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

TOM GEDE PRESENTATION

We are just going to go ahead and proceed with the first presentation which is on the *U.S.A. Patriot Act*, and I'll learn how to push the button here. There we go.

I'm generally going to cover the surveillance and wiretap laws that were effected by the *U.S. Patriot Act* in the United States, but I'll also try and cover a few other topics and issues, and of course, we'll have some time for questions and answers afterwards.

As you know, the President and Congress were brought into action rapidly after September 11th looking at, and looking for, new tools to deal with terrorism. Many tools had already been -- they were in the category of desired tools. They were tools that, I think, the U.S. Department of Justice had sort of on the books as proposals. But, by September 24th, Attorney General John Ashcroft asked for these new tools needed to identify, dismantle, disrupt and punish terrorist organizations.

Significantly, on November 8th, the Attorney General announced a shift of the primary focus of the Department of Justice in Washington from investigating and prosecuting past crimes to identifying threats of

future terrorist acts, preventing them from happening and punishing would be perpetrators for their plans of terror. If you think about this, this is a hugely significant shift in the focus of the Department of Justice. That of prosecuting to that of identifying and preventing terrorist acts. To quote, "We must prevent first, we must prosecute second". For the Congressional response, the Administration proposed what they called the anti-terrorism act of 2001. There was a House bill introduced on October 2nd, remember, this was from September 11th to October 2nd, so not much time was -- there was very little gap on this. In Congress things work very slowly and this -- this kind of timetable was very fast. It was called the *Patriot Act*, provide appropriate tools required to intercept and obstruct terrorism.

On the Senate's side, on October 4th, two days later, a proposal was made united and strengthening America or *U.S.A. Act*, passed with various limitations on wiretap and computer intercept provisions. The debate drew opposition from much of the technology and civil liberties groups, Electronic Privacy Foundation and ACLU and the like, but the bills were merged and passed and President Bush signed the *U.S.A. Patriot Act*

into law on October 26th, 2001.

This is a brief summary of the features. One, it allows federal officials to get wiretapping orders that follow a suspect to any phone the person uses. Allows federal officials a nation wide search warrant for email and physical searches in terrorism investigations. It authorizes nation wide search warrants for computer information on terrorism investigations, including billing records. It allows federal officials to seize voice mail with a warrant. It requires judicial monitoring of the FBI's use of the carnivore email tracking system. It authorizes individuals to sue the government if it leaks information gained through the new surveillance powers. And, it added a sunset date in four years for most of the new wiretapping and surveillance powers.

For the Canadians here, these are some of the dry and boring details of what the statutory authorities are in the United States relating to wiretap and surveillance. There is a principal wiretap statute in Title 8 of the *United States Code* that allows, and these are the key words, contemporaneous interception of a wire communication. It requires a probable cause shown and an order from a federal court or a warrant

which we typically call a Title 3 Wiretap Order because it comes from a federal court that is established under Title 3 -- under Article 3 of the *Constitution* and is Title 3 of the *Wiretap Act*.

Federal *Pen Register and Trap and Trace Statute* also in U.S. federal law permits law enforcement to install and use devices that record phone numbers that are called by a suspect, that's the pen register, or received, that's the trap and trace. It requires an ex parte showing to a judge that it's going to result in relevant information to an ongoing criminal investigation generally limited in time.

The *Electronic Communications Privacy Act*, or ECPA, is not really a wiretap or surveillance statute. It's a privacy statute that was passed by Congress to ensure that electronic communications are provided with an overarching privacy, but the law does allow an administrative subpoena to compel communication providers to disclose certain transactional records, such as a customer's name, address and length of the service.

And, the *Foreign Intelligence Surveillance Act* you heard referred to earlier, allows wiretapping of a foreign power or terrorist in the United States on a

probable cause showing, limited to foreign intelligence. It requires a court order or the United States Attorney General can do it without the court order when he certifies that he's using certain minimization procedures to minimize disclosure and guarantees there's no substantial likelihood of privacy violation.

What the *U.S.A. Patriot Act* did is it allows these pen register or trap and trace orders anywhere in the nation rather than in a particular narrow jurisdiction and for the internet. The information has to be relevant to an ongoing criminal investigation and allows the capture of routing or addressing information from internet users, but not content. The government has to use the latest technology to avoid intercepting content. This is very controversial because, as you can imagine, routing and addressing information on the internet may well involve a search engine searching for whatever somebody has put into their search, which may well reveal content or arguably can reveal content. And so, it's not exactly the same as a telephone number. On the internet you're actually reaching out and getting more information and the controversy to it is, of course, whether that additional information on

the routing and addressing information of an internet address is content.

The FBI has been using devices that screen through a lot of internet interceptions and there was quite a furor in the United States over the threat to privacy as a result of using the carnivore like devices. The Act does allow a recording of those intercepts on the internet through a carnivore like device, but requires complete recordation of which officers installed it, the date and time it was done, and -- and further requirements. These things were upheld -- pen registers and trap and trace was upheld in the United States Supreme Court under legal standards that indicate that a -- a user is voluntarily exposing their dialing information to the service company and, therefore, there's no legitimate expectation of privacy. The same would apply then to the internet routing and addressing information as long as no content is involved.

Nation wide subpoenas for electronic records was also a part of the *Patriot Act*. Previously, providers only needed to disclose name, address and length of service, but under this Act it now covers means and source of payments, such as bank accounts, credit card

numbers and the like. These disclosures are needed rapidly in terrorist investigations. Seizure of voice mail messages. There was sort of glitch in the law previously and voice mail was viewed as electronic storage of a wire communication and, therefore, required the more onerous Title 3 wiretap order and the *U.S.A. Patriot Act* cleared that up and made -- made it clear that a voice mail could be done with a single search warrant and not the more onerous Title 3 wiretap order.

The authority to share criminal investigative information, a subject we've discussed here a little bit before. The *U.S.A. Patriot Act* allows disclosure of foreign intelligence information from wiretap intercepts of criminal investigations to be shared with any federal law enforcement intelligence, protective immigration national defence or national security official. And foreign intelligence information relates to the ability of the United States to defend itself against attacks or terrorism. Also, the *U.S.A. Patriot Act* provided for nation wide warrants for electronic evidence. The Silicon Valley venue is the usual place where everybody had to go and it makes more sense to go to one place, than to have to keep bouncing around the

country.

Roving surveillance authority, the FISA, or *Foreign Intelligence Surveillance Act* was amended to allow surveillance to follow a person that uses multiple communications devices, cell phones and the like, or locations. This actually is already permitted in the non-FISA context and all the *U.S.A. Patriot Act* did was conform the FISA to the existing wire tap and surveillance law.

Under the *Foreign Intelligence Surveillance Act*, *U.S.A. Patriot Act* eliminated a showing under that Act that the target is in communication with an agent of a foreign power. It's getting very confusing these days whether somebody in al Qaeda is in fact the agent of a foreign power. And pen register and trap and trace need only be relevant to the investigation to protect against international terrorism. The reform of FISA for a broader surveillance order, this was controversial as well. Originally FISA required that the purpose of the surveillance was to obtain foreign intelligence information and that was changed to a significant purpose. The administration proposed a purpose instead of the purpose. That change of one word was significant because if the order coming from

FISA was that it could only be used to obtain foreign intelligence information, then -- then it was likely that that information was not the kind of information that could be shared, or would be shared, easily with law enforcement or protectoral officials who might need it for a case. And, that's a little bit of humour, call anytime, we'll be listening.

There is one additional aspect of *U.S.A. Patriot* I wanted to mention and that is that the *U.S.A. Patriot Act* also added a significant number of money -- anti-money laundering provisions and the U.S. Department of Treasury has been responsible for implementing those on the eve of an April 24th deadline set by the -- by the Act. The U.S. Treasury Department recently issued some far reaching regulations that will dramatically change the way thousands of mutual fund security dealers, futures merchants, money transmitters and credit card operators do business. The rules will increase the risks of regulatory sanctions for failure to maintain multi-pronged anti-money laundering provisions and programs that the government will now require commencing July of 2002. Eventually it will include those -- those rules will include hedge funds, pawn brokers, travel agencies, car, boat and plane dealers,

and private bankers, may all at some point come under that umbrella. The Act also tightened the provisions with respect to correspondent accounts and other -- other tools that can be used by money launderers, particularly for the purposes of terrorism, and while the sentiment in the United States was probably moving away from tighter rules on anti-money laundering, September 11th was a watershed change and the President and the Treasury Secretary immediately embraced the notion of tighter rules for money -- anti-money laundering laws.

With that I'll turn it over to Mr. Mosley to discuss the Canadian anti-terrorism legislation.