STATEMENT OF PROFESSOR PETER P. SWIRE
C. WILLIAM O'NEILL PROFESSOR OF LAW
MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY
SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS ACTION FUND

BEFORE

THE U.S. SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS & PROPERTY RIGHTS

ON

"LAPTOP SEARCHES AND OTHER VIOLATIONS OF PRIVACY FACED BY AMERICANS RETURNING FROM OVERSEAS TRAVEL"

JUNE 25, 2008

Chairman Feingold, Ranking Member Brownback, and members of the Committee:

Thank you for the invitation to testify today on "laptop searches and other violations of privacy faced by Americans returning from overseas travel." In recent months I have become increasingly aware of what I consider a deeply flawed policy. The U.S. Customs and Border Patrol ("CPB") now takes the position that it can seize and copy the contents of a laptop or other computing device for a traveler entering the U.S., based simply on its authority to do traditional border searches.

The government seems to believe that, if they can open a suitcase at the border, then they can open a laptop as well. This simplistic legal theory ignores the massive factual differences between a quick glance into a suitcase and the ability to copy a lifetime of files from someone's laptop, and then examine those files at the government's leisure.

This issue has come into sharp focus since the April decision of the Ninth Circuit Court of Appeals in *U.S. v. Arnold*. That panel clearly ruled that CPB can seize a laptop computer at the border, and examine its contents, without any reasonable suspicion of unlawful activity. Affidavits in that case and other credible reports show that agents at the border are going further -- they are requiring travelers to reveal their passwords or encryption keys so that government agents can examine the full content of the laptop or other computing device.

Other witnesses today will go into depth about crucial objections to these laptop border searches, including constitutional prohibitions under the First and Fourth Amendments, ethnic profiling, and severe impact on commercial and individual travelers who are forced to reveal confidential records to the government.

My focus is different, drawing on my personal involvement in the encryption policy battles from a decade ago. My thesis is that laptop border searches bear a striking similarity to the federal encryption policy that was attempted during the 1990s but reversed in 1999. My testimony presents a brief history of these "crypto wars," as they were called. In particular, the testimony describes the so-called "Clipper Chip," where the government hoped to gain the encryption keys in advance for telecommunications devices. The testimony then examines eight precise analogies between the failed encryption policy of the 1990s and laptop border searches. For each of the eight critiques, the testimony explains how the critique applied to encryption policy and how the same argument applies to today's border searches:

1. Traditional legal arguments apply badly to new facts about computing
2. Government forces disclosure of encryption keys
3. Severe violation of computer security best practices
4. U.S. policy creates bad precedents that totalitarian and other regimes will follow
5. Severe harm to personal privacy, free speech, and business secrets
6. Disadvantaging the U.S. economy
7. Political coalition of civil liberties groups and business
8. Technical futility of U.S. policy

Since I became aware of the issue of laptop border searches I have spoken to an array of businesspeople, computer security experts, civil liberties advocates, and ordinary people who hear what the government is doing. The reaction has been uniform: "The government is doing *that*? They are just stopping people at the border, opening people's laptops and making copies of what's inside? It could happen to anyone, even if they've done nothing wrong? That is simply not right."

I hope today's hearing will be an important step toward curbing the current practices.

Background

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow with the Center for American Progress Action Fund. I live in the Washington, D.C. area. My education includes graduating summa cum laude from Princeton University and a J.D. from the Yale Law School.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that role, I was responsible for coordinating administration policy on public- and private-sector uses of personal information, and served as point of contact with privacy and data protection officials in other countries. During this time, along with many other activities, I participated in the process that resulted in a new administration policy for encryption in September, 1999. In 2000, at the request of Chief of Staff John Podesta, I chaired a 14-agency White House task force on how to update government surveillance laws for the Internet age.

Since leaving OMB, I have worked and written on a very wide variety of privacy and computer security issues. For instance, I testified before this Committee in 2007 about problems with the use of National Security Letters by the Federal Bureau of Investigation. I am Faculty Editor of the "Privacy Year in Review" issue of *I/S: A Journal of Law and Policy for the Information Age*, which is distributed to all members of the International Association of Privacy Professionals. My testimony and other writings appear at www.peterswire.net and www.americanprogress.org.

First and Fourth Amendment Analysis of Laptop Border Searches and Apparent Lack of Administrative Safeguards

This hearing was prompted in large measure by a decision by the 9th Circuit in April of this year, in the case of *Arnold v. U.S.*[1] Earlier federal cases had upheld laptop searches at the border, typically finding there had been "reasonable suspicion" of the individual, which means specific and articulable facts that led the government official to have a basis for carrying out the search. In the *Arnold* case, the district court found no "reasonable suspicion" for doing the search. The district court thus suppressed evidence discovered after a detailed search of the laptop. A Ninth Circuit panel reversed. It found, incorrectly in my view, that the CPB can do a comprehensive search of a laptop at the border without any reasonable suspicion of the individual.

Affidavits in the *Arnold* case and other reports indicate that, at least in some cases, CPB has seized a laptop at the border and returned it a week or more afterwards. The reports are that individuals are told, in addition, that they have to provide the government their passwords and encryption keys in order for the government to able to read the files in the computer. Failure to cooperate, travelers are told, is a basis for denying entry into the U.S.

I invite the Committee to consider how this sort of seizure, perhaps done without any individualized suspicion, would affect your work and your peace of mind -- having your laptop taken away from you, with no assurance you will get it back, and with the knowledge that the government could make a complete copy of the contents for analysis at its leisure.

I disagree with the Ninth Circuit, and agree with the position of the Electronic Frontier Foundation that the Fourth Amendment should be found to require at least a "reasonable suspicion" before doing an intrusive search of a laptop or other computing device at the border. The amicus brief filed in the *Arnold* appeal on behalf of EFF and the Association of Corporate Travel Executives lays out the legal arguments in considerable detail. Because I have reviewed these materials, and agree with them, I do not repeat the analysis here.

There are also serious issues under the First Amendment created by the seizure and copying of a person's laptop at the border. A laptop contains an enormous amount of expressive activity, potentially including confidential journalist notes, criticism of the Department of Homeland Security, and an almost unimaginable range of other content. The First Amendment aspects of privacy and searches have recently been examined by law professors Katherine Strandburg[2] and Daniel Solove,[3] and I commend those analyses to the Committee's attention.

Although I believe the Ninth Circuit decision is incorrect under the First and Fourth Amendments, **the Congress could take action to provide safeguards against overly intrusive searches** of laptops, other computing devices, and other examination of First Amendment-protected content at the border. **Similarly, Customs and Border Patrol, acting with the Privacy Officer and Civil Liberties**

Officer of the Department of Homeland Security, could create administrative safeguards to minimize the intrusiveness of searches of this sort of sensitive content. Because CPB has refused thus far to release any information about its practices, we do not know if any administrative safeguards are currently in place.

An important first step should be for the Department of Homeland Security to conduct a Privacy Impact Assessment of the procedures for conducting such searches. This sort of Assessment could address important issues such as: threshold for when content searches take place; protections against ethnic profiling and other improper targeting of travelers; minimization procedures for any data collected from searches; logging and audit procedures for such searches; and strict limits against any non-customs-related use of data collected from such searches. These sorts of administrative safeguards are an essential initial measure to control intrusive laptop searches and reassure lawful travelers that crossing the border will not be made an excuse for government surveillance of our entire universe of expressive activity.

Why Laptop Border Searches are Like the Failed Encryption Approach of the Clipper Chip Era

The main point of my testimony today is that laptop border searches have a precise analogy to a previous, failed government effort to impose surveillance on computing. During the 1990s, the federal government attempted to regulate the spread of effective encryption for communications over the Internet. Federal law made it illegal to export "strong" encryption -- encryption that could not be easily broken. Most notoriously, the federal government proposed the "Clipper Chip." This chip, built into communications devices, would have provided the government with the encryption keys for communications, so that the government could automatically break the encryption once it had a court order. The "Clipper Chip" came to stand for a broader government attempt to get the encryption keys for private use of encryption, a practice known as "key escrow."

The testimony here gives a common-sense history of this technical area of encryption regulation. For purposes of today's hearing, my point is that laptop border searches are the Clipper Chip all over again. The same criticisms that applied a decade ago to the Clipper Chip specifically, and federal encryption policy more broadly, apply to laptop border searches today.

A decade ago, the flawed federal encryption policy alarmed a wide coalition of business, computer security, privacy, human rights, and many other groups. A large and bipartisan movement arose in Congress to object to the administration policy. This coalition confronted federal law enforcement and national security agencies in what came to be known as the "crypto wars." As shown by the witnesses at today's hearing, the same coalition is beginning to emerge with respect to border laptop searches, and for the same reasons.

As a law professor who wrote about encryption and later as a government official, I was personally involved in the encryption debates. I draw on that experience now to underscore the bad policy and ultimate futility of today's policy of laptop border searches.

Summary of the crypto wars. The crypto wars were widely covered in the press, and the history is told in great deal in writings such as Steven Levy's 2002 book Crypto.[4] I will give just enough of that history to indicate the reasons for concluding that border laptop searches are a close analogy.

Encryption roughly means the process of transforming text to make it unreadable (or very difficult to read) for anyone who does not possess the key for reading the text. Throughout history, encryption was the special province of governments, which kept close control over encryption techniques for military and diplomatic advantage. Two changes occurred by the early 1990's, however, that made encryption far more important to individual and commercial users. First, the Internet began its spectacular growth, especially after commercial activity was authorized on the Internet in 1993. Second, a fundamentally new approach to encryption -- called "public key encryption" -- became widely available. This sort of encryption allows effective encryption to occur even among geographically-separate people who have never met before. With public key encryption, you wrap your message in my "public key" that is posted publicly, and you send it to me. I then unwrap the message using my "private key" and the message has thus been transmitted securely.

Users of the Internet, including the first E-Commerce companies, recognized that strong encryption was essential to the growth of the Internet. E-mails and other traffic on the web rely on "message forwarding" -- my message to you is forwarded through multiple servers, operated by unknown and perhaps malicious owners. If we send our messages in plain text, then those intermediate servers can read the content, make copies, and cause untold problems. To take a simple example, it is a really bad idea to send a payment for $1 million in unencrypted form. One of the intermediate server owners could then make copies, try to cash that $1 million before the legitimate recipient can, and perhaps try to cash it multiple times. Similar problems can arise for non-commercial users, such as human rights groups overseas that are using the Internet to blow the whistle on human rights abuses.

The correct technical solution is strong encryption. Using public-key encryption, a user anywhere in the world can securely send a message to a recipient anywhere in the world. Commercial users, human rights groups, and anyone else thus has a straightforward way to avoid the insecurity that otherwise would exist for every message sent through the Internet.

The problem in the 1990s was that national security and law enforcement agencies vehemently objected to the new encryption technology. The National Security Agency (NSA) had the responsibility of intercepting and reading electronic communications outside of the United States. The NSA was deeply concerned that its collection would "go dark" if strong encryption became the norm. Within the U.S., the Federal Bureau of Investigation was concerned that strong encryption would undermine its ability to conduct wiretaps and read computers when seized. At the time, the main legal tool for the government was a set of rules prohibiting the export of most encryption outside of the United States. Although strong encryption was still permitted within the U.S., it was considered export of a dangerous "munition" to send effective encryption software to other countries.

The clash between the opposing views led to a proposed "compromise" in 1993 called the Clipper Chip. Proponents hoped that their approach would allow government surveillance to proceed effectively even as the private sector used encryption widely. Clipper Chip depended on "key escrow" -- the idea that the government could gain access to a database of encryption keys when a proper wiretap order or other legal basis existed. For supporters of Clipper Chip, this approach would maintain the traditional government ability to conduct a wiretap where the court order was in place. Supporters of Clipper Chip argued that the system would be trustworthy because the government would access the database of keys only with proper legal authority.

The reaction to the Clipper Chip was intense opposition from E-Commerce and other businesses, privacy and civil liberties groups, and a phalanx of computer security experts. I believe the computer

security criticisms were especially effective -- the Clipper Chip would mean deploying a known flaw widely in our communications system; the key escrow database was a single point of failure which, once breached, would compromise an enormous array of communications; and the "trust us" model (the idea that we should trust the government with our encryption keys) was not good enough given the U.S. and other governments' weaknesses in computer security.[5]

These technical criticisms of the key escrow were picked up by an increasingly effective political coalition of civil liberties and business groups. A growing chorus of criticism came from the Congress. By 1999, over 250 members of the House of Representatives had signed onto the Security and Freedom Through Encryption ("SAFE") Act, and opposition to the administration in the Senate was led by a bipartisan coalition featuring the unusual pair of John Ashcroft and John Kerry.[6] The proposed legislation would have blocked the key escrow approach, by which government would gain control of encryption keys, and would have opened up exports of strong encryption for E-Commerce and other purposes.

During this period there were intense discussions in the executive branch about how to proceed on encryption policy. Along with many others, I participated in this process, and I know that the computer security vulnerabilities caused by key escrow were intensively discussed. On September 16, 1999 the Clinton Administration announced a major shift in encryption policy, putting the U.S. on a path toward lifting most controls on the export of encryption. In my role as Chief Counselor for Privacy, I had the honor of speaking at the White House event announcing the change in encryption policy:

> I am here to underscore that today's announcement reflects the Clinton Administration's full support for the use of encryption and other new technologies to provide privacy and security to law-abiding citizens in the digital age. The encryption measures announced today properly balance all of the competing interests, including privacy, electronic commerce, and public safety. Encryption itself is a privacy and security enhancing technology. Especially for open networks such as the Internet, encryption is needed to make sure that the intended recipients can read a message, but that hackers and other third parties cannot. Today's announcement will broaden the use of strong mass market encryption for individuals and businesses.[7]

After the 1999 announcement, the use of strong encryption on the Internet and more generally was clearly established. Strong encryption, including for export, has remained legal since that time.

The Analogy Between Laptop Border Searches and the Encryption Policy of the Clipper Chip

The testimony now turns to the eight comparisons between the encryption policies of the 1990s and laptop border searches today:

1. Traditional legal arguments apply badly to new facts about computing
2. Government forces disclosure of encryption keys
3. Severe violation of computer security best practices
4. U.S. policy creates bad precedents that totalitarian and other regimes will follow
5. Severe harm to personal privacy, free speech, and business secrets
6. Disadvantaging the U.S. economy
7. Political coalition of civil liberties groups and business
8. Technical futility of U.S. policy

1. Traditional legal arguments apply badly to new facts about computing

In the crypto wars, the government relied on legal tradition -- wiretap orders historically were issued by judges, and such orders enabled the government to listen to the content of phone calls and other communications. Similarly, search warrants were issued upon probable cause, allowing physical access to computers. In the eyes of law enforcement officials, the Clipper Chip and other key escrow measures were needed in order to maintain the status quo. Without key escrow, in their view, wiretap orders and search warrants would often be frustrated by the technique of encryption. For many in government, it thus seemed obvious common sense to maintain the status quo of effective government access to information, once the wiretap order or search warrant had been issued.

Opponents of government regulation responded, effectively in my view, that key escrow was an unprecedented measure that did not recognize the fundamental facts of modern computing. In the physical world, we do not give the keys to our front doors to the government. Key escrow was unprecedented because of its requirement that each person affirmatively hand over the key in advance. In addition, key escrow would enable an unprecedented scale and scope of government surveillance. Key escrow in communications would enable access to the vastly increased flow of information enabled by the Internet, modern computers, and the reduction in the cost of telecommunications. Key escrow access to our physical computers would allow one-stop surveillance of a person's enormously detailed computer files.

Turning to laptop border searches, the government relies once again on a traditional legal argument. The government points out that there is a long history of physical searches when a person crosses the border, so there is nothing new at all about physical searches of laptops and other modern computing devices. Their legal argument roughly says: "Nothing to see here; move along."

As with key escrow, however, there is something to see here. The government's position essentially is that they can make the traveler open a suitcase, so they can make the traveler open a laptop. A modern laptop, however, holds exponentially more material than a physical suitcase. The 80 gigabytes of today' standard laptop could likely hold all the books printed in human history up through sometime well into the 20th century. Not only does the government get access to an unprecedented wealth of material with a laptop border search, but the government now has the ability to copy, store, and analyze that information at its leisure. Government agencies have access to the "Computer Online Forensic Evidence Extractor," a thumb drive designed to quickly extract and copy a complete image of a laptop or other computer.[8] In traditional border searches, travelers carried their suitcases with them once they cleared customs. With laptop border searches, the government can keep everything in the computer in perpetuity. With key escrow, the government position was "trust us" not to look at all the communications it could read. With laptop border searches, the government once again says "trust us" with all the data it can read.

2. Government forces disclosure of encryption keys

A central front in the crypto wars was whether users would be required to disclose their "private keys" to the government. As described above, the system of public key encryption was coming into common use as the Internet grew in the late 1980s and early 1990s. With public key encryption, you wrap your message in my "public key" that is posted publicly, and you send it to me. I then unwrap the message using my "private key" and the message has thus been transmitted securely.

For people who did not live through the encryption debates of the 1990s, it is probably hard to imagine how strongly many computer security experts feel about revealing their private keys. A quote from John Perry Barlow, co-founder of the Electronic Frontier Foundation, helps provide insight. Responding to a key escrow proposal, Barlow said: "You can have my encryption algorithm, I thought to myself, when you pry my cold dead fingers from its private key."[9]

For laptop border searches, the government is once again demanding that individuals and businesses turn over their passwords and encryption keys. Travelers are given the "choice" of handing over their keys or else being refused entry into the country. Because disclosure of encryption keys was such an intense flash point in the 1990s, the Customs and Border Patrol policy of demanding encryption keys may well prove far more controversial than its officials have realized.

3. <u>Severe violation of computer security best practices</u>

In the encryption debates, computer security experts played a central role in explaining why key escrow proposals would undermine secure communications for all applications on the Internet. In a world where people were routinely communicating across borders, it was vital to use strong encryption to conduct communications and transactions in a secure way.

A decade later, computer security has become an even greater priority in light of our experience with problems such as spam, spyware, viruses, and other sorts of malware. Computer hacking has evolved from its prankster roots into an organized business, featuring large "bot farms" that allow organized crime to launch large and effective attacks through computers they have infected. Federal agencies and major corporations have been repeatedly hacked, amidst growing reports of cyberattacks from overseas, some of them likely with government support. There have been growing reports of "root kits," where outside software gives hackers access to the "root" or fundamental control of the computer.

Data breaches have been a top story in the area of computer security. Most states have passed laws requiring notices to consumers about data breaches, and the Privacy Rights Clearinghouse has documented over 226 million data records of U.S. residents that have been exposed due to security breaches since 2005.[10]

In response to these daunting challenges, responsible corporations and individuals have instituted much stricter computer security. Users outside of the company are generally strictly forbidden from gaining access to the computer and its files. Controls are installed to make it harder to copy data through thumb drives and other external devices. Many corporations have instituted training and other procedures to reinforce the importance of not exposing the company's data to outsiders.

In response to the problem of data breaches, corporate America is rapidly shifting to a norm of encrypting the hard drives of laptops and other computers. The reason is that data breach laws have an exemption from notice where the data is encrypted. Once the hard drive is encrypted, the company saves the expense and problems of notice even if the laptop is lost. Another reason for the shift to hard-drive encryption is that Vista and other recent software makes it more user-friendly to routinely encrypt files in a laptop.

In this environment of heightened computer security, laptop searches at the border are a direct and flagrant violation of industry best practices. Private encryption keys are not supposed to be disclosed, but CPB demands those keys. Thumb drives and other devices for copying large amounts of data are routinely disabled, yet CPB mirrors the entire hard drive full of corporate or individual data. Turning over the computer to the government, with passwords and encryption disabled, also exposes the computer to the risk of root kits and other malware -- the computer cannot be treated as a trusted platform under industry best practice once it was been opened wide to a third party such as the government.

4. U.S. policy creates bad precedents that totalitarian and other regimes will follow

If the United States adopts a policy, then it is generally much harder for the U.S. to object if other countries adopt a similar policy. This problem arose with the key escrow approach to encryption. Even if you trust handing your encryption keys to the U.S., would you feel the same way handing the keys to all your communications to a totalitarian regime? A common theme in the encryption debates was that numerous countries would want to follow the U.S. lead and gain access to encryption keys, with many negative effects on commerce, free speech, theft of trade secrets, and so on.

The same applies to laptop border searches today. I explained just now why divulging passwords and encryption keys at the border violates modern security practices. Perhaps many of us would trust the Customs and Border Patrol itself, especially if careful procedures and audits were developed to protect against the risk of breach or mis-use of data. The problem would remain, however, that totalitarian and other countries would quite possibly imitate the U.S. border policy. For Senators and their staffs, would you want the entire contents of your laptops revealed to foreign governments? If Senators and their staffs are subject to such searches in the future, then the ability of the U.S. government to object will be at low ebb. By contrast, thoughtful policies for U.S. border searches, including being based on reasonable suspicion or probable cause, would provide a much more effective basis for the U.S. to object to overly intrusive border searches by other countries.

5. Severe harm to personal privacy, free speech, and business secrets

For reasons already described, the key escrow approach to encryption threatened severe harm to personal privacy, free speech, and business secrets. Privacy was threatened because the government kept the keys that enabled it to listen to any communication. Free speech was chilled because of the concern that the U.S. or any other government would be listening. Business secrets were at risk, and the security of business transactions was threatened, because the Internet was being based on insecure technology rather than strong encryption.

The same applies to laptop searches at the border. The Electronic Frontier Foundation and the Association of Corporate Travel Executives, on their websites, describe many of the scenarios that make such searches especially intrusive. For personal privacy, an individual's laptop may well contain diaries, love letters, a lifetime of saved email, private photos, passwords, financial and medical records, and evidence of almost any other intimate part of life. The text of the Fourth Amendment protects "persons, houses, *papers, and effects*." (emphasis supplied) This constitutional text highlights the Framers deep concerns about personal papers and related documents. There is a long history in the Supreme Court of granting especially strong protection to diaries and similarly personal papers.[11] Even if such "papers and effects" do not gain absolute protection under current Fourth Amendment doctrine,

this long history of concern should inform our government's policy toward searching through an individual's lifetime trove of personal papers.

Intrusive laptop searches by the U.S. and other governments would similarly chill free speech. One vivid example is a human rights activist entering or leaving China, perhaps on a religious or other mission that is controversial in that country. More generally, laptop searches make a trip across the border a potentially scary moment when legitimate First Amendment speech can be placed in a government database, with no known limits on how the computer files are saved and used. For example, someone in the opposite political party from the President could worry that campaign plans and other political activities would be copied and saved by the Department of Homeland Security. The government may say that they would not do such things, but the lack of legal safeguards once again means that we must simply trust the government not to mis-use its power.

The harm to business secrets from laptop searches is similarly substantial. The harm begins with the security violation of revealing passwords and private encryption keys; if the passwords or keys are used in any other settings in the company, then changes must be made in all of those other settings or else the system is exposed to additional intrusion. Others have catalogued other costs and problems that business confronts: exposure of trade secrets; compromise of the attorney-client privilege for material viewed by third parties; journalists' notes that would be protected by shield laws; and others. At the very least, businesspeople face the risk that their business will be interrupted by government taking of their laptop or PDA, even if "only" for a week or two. In the face of that risk, prudent businesses will increasingly have to resort to costly supplementary measures to ensure that important business information will make it past the border each and every time. Laptop border searches thus impose a new and costly tax on crossing the border.

6. <u>Disadvantaging the U.S. economy</u>

In the 1990s, it became increasingly apparent over time that U.S. encryption policy was harming the U.S. economy and advantaging competitors in other countries. The encryption limits specifically applied to exports from the U.S. to other countries. U.S. software and hardware companies were thus prevented from selling strong encryption to global markets. Over time, competitors in other countries, including Russia, started to sell high-quality encryption products and began to gain significant market share. A disadvantage of U.S. encryption policy was thus that sales that would have gone to U.S. companies were shifting instead to foreign competitors.

The same critique applies to laptop searches at the U.S. border. Foreign tourists will not like the idea of having their laptop inspected at the border, and may decide to visit elsewhere. International conferences and conventions will choose to locate elsewhere. Business travelers, at the margin, will decide to use teleconferences or otherwise skip the annoyance and risk of coming to the U.S. for a meeting. Laptop searches are one part of a broader issue about the extent to which the United States seeks to be open for business and open for tourism. Laptop searches send the signal that crossing the U.S. border may well be an unpleasant and intrusive experience. If laptop searches were vital to the fight against terrorism, then we might craft procedures to do them while minimizing the intrusion. The available cases, however, are not about terrorism-related investigations. For this reason, it may be useful for the Committee to ask the U.S. Department of Commerce to estimate the effects on the U.S. economy of laptop border searches.

7. <u>Political coalition of civil liberties groups and business</u>

The crypto wars featured an effective coalition of civil liberties groups and the business community. Civil liberties groups highlighted the negative effects of administration policy on privacy, security, free speech, human rights efforts, and other causes. The business community emphasized how encryption policy was negatively affecting growth of the Internet, putting trade secrets at risk, and disadvantaging American business at the expense of competitors overseas.

The hearing today shows that this same coalition is developing on the issue of laptop border searches. Testimony today comes from civil liberties groups such as the Electronic Frontier Foundation and Muslim Advocates, and a diverse and impressive set of civil liberties organizations have signed a letter objecting to current practices.[12] Also testifying today, as a sign of business concern, is the Association for Corporate Travel Executives. I can add, from my personal experience, that the current practices generate outrage and incredulity from a range of business executives and corporate security officers with whom I have discussed the issue. For instance, after I was asked to testify at this hearing, I raised the issue with a group of business people for global companies. They had been growing increasingly aware of the issue in the past year, and were contemplating a variety of expensive and inconvenient options for their companies, including prohibiting travel with normal laptops and instead issuing separate "travel computers" that would be thoroughly scrubbed before each border crossing.

Because the *Arnold* decision upholds intrusive laptop border searches, with no requirement of government suspicion, I believe the concern from both a business and civil liberties perspective will likely grow quickly. In the wake of the *Arnold* decision, there has already been increased discussion in technical circles on the web about what to do in the face of intrusive laptop searches. I hope this hearing will help avert the need for the large-scale and lengthy political mobilization that was required to reverse the worst aspects of encryption policy in the 1990s.

8. <u>Technical futility of U.S. policy</u>

One of the final arguments against U.S. encryption policy in the 1990s was that it was ultimately futile as a technical matter. The U.S. rules said it was illegal to export strong encryption, but it was impossible at a practical level to prevent transfer of encryption software from the U.S. to other countries, whether over the Internet or through the mail or physical delivery. In addition, over time, buyers outside of the United States were increasingly able to buy strong encryption from non-U.S. suppliers. The strict U.S. rules were ultimately repealed in part due to a recognition that they were simply not succeeding at preventing the spread of encryption.

Similarly, laptop searches will not succeed at a technical level at preventing data from entering or leaving the U.S. Computer security researcher Chris Soghoian in May posted a story called "Keep Your Data Safe at the Border."[13] Soghoian presents an eight-point checklist for how to get your data legally across the border without being searched. The primary trick is to send encrypted files to yourself once you get to your destination country.

The Soghoian article shows the futility yet burden imposed by laptop searches at the border. Any terrorist who is even moderately well informed can learn how to send the crucial files legally and safely across the border. In addition, a terrorist who is willing to lie to the customs agent (certainly a possibility worth considering) can use TrueCrypt or other software that does the following trick -- it allows you to encrypt a secret cache of data inside your encrypted hard drive. Then, when an investigator forces you to open your encrypted files, the secret cache remains invisible to the

investigator. This TrueCrypt approach requires lying to the custom agent about whether you have opened up all of your files, but it is a technical measure already available with widely-available software.

Although these approaches show the inability of laptop border searches to catch moderately smart criminals or terrorists, the approaches are costly and burdensome. Companies, civil society groups, and individuals who do not want their data read are forced to go through fairly complex contortions to prevent access by the government at the border. As with the crypto wars in the 1990s, a system that can be evaded by competent criminals but imposes large costs on honest citizens should be avoided.

In conclusion, I thank the Committee for the opportunity to address these important issues, and I would be glad to answer any questions.

---

[1] The briefs and other materials in *U.S. v. Arnold* are available at http://www.eff.org/cases/us-v-arnold.
[2] Katherine Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," 49 Boston College L. Rev. No. 741 (2008), available at http://ssrn.com/abstract=1136624.
[3] Daniel J. Solove, "The First Amendment as Criminal Procedure," 82 N.Y.U. L. Rev. 112 (2007), available at http://ssrn.com/abstract=924900.
[4] Steven Levy, Crypto: How the Code Rebels Beat the Government: Saving Privacy in the Digital Age (2002)
[5] The Center for Democracy and Technology assembled 11 of the leading computer security experts to write a report called "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption," (1998), available at http://www.cdt.org/crypto/risks98/.
[6] See "Summary of Encryption Bills in the 106th Congress," available at http://www.techlawjournal.com/cong106/encrypt/Default.htm.
[7] Transcript of Special White House Briefing on Encryption Technology, Sept. 16, 1999, available at http://seclists.org/politech/1999/Sep/0023.html.
[8] Benjamin J. Romano, "Microsoft device helps police pluck evidence from cyberscene of crime," Seattle Times, April 28, 2008, available at http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html.
[9] John Perry Barlow, "Decrypting the Puzzle Palace," (1992), available at http://www.matarese.com/matarese-files/5969/decryptingpuzzle-palace-john-perry-barlow-july-1992/index.html.
[10] Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[11] The leading Supreme Court case is U.S. v. Boyd, 116 U.S. 616 (1886). See Peter P. Swire, "*Katz* is Dead; Long Live *Katz*," 102 Mich. L. Rev. 904 (2004) (discussing the history).
[12] The letter, with signatories, appears at http://www.muslimadvocates.org/docs/Coalition_sign_on_letter_re_invasive_border_interrogations_--_SJC.pdf.
[13] Chris Soghoian, "Keep Your Data Safe at the Border," CNet, May 5, 2008, available at http://news.cnet.com/8301-13739_3-9935170-46.html.