DHS Says "Suspicionless Searches" of Laptops and Smart Phones OK at US Borders

February 8, 2013 - The Department of Homeland Security has issued a memo which states that they have the right to search any computer, smart phone or other electronic device being carried by anyone crossing a US border. No suspicious activity is required. Anyone planning on traveling outside of the United States should consider taking some precautions to protect their privacy and their information if they plan on taking a computer with them.

The memo, which was apparently release on January 29th, has not been release to the public. The ACLU has filed a Freedom of Information Act request to change that. But the executive summary of the memo is available and it speaks volumes. It includes statements such as:

- "ICE and CBP exercise longstanding constitutional and statutory authority permitting suspicionless and warrantless searches of merchandise at the border and its functional equivalent. Two public Directives issued in 2009 (CBP Directive No. 3340-049 â€œBorder Search of Electronic Devices Containing Informationâ€• and ICE Directive No. 7-6.1 â€œBorder Searc of Electronic Devicesâ€•) impose requirements governing use of this authority in searching, reviewing, retaining, and sharing information contained in electronic devices."

- We conclude that CBPâ€™s and ICEâ€™s current border search policies comply with the Fourth Amendment. We also conclude that imposing a requirement that officers have reasonable suspicion in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits.

- "[W]e conclude that the laptop border searches allowed under the ICE and CBP Directives do not violate travelersâ€™ First Amendment rights."

The bottom line here is that anyone traveling across a US border could very easily find their electronic devices being searched. And there have already been cases in which those devices have been seized and their owners subjected to rigorous questioning & short detentions.

Having your computer seized could be disastrous to anyone who uses it for business. It is not uncommon for travelers to bring customer databases and billing information with them when traveling. Lose your computer and you could be out of business.

But even you don't use your computer for business, you could wind up losing your pictures, your MP3 collection and all of your email. Not something that most people want to contend with. But there are precautions that you can take.

First, if it is affordable, consider getting a travel tablet computer and a throw away phone. Keep the information that you store on these devices to a minimum and back up your data online. If you have a program like GoToMyPC, you can actually transfer your data from these devices to your PC at home prior to coming back to the United States. Once you do that, you can delete any information that you store on your travel devices. On the off chance that DHS seizes them when you come home, you haven't lost any data.

If that option is cost prohibitive, then before you travel make sure you back up your computer and your phone to a device that will remain in the United States. There are a wide variety of online services that can be used for this purpose and the pricing is minimal. If you have an extra computer or hard drive at home, then you may be able to simply backup your computer to one of these.

Get a program to wipe out any deleted files on your travel computer and learn how to use it. When you delete a file, the data in the file actually remains on your computer until it is overwritten. But there are programs out there like EvidenceEliminator that will wipe these files out. They can also be setup to wipe out your browser history and any stored files downloaded from the internet. The best programs in this category not only overwrite old data but they will also encrypt portions of your drive using Department of Defense standards.

Seriously think about using an encryption program that has strong password protection such as PGP (stands for Pretty Good Protection). Some encryption programs will actually hide your data, allowing the computer to boot normally. Whoever is inspecting a system setup this way won't be able to see your files and will have no idea that they are actually missing much of the content on your computer. This also has the added benefit of protecting you if your computer is ever lost or stolen.

And finally, make sure that everything on your travel devices is legal before you go. Pirated software or illegal content could be enough to get you arrested when you come home. And you should know that some content protected by the First Amendment in the United States may be illegal in your destination country. Knowing this before you travel could be the difference between an enjoyable trip and a room where the view is blocked by bars.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS