Reboot Communications
Public Safety Technology Conference April 29–30, 2002
Web site: www.rebootnorthamerica.com

LOUIS FREEH PRESENTATION

Thank you very much Tom for that very kind and warm introduction. I wish some of the Christian brothers that I had in high school could have heard parts of it. I went to a high school in New Jersey. It was a great school, but the teaching order that worked there, the last stop before they came to our high school was a reformatory, so, we had a tough time convincing them that we hadn't yet been convicted of anything.

It's a pleasure to be here. Thank you very much and good evening and my congratulations Tom, to you, and the Western Conference of Attorneys General and to all of you who have supported not just the conference, but the theme which is so topical and relevant, not only in the post September 11th world that we live in, but as we face what will be continuous and complex challenges. It's a pleasure here to see some of my good friends and former colleagues, particularly Ward Elcock, who you just heard, the Director of CSIS, and I'll mention a little bit some of the cases and matters that we worked with him and his agency, but just an outstanding leader, insightful and a wonderful partner certainly for those of us in the FBI in the United

States. To Mr. MacAulay, who is not here, also a very great partner, particularly in the areas of counter terrorism, who worked very, very closely with my former colleague and friend, Janet Reno, who you will hear from tomorrow, who was a wonderful Attorney General and a delight to work with.

I have -- and I had when I was the Director, six young boys, so, it was particularly important to have Janet Reno as my Attorney General. On a couple of occasions, I learned later, my children had hung up on her when she called me. In fact, I ran into her one day and she said, I called you last night, but your son hung up. He said you were playing Nintendo. I wasn't playing Nintendo, it was another game, but it really -- it really didn't matter.

I first met her when I was being nominated for the job. The President called me and my family down to the White House which was a very wonderful event for us and I was in the Oval Office with the President and he was speaking to me and they were preparing the ceremony. All of a sudden we noticed a commotion out in the yard. We didn't quite understand what was going on. We came out, he made his introduction at the podium and I noticed that my six year old was in the front row

dripping wet. I couldn't understand what was going on. In fact, he asked me what the problem was. I said it was probably just the heat of the day, he was very overheated. When I found out later right before the ceremony, he was -- the older boy, looking into this pond, there was a pond in the middle of the rose garden, and the three year old came up and pushed him in which caused an enormous commotion and I assured the President I could do better controlling some armed agents than a couple of small boys.

My background, very briefly, I grew up in New Jersey and I worked in the U.S. Attorney's Office for about ten years. Rudy Giuliani was my U.S. Attorney -- just an outstanding lawyer and leader back then. Certainly, in the very sad events that transpired on September 11, he acquitted himself as all of us who knew him would have predicted. Just a wonderful and outstanding leader for both Canada and the United States in many of the aspects of his decision making during that period.

I'd like to talk a little bit about the strategies for public safety transformation that are before you and I think I'd like to begin by saying that the conference highlights really two of the critical

elements for that transformation to be successful. One is the partnership and the interaction between law enforcement agencies and intelligence agencies, if public safety is to become a comprehensive national and international initiative. And I don't think you would find a better example or template of that than what exists between Canada and the United States, particularly, which I will speak about in a moment.

The second critical element is really the partnership between the public and private sectors. Long gone are the days when a government, itself, can protect the country and our liberties, both countries, against the threats which are emerging and continuing. For the first time, maybe recycling our history back two hundred years when government was a part time operation and the citizen soldier and the artisans and formers were the defenders of the countries, both countries. We've almost come back to the point now given the convergence of technologies and globalizations and the threats before us, where a very unique corralling and obligation on behalf of the private sector arises once again. And, in the areas of technology and globalization, as I think I will discuss a little bit in a moment, will highlight that very

much.

I'd like to leave a little bit of time at the end of the session for some questions and I would encourage you please to do that. I was the Director, as Tom said, for about eight years and during that period of time I obviously answered a lot of questions. In fact, the FBI Director, as an agency chief, probably answers more questions publicly than almost any other Washington official because he reports to a number of different committees, to judiciary committees, to appropriation committees, to intelligence committees, to government reform committees, foreign relation committees, commerce committees, etcetera, etcetera. So, not that it was an enviable record in terms of numbers, but I certainly testified more than probably most of my comparing -- comparable colleagues. So, I would encourage you please to answer any questions -- ask any questions and I will leave some time to do that.

The five major challenges I just wanted to touch on briefly this evening which are relevant to our discussion here include, as I mentioned, globalization. Globalization has changed the rules of the game with respect to threat assessment, threat management and the

implementation of strategies. The second key challenge is obviously the convergence of technologies which allows a small group of individuals the economy of scale in terms of technology to challenge the greatest powers on earth in terms of military and economic strength and that's because of the robustness and the incredible impact that these technologies can have, and we'll talk about those in a moment, particularly as related to cyber threats and weapons of mass destruction.

The other key challenge, as I mentioned, is the public and private partnership. Now, more than ever, that key alliance has to be sustained if we're not to only understand these threats, but to manage them successfully. Balancing the need for public safety against our liberties, the protection of our privacy is a key challenge which will become more pronounced as technology intrudes and manipulates the playing field in terms of these particular threats.

Finally, the key element of sustaining this commitment and the enormous resources which must be brought to bear, not just from a government point of view, but also from a private sector point of view. In terms of the globalization of the threats, look simply

at the Al-Quida organization. From using Immarsat telephones to the internet for communications purposes to much more primitive means such as messengers, ancient money exchange systems, membership in sixty-two different countries. And, as we saw in the East African bombings case, not the prototype of what we have learned to be traditionally the whole mox of a terrorist. The subjects in that case were fishermen and store clerks and teachers called together for a particular operation in a very compartmentalized and very clandestine manner. But, the membership is a global one. It's not national. It's really one that spans the globe and increases the -- not only the exposure, but the potential impact of that threat.

The convergence of technology, again, computer technology, weapons of mass destruction, these are new factors, relatively new factors, in the realm of public safety and national security, particularly, when we put them in the hands of a terrorist organization who are willing to die to commit their particular acts.

Balancing privacy and our liberties. Nobody wants to be so good at national security or public safety that we sacrifice our key liberties. Our democracies, particularly between Canada and the United States, our

shared democracy, our concept of civil law, the rule of law, the protection of individuals, the independence and freedom of individuals, we have to balance these critical factors as we take necessary steps to defend, not just ourselves, but each other.

With respect to that particular tension, the key technology issue of encryption is perhaps the best example. In fact, encryption probably embodies more than anything else, the five challenges that we spoke about earlier. The entrusting to the government and its agents of powers to deal with new technologies, but to do someone away that does not impact or impair or compromise the basic liberties and freedoms that we have all learned to love and for which many people have died. Sustaining a commitment and the resources, enormous resources which are required.

With respect to the Canadian and U.S. partnership, if I could just briefly touch upon that. In the areas of terrorism, cross border crime, espionage, there is actually no stronger relationship that exists in the world, at least in my experience, than between the law enforcement intelligence services of both countries, and I know that from a first hand position. With respect to the Canada terrorism issues, we saw only a

short time ago in the Rasam case, the collaboration and the mutual support and the transparency between the two intelligence services, as well as the law enforcement components in identifying and reacting successfully to that particular threat. The events of that case did not take place in a vacuum. For months and months prior to the millennium, elements of the FBI, our intelligence agencies, the R.C.M.P. here in CSIS worked really hand in hand to the point of exchanging officers and operations plans. So, when things got very, very confused during the Rasam case, for instance, everything was really in place. Officers had been exchanged, we had each been briefed on each other's activities and that case was handled in a c-most fashion.

A little way before that there was a case involving a man called Hani al-Sayegh, who was ultimately charged as one of the bombers in the attack at the Saudi Arabian barracks, the Khobar barracks, in 1996. That particular individual who was arrested in Canada by the work of the CSIS, brought back to the United States, ultimately brought back to Saudi Arabia and ultimately charged in the United States. Again, epitomize the very, very seamless and incredible

relationship between the agencies of both countries, and that's how the threat to globalization is addressed. In fact, I think that's the most important critical element in addressing that particular threat, because one country unilaterally, or a group of countries regionally, cannot begin to assess or deal with the threat. The same type of cooperation and transparency exists between us and the R.C.M.P, and when I was a young agent with the FBI in New York City, the first officer of the R.C.M.P. I met was a man named Rocky Graciano, no relationship, I think, to the boxer. He was assigned to the U.S. Attorney's Office in New York City as a full time liaison and the work between the FBI and the R.C.M.P. continuing to this day in the realm of organized crime has been nothing but extraordinary. Again, because of the trust and the reliance and the mutual sharing of information and assets.

The Catronie case, which is a case in the United States Supreme Court, typifies the relationship and the long history of that relationship. Catronie being an organized crime figure here in Canada at the time and the care with which he was brought back and tried and ultimately convicted in a Supreme Court case that went

to the legal merits and verified the manner in which the two countries, with somewhat different laws on the subject, were able to compatibly exchange and -- and work together. So, the first part of that puzzle which is the synergy between the agencies in different parts of the world. I don't think you could find a better model or a better template and Commissioner Acrodelli, Director Alcox, many others here, as well as their colleagues in the state local and provincial forces, have really solved what is probably the most difficult part of the puzzle. The public-private sector link which is more newly found for all of us, again, just as important, and I want to try to discuss that in a little bit.

Going back to September 11th, again in the context of the challenges that I've mentioned before, those attacks did not take place, of course, in a vacuum. In 1993, if you recall, there was an attack against the Trade Tower. The individual who was ultimately convicted, Ramzi Yousef, was trained in an al Qaeda camp and after he was convicted he said several things. First of all, the plan to attack the Towers was a very simple one from their point of view. They were going to explode one tower and collapse it into the other.

The other issue that he mentioned, which again is very relevant to our discussions here today, is the issue of weapons of mass destruction. The bombers in that particular case had planned to put into the explosive device a chemical or biological agent which we call today broadly, a weapon of mass destruction, so that no matter what happened as a result of the explosion, hundreds and thousands of people would be killed. When bin Laden's co-conspirators were convicted in New York City a year ago with respect to the East African bombings case, one of the charges in that indictment specified that they took steps in terms of their conspiracy to accumulate weapons of mass destruction which they were to use. Some of the preliminary searches and analyses with respect to the documents, including laptop computers taken in Afghanistan, again, corroborate the fact that this is a group which not only in regard to the East African bombings case, but continuously thereafter, contemplated, indeed took steps, to actually use these particular agents with what would be even more potentially devastating impact than the horror that we saw on September 11th.

How do these -- how do these globalization issues and the threat square with everything else that's going

on? Well, we know that everything is subject to globalization. If you look at the development of world commerce and economies, the fastest growing part of that is really the development of the provision of services overseas. It was remarked during the demonstrations at the IMF and the World Bank where people were concerned about the exploitation of Third World countries, the facts actually belie that because most of the world's economy, with respect to the provision of services, is now being done in very, very far away places. Major companies all over the world are out-sourcing services including call centers and backup office operations in countries in distant corners of the world because a decent education, an internet connection, and Microsoft Office can really change dramatically, as it has, the whole globalization picture. I don't think since World War I when steamships took to the seas and made sure that trade was internationalized, have we seen a similar and exponential growth of business, economy and services, all related to the ability to use the internet and telephone connections to provide services to major countries and major centers of power. That is why the weapons of mass destruction and the threat of cyber

attacks, particularly emanating from a terrorist group, become very, very important to us.

We saw a very short time ago many, many examples of the cyber threat, and I know that's been a very important subject of your discussions here. If you remember going back just a year or two, the "I Love You" virus, the "Melissa" virus, the phone master's case, many other cases which really are the tip of the iceberg. When I left government service after twenty-six years less than a year ago, I was amazed at the robust growth and the explosion of cyber crime and the potential vulnerabilities both to governments and countries and companies that this technology permits. We had a case involving City Bank where a subject in St. Petersburg, Russia, using a laptop computer in his apartment, broke into City Bank, New York, and move several millions of dollars out of other peoples' accounts into accounts which he had dedicated.

Another case where a very young man in Stockholm, Sweden, hacked his way into the 911 systems in northern Florida and began to shut them down as a challenge, something that he wanted to accomplish. And, in doing so, knocked out police, fire and rescue services in a whole swath of Florida. Again, without leaving the

privacy of his home. Cases involving the Lowes Corporation, the Bloomberg Company in New York, all public cases now, involved cyber threats and extortion and manipulation from literally across the world. We had subjects in one of those cases who turned out to be from Kasikstan and the initial inquiry indicated they were locally based, but upon further investigation, again, using not only government investigators, more importantly perhaps systems administrators and network engineers in the private sector, were able to trace this particular case back to a group of individuals literally in Kasikstan.

What has to be done and what will be done to deal with that threat, again, the government cannot do this alone and that's a theme that I think bears repeating. Not just by former government officials, but I think many people, particularly on the cutting edge in government, will be the first to tell you that.

When I was at the FBI, one of the things that we did was create in Washington a National Infrastructure Protection Centre, NIPC. And, the purpose there was to create a centre of expertise where computer investigators looking at codes and ones and zeros, as opposed to fingerprints and confessions, so to speak,

would be able to work this most difficult class of cases. Cases that challenge the best of our minds and the strongest of our machines. This is an aptitude and an expertise which the government is not able to capture and contain and home grow. It's very, very obvious from some of the cases that I looked at that this is something that is uniquely residing in the expertise of most of you, or half of you, here, i.e. the private sector.

The Infrastructure Protection Centre was designed to do two things, create a centre of expertise, but more importantly, to involve the private sector in these most difficult and most potentially catastrophic types of cases and investigations. And, we were very successful at doing that. We got a buy in from a number of universities, people in the private sector and their CEOs, who were willing to commit help and assistance and even human resources. Ironically, and not ironically perhaps with the government, I had a meeting with several of the major CEOs in the country, including Microsoft and Sun Systems, and as a result of the meeting they offered to provide us assistance, particularly some of their scientists. We found out after that that there was a particular statute, only

the government is capable of this, which prevents it from accepting gifts such as that. So, we had to go back to Congress and ask them to change the statute, which they did. So, at least in the United States, it's now not illegal for a major corporation to give technical assistance to the government in a particular case.

The other program that has been successful is one called the Infragod Program, and the notion there was to create in our major centers around the United States, an association between the government investigators, computer investigators, and those in the private sector. Particularly in the key infrastructure centers, energy, transportation, banking, those key sectors whose infrastructure is certainly a target and a continuing target of opportunity for individuals and groups who, with the ability and the know how, could certainly wage as devastating an attack as anything that we have seen to date. Shutting off the power systems in this country or the United States in the middle of winter, affecting transportation, hospitals, the delivery of emergency services, as I mentioned, potentially could be as catastrophic as anything else that we could imagine.

We also set up computer squads in each of our fifty-six major divisions. That is because traditionally the FBI is broken down into specific crime squads. There's a white collar crime squad, a bank robbery squad, drug squad, etcetera. We know and we experienced the need for this particular expertise to be not only a crosscutting resource in our fifty-six offices, but one where particular expertise had to be obtained and maintained. We went quickly to the private sector for help in training, standardization of equipment, and that's a program that still continues. I was very pleased to see the Congress, just several weeks ago, award several hundred million dollars to that agency, the FBI, to get it what it needs most and that is the equipment, training and technical ability to work effectively in the information age, and that's a c-change for that agency. I would tell you it's a c-change for all of our law enforcement agencies. Maybe less so for the intelligence services which, I think, on a technology plane, were there a little bit before us. The CIA, publicly described now, has gone into the enterprise of research and development in some of these high-tech areas enlisting and inviting the public sector -- the -- the private sector to come in and

assist, and that's what's going to have to be done on a more regular basis.

The weapons of mass destruction I spoke of briefly. We saw, certainly, the Anthrax cases in the wake of September 11th, but even before that, in the Trade Tower case and the Embassy bombings case, in the Tokyo subway case, the ability to manufacture Sarin, which is gas, Ricine, a highly toxic poison which is made from caster beans. Many other of these chemical or biological agents -- very easily done. You can download the formula on the internet in some cases. They can be made with almost no investment of capital, in your kitchen or in your backyard, and delivered very deadly and without a complicated or expensive system. You don't need an ICBM to deliver effectively these particular agents. They can use, and have used, the briefcases, aerosol cans, things like that. It changes the -- the scope of the threat and the necessity to enlist not only new resources, but particularly private sector resources. The whole notion of homeland defence when you boil it down, may call for an additional military command for the United States, the Northern Command, which has been created. But more than anything else, homeland defence and national security

from a counter-terrorism point of view means more and more the participation and the leadership of the private sector and the enlistment of the state and local agencies, particularly in the United States. Unlike Canada, unlike probably most countries in the world, the United States has never had a national police force and that's because the framers, when they wrote the Constitution, had in the back of their mind several things, but particularly did not want a national police force and it came from the history of the Revolution and their own experience as individuals and farmers. So, the rights of the states, in terms of public safety, were made predominant over the federal government, which, of course, was a part time operation and Washington didn't exist at the time. As a result, there's never been developed in the United States a national police force. The FBI, when I left and it's not changed much since, has about 11,600 police officers. That's less than the Chicago Police Department and that's to cover a huge variety of crimes and programs, including national security, counter terrorism, economic crime, which is the single largest portfolio of the FBI, involving now computer crimes and very complex issues, public corruption issues, civil

rights cases, etcetera, etcetera. But, the notion has been to keep this particular agency to the numbers where it presently rests, and even if you add up the other federal agencies, they do not come anywhere near the 750,000 to 800,000 state or local police officers in the United States.

I'm sure you've had the experience in some states driving a couple of miles, you're in another police jurisdiction. That's why there's 17,000 police departments in the United States. In most places in the world this is a huge anomaly, particularly given the responsibilities that those officers have. The dividing line between federal and state crimes is not very clear at all in most of the violent crimes, drug crimes, property crimes, and even some of the economic crimes. The fact that there is really relatively few disputes between who works a particular case is remarkable and I think a testament to a long history of relationships between the federal and state agencies. But these new threats involve not embassies, not worships in every case, but the targets that we saw on September 11th. The mail becomes a delivery system for weapon of mass destruction. We need to be concerned about stadiums and schools and tourists on buses,

etcetera, etcetera.

The technology available, again, the globalization of the threat and the targeting change the rules of the game from a law enforcement and national security point of view. The Deputy Director of Operations at the CIA was just quoted yesterday as saying that preventing another attack is going to be extremely difficult given the number of potential targets and the fact that we have an enemy willing to die for his cause. That means that the war against terrorism, the threats, have not receded into the background. I don't think most people would admit that they have, although here at this particular moment, the issues of commitment and resources become very paramount. Where is the war on terrorism going to go? I think, and I suggest, unfortunately, to the realms of cyber attacks and weapons of mass destruction. I think those are the two most predictable areas given the availability of technology and what we know to be the motivation of some of these groups, where we are the most vulnerable, which is why all these challenges that I mentioned before come very immediately into play.

What else are we going to rely upon the private sector to do and how are these challenges going to be

met? I think, perhaps, the best example, as I mentioned, of maybe all five challenges, globalization, the convergence of technology, the privacy-public balancing, the commitments and the costs, could be illustrated in the issue of encryption technology. I know there's some representatives here from some of the providers and all of us are users and all of us are affected by this great technology, and I call it a great technology, as I have in many occasions testifying before our Congress and others. The government, for many, many years long before the private sector, was the main consumer and user of encryption technology and for obvious reasons, protecting data, protecting information. Government information, in particular, has always been a key requirement whether at war or at peace. So, this is a critical technology and an important one. It's also critical to commerce and to Canada and to the United States, not just because of their economic size, but because much of what we do in terms of innovation, research and development come down -- comes down to intellectual property which is where -- which is stored most easily on systems and in networks. One of the issues that we had to deal with in 1996 was the storage

of what we called economic espionage coming from many places around the world, dozens of countries, most of whom are friends of the United States, using clandestine means to steal economic information, as opposed to military information. And then, in some cases, taking that information and using it in their national production, again, competing very effectively and ultimately out competing the company, wherever it may be, that spent millions of dollars in research and development. And, we found in that discussion that most of this information and most of this key technology was intellectual property which resided on systems and which employees of companies that produced and traded in these intellectual properties had access to. So, literally with the stroke of a computer you could download the most important trade secret of a company, maybe a formula for a biochemical, maybe a pharmaceutical formula, whatever the case may be, and send it literally across the world without, again, leaving the privacy of your office or perhaps your home.

We found that encryption, therefore, was very, very critical for the protection of these secrets, but encryption to which the company and the owners of that

property also had access. So, you didn't have the situation where an employee, a rogue employee, has the keys to the kingdom unbeknownst to and out of the purview and control of the administrator and the owner. It's like somebody having a key to your house that you don't want to have a key and not being able to get it back so to speak.

In 1996 the Congress passed the *Economic Espionage Act*, which for the first time made the theft of a trade secret a federal crime in the United States, which for many, many years had been a state and local offence, but not a federal one. And part of it was in response to very aggressive espionage in terms of economic secrets, but part of it was also because the technology had changed so much and encryption now would be playing a role of protecting those secrets. So, encryption is a good thing, not a bad thing. Where it becomes difficult and problematic is when it's used by terrorists or members of organized crime or spies to conceal and steal things of value, great things of value, whether they be from a government agency or -- or from a private company. And the problem, of course, as we all know, with the strength of encryption today is it -- it can't be broken by brute force. That the

algorithms are so strong that linking all of our computers together and putting our scientists together will not, for the most part, access in a real time basis plain text which is important for law enforcement agents or intelligence agents in the pursuit of their job.

Just look at it from a historical point for a moment. You know, George Washington used encryption with his generals because they wanted to make sure that what they were doing, if the commands and messages were -- were taken or they fell into enemy hands, that the opponent would not know their plans or their secrets, but it was a different kind of encryption. It wasn't the zeros and ones of the hundred and twenty-six bit strength that would take several times the universe to break by using any kind of a brute force methodology. So, what law enforcement is faced with and what national security protection is relegated to is really a uneven playing field with respect to access to this information when it is appropriate for the agency to have access. And I stress that, because that is the issue of privacy, that's the issue of balancing public safety, and not only privacy, but individual rights and liberties.

If a law enforcement agent believes that a person conceals in their home or their papers evidence of a crime, what he or she does in Canada, as well as the United States, is they go to a Magistrate, who's not a law enforcement officer, and make a showing of probable cause. Probable cause is showing that more likely than not a particular piece of evidence will be found in the place where the Constable says it is. The judge, if he or she is satisfied with the probable cause standard, issues a warrant and the Constable then goes and executes the warrant. In the information age that may be a stream of communication, it may be stored data, and the person with the warrant is absolutely authorized to seize that communication, whether it's stored or in transit. The problem with encryption technologies are that once seized, lawfully seized with a court order, the information is of no value because the plain text cannot be retrieved. So, the solution has to be one that meets two criteria. One, the legal standards so we don't change the balance requirement for probable cause or a judicial order. At the same time, we've got to have some type of assistance to that law enforcement officer in that particular situation when literally life or death may depend upon the

information secreted and encrypted in that manner. Ramsey Yosuff, in addition to being convicted for trying to blow up the Trade Towers, was also convicted in New York City of another plan, and this was a conspiracy to blow up eleven U.S. airliners in the Western Pacific and to do it in a period of several hours. The co-conspirators were to go aboard these planes, various aircraft, U.S. aircraft, bring on board various explosive ingredients that taken one by one probably at the time would have passed muster in terms of any airport security, get on board the aircraft, put the device together with a timing watch, Tasio watch, and then leave the flight and have it detonated at a future point. They even went so far as to test out one of these explosives on a Japanese airline where it exploded, a passenger was killed, the airliner didn't come down, but this was a plan that required, because of the scheduling and the timing, vast amounts of data put in a computer and that computer was found. It was left behind in Manila when the subject's apartment caught on fire, they left and the -- the United States ultimately was able to get a hold of that computer. One of the files, actually a couple of the files on that computer, were encrypted, which not only

substantially delayed, but almost made inaccessible the particular information relating to this conspiracy. In addition, there was a plan found to assassinate the Pope, who was due to visit Manila in that particular time frame.

Drug dealers are using encryption, we now know, to carry on vast drug trafficking activities. We know that the cartels, some of the major drug cartels, in recent days past hired software engineers to write some of their programs, encrypted. This is a huge problem for law enforcement, for national security. I don't know how we can in a mature and reasonable way talk about national security in an information age without addressing this particular problem. The UK has addressed it in part by passing a new statute, a statute which commands the holders and makers and users of encryption to make it accessible to police under very strict judicially supervised circumstances. Something akin to that has got to be addressed certainly in the United States.

The *Patriot Act* which followed the September 11th events was hailed by some as critical legislation. It was criticized by a few as over reaching. I think the reasonable interpretation is that it was -- it was

fairly conservative in terms of the new powers, if that's what they were, that the law enforcement agencies received. One of the new authorities, for instance, was the ability to get a -- a credit report on a subject of a national security case and for years that was not the case because there was a statutory prohibition against doing it. I used to testify that, you know, I couldn't get what a used car dealer can get, which was a credit report on these particular subjects because they were placed outside the normal investigative access.

Some of the other provisions of the *Patriot Act* with respect to expanded money laundering, investigatory powers, were not really, in my view, in my experience, radical, and I think it's good that they weren't. It was a very conservative and very temperate approach to what was clearly described as a -- a gap and a need in some cases, but they didn't over reach. Just like none of the people who had been charged with crimes relating to September 11th have been hauled before anything except Civilian, Article 3, Courts and Judges in the United States, although there's been discussion of military tribunals. If you look at what's happened, we have just followed our civilian

traditional procedures where even the worst of the accused receive not only all the benefits that everyone else receives, but in capital cases, obviously, additional procedures and resources for their defence. But, in the key area of encryption, we're left a little bit short and my fear, as the Director, and my fear now as a citizen and a father, is that at some point in the course of an investigation or an exchange of information, someone in the private sector or someone in the government will have in their possession plans to conduct a weapons of mass destruction attack or another such attack as we saw on September 11th and that information will be constructively unknown to us, actually in reality, unknown to us because the plain text of it will not be retrievable in any format or by any means currently available to the government law enforcement.

So, what's to be done about that? Well, we went around and around for a number of years about statutory requirements, a little bit like the one that has passed now in the UK, but there was no strong support for that. And the privacy groups and the industry groups had, what I thought, were and remain, very strong and very good arguments about why the industry should not

be forced and required to provide the keys to its products, particularly when a lot of encryption can be downloaded from the internet and can be changed and permutated very, very quickly. The argument in response to that was the commercial encryption that is made by industry providers and software companies covers not the whole universe, but a big part of that universe, and a very important window for law enforcement and national security when no other is available. But, be that as it may, the *Patriot Act* notwithstanding, there has been no resolution of this particular problem and nobody wants to be in a position, whether you're a government official, a corporate official, or an affected personal position, where this information was in our possession and known and nobody could do anything about it because we couldn't access it and we couldn't unscramble it in time and there was no means and no place to go with this particular problem.

Some of the work that's been done to address that, Congress recently funded a technical support center where, again, government personnel, but more importantly private sector resources and personnel, will come together to try to work these particular

problems. Now, maybe it's a non-network solution, maybe we attack the information at the keyboard juncture, etcetera, etcetera, etcetera. There's all kind of ideas and technologies and I'm convinced the ability to solve this particular problem, again, not by the government working alone, and I think that's the key part, it's having the private sector involved.

Voluntary contributions, as well as ideas and innovation and leadership by the private sector here is very, very important. As we increase the strength of these encrypted programs and products and devices, we have to keep in mind that the one person I think we would all agree we don't want to keep out, is a policeman or a policewoman who has a court order in hand because they've met all the legal requirements that we have set for them. We've protected our liberties, we've done everything the way we would want it to be done when a powerful tool is given to law enforcement or national security, but we would like to know and like to have the comfort that that particular information would somehow, in some way, be available. And that's going to remain a challenge for us. And as I said before, I think it exemplifies in summary all five challenges. The key part, again, is the -- is the

private and public partnership which is why I think this particular forum and others like it are excellent and outstanding in terms of just bringing you together as a community because you are community, a unique public-private community exchanging information, raising problems, coming up with solutions, technologies and ideas. There's -- there's a lot to be done. The -- the playing field has forever changed and I think what's to come is a continuing threat. What it has to be matched by is a continuing commitment and huge resources. I could tell you from just a short time in the private sector the amount of resources necessary to protect companies, whether we're talking about physical security or ventilation systems, information systems, the creation and maintenance and protection of information, a key corporate, private, public challenge and as many ways as there are to protect it, there are more ways and challenges to deal with in the days to come. So, this is the -- this is the unique challenge of our age, I think. National security, economic security, I actually believe they are one in the same to the extent that we protect our economic security, we protect our national security, which is why the public-private partnership is not a

forced marriage. It's really one made of need, but also the potential for solving all these problems resides very uniquely there.

I'd like to leave a few minutes for some questions and please, again, if you have some issues or questions past or present, I'd be happy to try to address them for you. Thank you very much.

MR. FREEH: Yes sir?

(QUESTION FROM THE AUDIENCE NOT AUDIBLE)

MR. FREEH: Okay. The question is with respect to protecting our freedom to move and travel the security procedures that have been put into place, or a I should say enhanced, since September 11th, what do we think about that and what -- what does the future hold?

I think the answer is really going to be, again, in technology. I mean, I'm not privy to all of the science and innovation there, but most of what we need to defend against can probably be relegated to technical solutions. Now, you still need humans to operate that technology which is one of the bigger problems that I think surfaced in the intense of analysis of the security systems, particularly the airport, that the airport was not really a hardened facility that we were watching passengers, but people

that were cleaning aircraft and providing food were just in and out of the facility without any challenge or security whatsoever. So, I think part of it is really going to be the application of either current or future technologies by people who are expert and knowledgeable about their operations. There's got to be a procedure, for instance, for identifying, you know, a trusted traveler. Whether it's a business person or a mom or a student who, with very complete and maybe updated information, can be relied upon as a trusted traveler who doesn't pose a threat. And then, either by a biometric device or some other means, tagging or identifying that particular traveler, so when he or she appears, there's an expedited and facilitated way on and off an aircraft, or out of a secure location. You know, one of many, many ideas, but, you know, I don't think this is an overwhelming challenge. I think we're sort of looking at the, you know, the very hasty application of our current procedures, which probably in and of themselves are not going to do the job. Yes sir?

QUESTION FROM THE AUDIENCE: The FBI seems to be much more proactive in terms of working internationally and being proactive gathering data especially because of

the terrorism issues. Doesn't it make more sense for us to try to combine -- for the U.S. to combine these agencies and have a single agency and is it easier for other countries to work with us if we had one organization instead of all these different agencies? And I guess the bottom line to this is does Tom Ridge have a chance?

MR. FREEH: Well, you know, I think -- I think the proposal is -- is to really coordinate, as opposed to just, you know, combine lock, stock and barrel, all the different agencies. His role right now is a coordinating role and, of course, his proposal, as well as General Scowcroft's recommendation is to look at the efficiency of combining different intelligence operations and agencies into one single point of contact and expertise. I think that makes a great deal of sense. What certainly makes sense is coordinating, you know, the law enforcement and the intelligence piece. As we saw in the Rasam case and many, many other cases that I've mentioned, the necessity for interaction between the law enforcement and the intelligence networks is critical. In fact, long before September 11th, actually a year before the East African bombings, the FBI and the CIA, this is public

information, put together a bin Laden cell, an al Qaeda cell, and we had officers working side by side with agents who became expert in this particular area. In fact, the -- the lead FBI agent in that endeavour, John O'Neill, very tragically, very ironically, left the FBI about a week and a half before the Trade Tower, took a job with the World Trade Center as the head of security, was one of the people killed. But that initiative, first of all, it gave them a -- a jump start when the Embassy bombings occurred. And the reason that case was put together so well was because they were working on a year of collected and shared data, but also the two agencies were working very, very closely together. In the post September 11th environment the synergy between law enforcement and intelligence is absolutely critical. We opened up about thirty new offices overseas in the FBI because the -- the need to work with our counterpart, law enforcement agencies, as well as the security services in those country -- countries became very, very critical. So, I think, whatever we do at home has to be done carefully. We don't want to completely blur, for instance, or even partially blur, the distinction between law enforcement and intelligence, because

there's different interests, particularly liberties and privacy and truths that I think have to be protected by having a -- a public system in terms of the law enforcement process, because it is all public, and a clandestine system which has to be clandestine if it's going to be effective. In terms of all the different intelligence agencies, you know, I think these proposals are very serious for the first time and -- and are being looked at very carefully.

QUESTION FROM THE AUDIENCE: Little has been said today about the importance of private security, yet private security is one of the fastest growing sectors of the service industry. Yet, for the last decade there's been a great deal of suspicion about its level of accreditation and training. Would you like to speak to the question of partnerships with private security?

MR. FREEH: Well, of course. Private security is going to provide, in the issue of homeland defence and counter-terrorism cases in all of the things that we discussed this evening, a very critical ingredient, because as a source of information, whether it's a security operation at a flight school or at an airport or at a -- a shipping yard, is going to be the original source, in many cases, of very critical information and

intelligence, as long as there's a means to get that to the right places, which is why I think your question on credibility and certification is very appropriate. Part of the challenge that we're going to have as we manage these threats is to properly educate and create channels of communication and information exchange between private security firms and the people who are given the governmental responsibility of national security or homeland defence. So, I think accreditation issues, training issues, standardization issues -- there was a report released in February, you may have seen it, which was sponsored by CIO in the Untied States, as well as the U.S. Attorney's Offices and the FBI, that set out for the private security community, particularly in the -- in the IT areas, suggested guidelines to come up with security plans, process for testing that plan, reporting requirements -- when and where do they report. They don't report everything, obviously, but the things that are important have to go to a particular place, but that's really just the beginning of, I think, an answer to your question, which is giving them the credibility through accreditation, training, and information exchange, where they can be as effective as the, you

know, the 750,000 police officers are out there for the FBI everyday. In fact, there's probably more in terms of private security, so, there's a lot we need and can do in that -- in that area. Okay. Thank you.