Testimony of

Susan K. Gurley

Association of Corporate Travel Executives

Hearing on

Laptop Searches and Other Violations of Privacy

Faced by Americans Returning from Overseas Travel

United States Senate Committee on the Judiciary

Subcommittee on the Constitution

June 25, 2008

Chairman Feingold and distinguished members of this committee: I appreciate this opportunity to present the views of the Association of Corporate Travel Executives (ACTE) regarding the unrestricted authority claimed by the U.S. Department of Homeland Security (DHS) (including the U.S. Customs and Border Protection (CPB) and the Bureau of Immigration and Customs Enforcement (ICE)) to inspect, copy, or seize electronic devices – without provocation and/or suspicion – from any individual crossing a U.S. border. The seizure of laptops and other electronic devices is real and is not mere speculation.

ACTE at www.acte.org is the leading non-profit trade association providing education to the corporate travel industry. ACTE represents the safety, security, and service interests of all business travelers, and the financial concerns of more than 2,500 members from 82 countries, including the United States. ACTE's members represent an aggregate of $300

billion (USD) in annual business travel expenditures and include companies listed in the Fortune 1000 and Global 500. Business travelers contribute 65 percent of all airline revenue and represent the core customers of the hospitality industry in every major U.S. city.

ACTE's member companies have hundreds of thousands of travelers in the air at any given time. They routinely cross U.S. borders. ACTE represents billions of dollars in travel-generated taxes and many times that amount in direct expenditures, which support U.S. and global commerce. Even by a conservative estimate, this trickle-down effect of ACTE members on the overall American economic infrastructure is substantial. Moreover, it cannot be measured in dollars alone, but in jobs, innovation, corporate growth potential, company reinvestment, and ultimately stock value. The business traveler is a critical part of the U.S. – and the world's – economic future. The successful, seamless flow of business travel is critical to the American business profile and its influence in the global marketplace.

All international and U.S. business travelers who cross U.S. borders have two things in common: all carry electronic devices such as laptops, cell phones, Blackberries, iPods, and flash drives; and all are currently subject to the claimed authority of CBP or ICE officials to inspect and seize these electronic devices without provocation, suspicion, or warrant.

You will hear a number of compelling arguments today that these electronic devices are an extension of an individual's personal expression. You may also hear how the lack of established, published inspection procedures may lead to "profiling." Both of these are valid points. I am here to advise you that the unjustified retention and/or copying of proprietary and sensitive business information pursuant to the warrantless seizure of laptops and other electronic devices imposes both a personal and economic hardship on business travelers and their corporations.

In today's wired, networked and borderless world, one's office no longer sits within four walls or a cubicle; rather; one's office consists of a collection of mobile electronic devices such as

a laptop, a Blackberry/PDA, and a cell phone. It is common for business travelers to carry laptops and other electronic devices that contain both personal information (including health and financial records, addresses, etc.) and confidential business-related information (e.g. business plans, internal memoranda, contracts, passwords, and data). These devices constitute the office of today.

Under the U.S. Constitution, a warrant is needed to search a physical space, such as an office. Yet, the warrantless and unanticipated seizure of one's mobile office has been allowed to occur and can immediately deprive an executive or company of the very data – and revenue – a business trip was intended to create. As a businessperson returning to the U.S., you may find yourself effectively locked out of your office indefinitely and thereby deprived of the resources required to sustain your livelihood. Other rights are at stake as well. For example, the confiscation and downloading of a lawyer's client-related information could potentially violate attorney-client privilege. Similarly, the copying of a journalist's notes and interviews can impact the confidentiality of his/her sources and have a chilling effect on sources' willingness to speak to journalists.

There have been cases where information or hardware has been seized indefinitely, representing at a minimum a loss of the cost of the equipment either to the company or to the traveler. In the case of an independent entrepreneur, a laptop seizure can represent the loss of his or her entire business.

It can be argued that the percentage of seized computers and data is small in comparison to the total number of travelers crossing the border. However, because of a lack of transparency, the actual number of laptop seizures and the concurrent data downloading and potential data breach is not known to the public. ACTE surveyed its members in February 2008 on this issue; of the 100 people who responded, 7 reported that they had been subject to the seizure of a laptop or other electronic device. The survey also revealed that eighty-

one percent of survey respondents were unaware that the information on laptops and other electronic devices could be mirrored and held.

Even though the total number of business travelers subject to these searches and seizures can only be estimated, what is certain is the severe economic and behavioral impact that can follow when a laptop is seized. Some of the financial loss comes as a professional stigma associated with the seizure of one's laptop. Fifty percent of the respondents to ACTE's February 2008 survey indicated that having a laptop seized could damage a traveler's professional standing within a company.

Another concern is the lack of published U.S. government policies and DHS regulations that inform the public as to the government security measures in place to protect data when it is downloaded, who will have access to this information, how long the information can be stored and where it is stored, and how it will eventually be disposed of. The Government Accountability Office does not give high marks to the U.S. Department of Homeland Security and/or the U.S. Transportation Security Administration for data protection. The seizure of data or computers carrying corporate sales strategies, business plans, pending patents, or other sensitive proprietary information, could force these companies to implement new and expensive internal travel policies to counter potential data leaks and/or seizure.

In fact, this is already happening. Measures that companies are taking include sending data to themselves via web-accessible email, encrypting files, or using secure USB drives. In addition, companies are purchasing additional computers that are scrubbed of any prior emails so that they can easily be replaced. Furthermore, it is our understanding that some senior executives are prohibited from carrying any computers. All of these measures and business behavior changes cost time and money.

The title of this hearing is: "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel." But the fact is that laptops are also being

seized without recourse from foreign businessmen, journalists, and others – who are not U.S. citizens – without justification. ACTE is here to represent their interests as well.

According to a March 2008 release from the Travel Industry Association, "the United States welcomed 9 million fewer overseas visitors in 2007 than it would have if it had simply kept pace with post-9/11 worldwide long-haul travel trends. This decline has a serious economic impact resulting in a loss of billions of dollars of new visitors spending." This decline includes fewer foreigners attending conferences, meetings, and conventions in the U.S. ACTE believes that part of this decrease is due to the perception that the U.S. has withdrawn its welcome mat and made it difficult for visitors to come to the U.S. The U.S. cannot afford to be viewed as unwelcoming and thereby lose an opportunity for a visitor to attend a meeting for the first time in the U.S. and have a positive U.S. experience. The concurrent worry that their laptop (or other electronic equipment) may be seized and their personal, financial, health, and/or business information downloaded, adds to the perception that the U.S. is no longer a welcoming country.

In the June 11, 2008 edition of USA Today, a front-page article discussed the fact that the U.S. government is warning U.S. visitors to the Beijing Olympics that their laptops are likely to be penetrated by the Chinese government aiming to steal trade and business related secrets. Yet the U.S. government effectively does the same thing by seizing computers or electronic data, without explanation, and without apparent safeguards. Does the U.S. want to be perceived in the same light as the Chinese government when it comes to downloading information from laptops?

ACTE urges Congress to clarify border procedures – especially those entailing laptop seizures and the inspection of proprietary and personal data. We understand and support reasonable measures to protect the integrity of the U.S. border and the safety of its people. However, we believe these objectives can be met without sacrificing due process of law.

This might entail legislation to require, at a minimum, "reasonable suspicion" to search or seize electronic devices and their electronic files.

Finally, we are requesting improved and transparent communications from DHS (including ICE and CBP) regarding the policies and safety measures that they have in place to protect downloaded data and/or seized laptops in cases where the legal standard for seizure is satisfied. We request that the Committee undertake the following:

- Request a privacy impact assessment from the CPB on the number of seizures of laptops or other electronic devices; the minimum, average, and maximum amount of time that it takes to return the laptop and or other electronic device to the owner; and the reasons for the seizures.

- Require that the policies regarding laptop seizures be published by DHS in the Federal Register and on the agency's home page under quick links (http://www.cbp.gov/xp/cgov/travel/). This would allow any traveler to go to the site and know his/her rights. These policies should include, at a minimum, the following:

    - Policies for protecting the integrity of the data;

    - Policies for the length of time seized data will be stored and where and how it will be stored;

    - Policies for whether the downloaded information will be shared and, if so, with what other U.S. government and international agency(s) and under what circumstances;

    - Policies for who within the federal government will have access to the information;

- Information as to what rights a traveler has to ensure that his/her laptop and/or other electronic devices are returned; and
- A requirement that a receipt be given immediately to anyone whose laptop is seized with information regarding whom to call for information about the seizure.

Ultimately, ACTE would like Congress to consider laptops and other electronic devices as an extension of an individual's personal and professional identity and uniquely different from other forms of baggage.

In conclusion, I would ask the members of this committee to consider the following analogy. The hearing today is taking place in a federal building. All visitors meeting with their Senators are subject to a possible search and some kind of inspection. Suppose that search was extended to include the contents of all cell phones, Blackberries, and other electronic devices. Suppose too that the electronic devices constituents brought with them were seized and copied. Would you allow the seizure of your constituents' property and data, perhaps indefinitely, without a warrant and/or justification? This is essentially what is happening to our constituents – who are also your constituents – at the U.S. borders.

The Association of Corporate Travel Executives would like to thank Chairman Feingold and this committee for responding to an issue that will have long-term implications for corporate America, the international traveling public, and the global economy. The resources of our association are at the disposal of this committee and DHS and its Border Protection authorities.