am told, been criticized for a lack of an omnibus privacy statute. But in the federal government space, at least, one certainly exists, and that is the Privacy Act of 1974. In the private sector, privacy principles are slightly harder to explain, in that there is not one single piece of legislation. However, I would joyfully and passionately pronounce that while the legislative framework is complex, the enforcement--from a multitude of sources--is tremendous and zealous. In fact, it is this multiplicity of sources--legislative, judicial, federal, state,

and local, and not to mention the ever-present press--that makes me so proud of our commitment to privacy and fair information principles, both in the government and the private sectors.

At the federal level, as you already know, a strong commitment has been made by those who regulate the private sector, such as our friends at the Federal Trade Commission, the federal banking agencies, and the Commerce Department.

The United States' approach, as many of you have heard, is a sectoral one. As the string of judicial pronouncements have focused on sensitive sexual behavior and information, the legislative framework has focused on sensitive information used by regulated industries, particularly financial services and the healthcare industry.

In the banking sector, the one with which I am most familiar since I began my career as a banking lawyer, we have federal and state bank and insurance regulatory agencies which oversee and enforce a multitude of statutes affecting how financial institutions behave. The Fair Credit Reporting Act and the Gramm Leach Bliley Act each function at the federal level to limit the collection and use of sensitive personal financial information by private actors in the lending space. In addition to GLBA and FCRA, however, there are other federal consumer protection laws in the banking arena that safeguard sensitive information and empower consumers. The Equal Credit Opportunity Act, the Truth in Lending Act, the Electronic Fund Transfer Act, and the Fair Debt Collection Practices Act, and the multitude of regulations under these statutes, each in some way reinforces the importance of disclosing to consumers how their information will be used or affords consumers clear means for checking and correcting information that may cause financial harm.

State consumer protection laws as well as banking and insurance laws, and the respective commissions that enforce these laws, also play a role in enforcing fair dealings with the consumer, including the use of the consumer's information. This is far more than a system of best practices and principles. This is a system of regular, on-site compliance examinations by regulators, a system which can impose fines of up to \$1 million a day for the most egregious of infractions. This is a system that has bite.

The system of access and redress that has been created under the Fair Credit Reporting Act allows individuals to ensure the accuracy of their data while also providing accurate, equal, and secure information to banks and lenders who seek to make everything from credit cards to home mortgages more readily available. This system is one of the most robust access mechanisms to personal data, and has provided confidence in the U.S. consumer credit system that has made it one of the most vibrant in the world. The Fair Credit Reporting Act and the Equal Credit Opportunity Act have ensured that we as a country have provided equality of opportunity regardless of race, gender, ethnicity, or national origin to what we consider one of the most fundamental elements of the "American Dream," the ability to own one's home. We as a country, at least those of us who have only been in the credit marketplace since the Act first passed in the early 1970s, take for granted that ours is a safe, secure, and equitable system that is a platform for opportunity and advancement while also protecting the privacy and the sanctity of some of the most sensitive of our personal data. The Bush Administration, as

many of you may know, is seeking to ensure that the uniform national standards in the FCRA are not only maintained, but are enhanced by affording consumers some significant new tools targeted at preventing, detecting, and recovering from the crime of identity theft, the fastest growing financial crime facing American consumers today.

The Health Insurance Portability and Accountability Act of 1996--and its thousands of pages of privacy regulations--provide greater protections for citizens than ever before in the use of their sensitive health records. President Bush's decision to move forward with this health privacy rule marked one of the first privacy-enhancing decisions of his Administration. HIPAA's Privacy Rule--still a relatively new set of regulations in its active enforcement--requires that health care providers give individuals greater insight about the use and disclosure of their medical records, greater access to those records, and enhances the individual's ability to control the use and dissemination of those records. The new rules also provide for federal oversight where an individual believes her health privacy rights under the new rules have been violated.

The Children's Online Privacy Protection Act and a host of other related laws protect the privacy and security of our children online. The Department of Commerce's Technology Administration--where I served as chief counsel before joining the Department of Homeland Security--and the National Telecommunications and Information Administration--have worked towards enforcing these principles online both through legislation and also through encouraging self-regulatory frameworks. The Commerce Department has recently been involved in creating a "safe space" for children online through a "dot-kids" domain, And of course my good friends at the International Trade Administration continue to work closely with many of you here today on international commercial data protection frameworks.

The Commerce Department, and even more importantly, privacy professionals from the private sector, have worked closely with groups like TRUSTe and BBB Online to promote best practices and principles. The private sector is particularly to be commended for advancing the dialogue on privacy in the United States, both by appointing senior-level officials whose primary role is to advocate privacy-enhancing decisions for their corporations, and for adopting a self-regulatory approach, through formal seal programs and smaller industry-sector working groups. This approach may be harder to explain, but the marketplace, as both an instrument of sanction for privacy offenders and would-be offenders, and as a forum for innovation, in both technology and policy, to meet privacy needs, has proven one of the greatest forces for privacy advancement.

And we cannot forget our friends at the Federal Trade Commission and their important work. The Federal Trade Commission is the only Federal agency with jurisdiction to enhance consumer welfare and protect competition in broad sectors of the economy. It enforces the laws that prohibit business practices that are anticompetitive, deceptive, or unfair to consumers, and seeks to do so without impeding legitimate business activity. The FTC also promotes informed consumer choice and public understanding of the competitive process. The agency's work is critical in protecting and strengthening free and open markets in the United States, and, increasingly, internationally.

And who among us—certainly not I, who has sat across the table as the representative of a company that was on the receiving end of an FTC investigation—could overlook their enforcement of Section 5 of the Federal Trade Commission Act. Thanks to the championing of Commissioners Swindle and Thompson and others, under the leadership of Chairman Timothy Muris, the Federal Trade Commission has continued, and in fact, drastically increased, the number of staff devoted to enforcement of unfair and deceptive trade practices in the privacy area. Chairman Muris, as he recently explained in his remarks at the Progress and Freedom Foundation meeting in Aspen, Colorado, seeks to focus on harms, such as identity theft, nuisance, and fraud, that arise from violations of privacy and the misuse of personal information in the commercial space.

And this is just at the federal administrative level. A host of state attorneys generals have sought to enforce state unfair and deceptive trade practices acts in the privacy arena. A number of states have constitutional privacy protections. And a host of litigators and class action lawyers have pursued privacy violations, both real and imagined, against corporations on behalf of individuals and groups. This multiplicity of federal, state, local, judicial, legislative, administrative, and regulatory enforcement mechanisms is no doubt complicated. But it also leaves individuals with a multitude of avenues to pursue and redress wrongs.

Privacy and the Homeland Security Department

And so, we have evolved from the right to be let alone, to personal privacy in the bedroom, to freedom of choice in the doctor's office, to online privacy, to now, in the days after September 11, a growing concern about the intrusion of our federal government in the name of Homeland Security.

It is surely one of the greatest honors that I will experience in my career—to have been chosen to serve as our country's first statutorily mandated Privacy Officer. And it is certainly no accident that the first privacy position created by Congress has been placed at the Department of Homeland Security. This new Department, formed largely in response to the events of September 11, 2001, encompasses the work of 22 former federal agencies and 182,000 federal employees. There is no question that the use of personal information about citizens and visitors to our country is fundamental to the department's mission.

This new Homeland Security Department includes the Coast Guard, the Secret Service, the border and customs agencies, a science and technology research unit, an information analysis section, an infrastructure protection division—focused on improving and hardening arteries—both old, like our power and utilities grids, and new, like the Internet. The Homeland Security Department includes the Emergency Preparedness and Response directorate—including an organization known as the Federal Emergency Management Agency, or FEMA, whose sole mission is to assist Americans in being prepared for, and being able to respond to, disasters of any variety, including terrorist attacks.

This department employs tens of thousands of federal workers whose primary job is to prevent the entry of transmission of dangerous goods or persons to our country. These are the men and women who have been described as "standing on walls." They are those who are vigilant, at the borders, in our waters, at our points of entry. They protect us, they educate us, and they assist us when

disaster strikes. It is my office's job to ensure that such activities are performed, at all times, with the greatest respect for the individual--regardless of citizenship, age, race, gender, national origin, or ethnicity. But the very performance of these jobs shows respect for the dignity of the individual--the dignity of that person's right to live safely and move about freely--free not only from unwanted or inappropriate government intrusion, but free also from the physical threats of those who would do them harm simply because they are in America or because they are Americans.

Homeland Security truly means what it is named. Though created out of the ashes of September 11, it is not solely a counter-terrorism agency. Though focused on the tangible assets of our country, such as borders and transportation systems, it is about more than just things--the mission of this department is to protect and defend the homeland in all its facets--both tangible and intangible. As Secretary Tom Ridge has said, this Department is not just about protecting America's assets. It's about protecting America.

Many people thought, when I took this job, that I had a hard job, maybe even an impossible job. But after meeting Secretary Ridge, I knew that while the issues and decisions were going to be hard, it was by no means going to be an impossible job, because, as I like to say, Secretary Ridge "gets it." Secretary Ridge understands what it means to be an American, to have freedom of choices and determine one's destiny. He understands, as does, I believe, the entire senior leadership at the department, the importance of not losing the intangible qualities that make America great, while we strengthen our physical defenses against those who would quash freedoms.

It is clear to me from my work side-by-side with the senior leadership of this department that we are all equally committed to creating a safe society, and each of us has a role in that mission. While safeguarding the people and the places of our country, we must also maintain the liberties and the way of life that have made this country a symbol of freedom and opportunity for people around the world. Part of maintaining those liberties is safeguarding the dignity and the uniqueness of the individual-and protecting the privacy of that individual.

In a speech, just a few days before I joined the department, Secretary Ridge articulated his vision for how the Department of Homeland Security would work with my office: that the privacy office "will be involved from the very beginning with every policy initiative and every program initiative that we consider," to ensure that our strategy and our actions are consistent with not only the federal privacy safeguards already on the books, but also "with the individual rights and civil liberties protected by our laws and our Constitution."

I am very much in agreement with the statutory definition of my office's position as being both "within" and "without" the Department of Homeland Security. As part of the department, we are able to serve as educators, as leaders, and as full participants in the policy direction of important programs. And as outsiders, we are able to turn a critical eye on the most controversial and the most mundane aspects of the Department's operations. But I do not position my office as the enemy of the mission of this department. Rather, I see it as crucial, fundamental. The protection of privacy is neither an adjunct nor an antithesis to the mission of

the Department of Homeland Security. Privacy protection is at the core of that mission.

And the Secretary has thought about, as I obviously do every day, what it means to use personal information in the federal government space—as custodian of the public's security, information, and trust. Secretary Ridge, in a speech to the Association of American Universities, said that "Fear of government abuse of information" is understandable, but we cannot let it stop us from doing what is right and responsible." The antidote to fear, he suggests "is an open, fair, and transparent process that guarantees the protection and the privacy of that data." He is in complete agreement with the advocacy community, with which I work so closely, to bridge the gap between those on the inside and the outside. A dear friend and colleague from one of our leading advocacy groups formulated his thinking this way to me recently: "We recognize that there will be elements of the Department's work that must, by definition, not be part of the public realm. But to compensate for those highly sensitive activities, the process towards creating those policies or programs must be that much more transparent, and the protocols for oversight must be that much more stringent, to make up for the lack of public scrutiny, of government in the sunshine, that we all hold so dear."

Secretary Ridge has pledged, and I will agree that "we will work together to ensure that our new programs appropriately use information, that we protect it from misuse, and that we discard it when of no further use."

Most importantly, our entire leadership pledge that in the course of protecting our homeland "we will not, as Benjamin Franklin once wrote, trade our essential liberties to purchase temporary safety. We must and we will be careful to respect people's privacy and civil liberties."

I am truly honored to be a part of the team of dedicated and passionate professionals at the Department of Homeland Security, and to be a part of the important mission of protecting this country. I can think of few more important missions for a federal government than to keep our country and our citizens safe. And few more important tasks within that mission, than protecting the quality of what it means to live free in America, truly one of the most open societies that history has witnessed.

Role of the Privacy Officer

The Department of Homeland Security privacy officer is the first Congressionally created, statutorily defined privacy office the federal government. The statutory description of the job encompasses not only Privacy Act compliance efforts, but also the evaluation of emerging technologies for privacy impact, as well as the evaluation of legislative and regulatory proposals on privacy. Importantly, the Homeland Security Act, in which my office was created, specifies the completion of privacy impact assessments of proposed rules of the Department as part of the duties of the privacy officer. The Act also articulates the need to review legislative and regulatory proposals across the Federal government, also, importantly and uniquely, provides for a direct reporting relationship between my office and the United States Congress.

Even more than statutorily defined and required roles, however, a privacy officer is an agent for communication and education across the organization. I am creating a team that embeds privacy awareness into the structure and the culture of the organization. That will be accomplished not by one person alone, but rather by working side-by-side, as I've already begun to do, with the policy, legal, systems, and other professionals across the organization to embed an awareness that exceeds the confines of a privacy office. It is a new and different framework, I understand, to have a privacy office within a Department, or as other countries would describe, a ministry. But this is no usual ministry. Encompassing 22 former agencies, the Department of Homeland Security seeks to meld historic agencies--like the Customs Department, which, any employee will tell you, is mentioned in the Constitution and dates back to 1789--with new agencies, like the Transportation Security Administration, created in 2001. How to fit these units together so that their missions, their cultures, their operations are both streamlined and made more effective is an historic challenge and a historic opportunity. Not since World War II has the federal government in the United States sought to reorganize, become more effective, and rededicate itself to a new mission.

How wonderful an opportunity to have joined the department just six weeks after it opened its doors. What a daunting task to embed a culture of privacy into an organization which is currently redefining its culture. But what better time than now? What better way than to be part of the leadership team--to inform decisions, to advise and counsel, to debate and argue when necessary, but to be perceived as an ally, an element, not only as an outsider, or a watchdog (which is also partially what I am, and certainly how I've been described).

The role of the Privacy Officer is to be both within and without. To sit on that wall, to look over and see and hear and ingest the complaints, the concerns, the demands of those outside--citizen and non-citizen alike, and to bring those concerns back inside--and operationalize them, make them real, inform the decisionmaking process in a positive and proactive way. And conversely, to be the vehicle for transparency, accountability, and fairness, through Privacy Act notices that really describe new technologies in plain language that people, even those who didn't go to law school, can understand.

Internal Resources

It is a wonderful role. It is a joyous thing that the members of Congress created this role, and that, even more, the leadership of this Administration and this Department have embraced it. And it is not just an effort of one person. On my team, in the coming months, our headquarters staff will include not only lawyers, but technologists and policy makers who speak with both domestic and international expertise on data protection and privacy. In addition to our headquarters staff, throughout the component parts that now make up the Department of Homeland Security, we already have over 300 employees working full-time on Privacy Act and FOIA compliance work. The total budget allocated towards fulfilling the department's statutory mission on Privacy, including Privacy Act and FOIA compliance will exceed \$10 million dollars in 2004. And these numbers do not even consider the hundreds of dedicated civil servants in the legal department, on the chief information officer's team, in the management directorate, or throughout the policy shops and program development and

technical development offices throughout the department, whose critical work assists my team in creating privacy impact assessments and Privacy Act statements. I am counting on each of these, and many others, to help us educate all of the employees of this vast new organization that their jobs can be performed effectively, zealously, and fully, while at all times respecting the dignity and the sanctity of the individual. I know it can be done.

External Dialogue

And just as we are fully engaged internally, the privacy office must also be part of the external dialogue, and that is why I am with you here today. It is certainly an important challenge, to achieve the security that we need to grow and flourish as a country, as an economy, as a community, while also protecting the rights and the privacy of the individual.

Just as the defense of our homeland is a responsibility that we all must embrace, so, too, is engaging in the debate over how to achieve security while protecting privacy. In fact, our ability to have a free and open debate is a direct result of the freedoms that are at the bedrock of our society. And our willingness to engage in this conversation is, again, a sign of support and respect for our colleagues, our citizens, and our country.

We will achieve a free and open and transparent dialogue and information sharing about federal government through a variety of channels. In the most formal way, agencies are required to publish Privacy Act notices and Privacy Impact Assessments on new uses of technology and new collections of personal information. As you have already begun to see in notices about programs like the Computer Assisted Passenger Prescreening System or CAPPS II, we have endeavored to make these notices meaningful, robust, educational, and to provide true transparency as to intent. We have provided in these and other notices a fulsome view of the types of data intended to be collected, the purposes for which the data is collected, the data retention mechanisms in place, and the access and redress mechanisms. We have attempted to clearly define the purpose limitations for these systems, and have looked to Congressional language and intent for narrowly drawing these frameworks. Importantly, we have pledged that to the greatest extent possible, these access mechanisms will be equal for all persons, regardless of citizenship.

We have provided, through these notices, a lengthy comment and dialogue period--more than is required by law. We have opened and engaged in the debate formally. We have also provided not only the usual fax and postal mechanisms for commentary, but we have even provided an email address. One day last week, my office--and that includes the personal computer on my own desk--received 7,000 comments on one of our notices. That's more than 100 times the usual number of comments received to these types of notices during an entire comment period--and that was just one day during the 60-day period.

I have endeavored at all times to have an open door--and not just to those in Washington, and not just those in the data protection community. We must hear from ordinary citizens what their concerns are--and directly, not just through groups that seek to represent their interests.

I have encouraged all parties--citizens of the United States and other countries, members of Congress and members of Parliaments, data protection authorities from around the world--to engage with us, in a positive, productive, and also civil way. I believe that we can move forward together to achieve our mission of protecting and defending our lives and our way of life, preserving the liberties and freedoms--including that right to be left alone--that we all hold so dear. I encourage you, my colleagues in the data protection community, to place yourselves at the center of your internal debates on governmental use of information, whether in the security, law enforcement or counter-terrorism arenas. It is frankly, a harder, but more important place to be, than remaining on the sidelines and pointing fingers.

I am honored and pleased to find myself once again at the center of this debate over the privacy, the sanctity of the individual in our increasingly complex information society. It is a great debate, a great challenge, and a great opportunity to serve the people of our countries.

It is often questioned, as we've said, whether we can achieve both security and privacy. To this, I of course, answer a resounding YES. The framers of our Constitution clearly thought so: their enumerated list of purposes for government included: establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, AND secure the Blessings of Liberty to ourselves and our Posterity. It is my great hope, and my great belief, and my job, to ensure both domestic tranquility and to secure the blessings of liberty to ourselves and our posterity. Anything less is a failure of our social contract, a failure of our mission, and a failure to advance a safe and open society. And I can assure you, in this, too, we will not fail.