

## Laptops and the USA

Members may have already seen the recent information relating to random searches of electronic devices by US Customs and Border protection staff, and others. This was further highlighted when a story broke in the media and senior representatives from BAE Systems (Mike Turner and Sir Nigel Rudd) were temporarily detained at Huston Airport, during the week of 12 May, and their laptops and Blackberry's were examined by the US authorities, as part of on-going investigations by the Department of Justice.

These reports confirm that US Customs and Border Protection (CBP) officials have the totally unfettered authority to search laptop computers, personal digital assistants, cell phones, thumb drives and other electronic devices at US borders **without** suspicion or probable cause, as permitted under existing authority. CBP is permitted to access and copy information stored and even seize the devices themselves. According to the internet: "The agency does not need to show a probable cause to look inside suitcases or laptops. It has broad search authority at the borders to determine admissibility and look for anything that may be in violation of criminal law."

It has been pointed out that such devices often contain confidential corporate and personal information that CBP would have the authority to access. The potential ramifications could include attorneys being forced to expose sensitive information about their clients, and executives being required to expose commercially sensitive data to CBP officials with no clear limits on what they can then do with it, including the fear that this could then be handed over to US-based competitors.

The Association of Corporate Travel Executives (ACTE) has issued a warning to all business travelers to limit proprietary information on electronic devices when crossing US borders, and to eliminate any personal data, including photographs, finances and email that you do not want examined by CBP officials. A 2008 ACTE survey indicated that over 80 percent of responding travel managers were totally unaware that laptops and other electronic devices could be confiscated indefinitely.

*"ACTE filed an Amicus brief contending that a traveler's laptop was essentially intellectual property and not the same as luggage nor freight," a spokesperson for the ACTE, has said. "The court has disagreed, and this decision will have significant impact on business travelers who have no idea their data is subject to search and seizure."*

There are, of course, a number of related queries that have been raised relating to devices such as laptops that have disc encryption, and what guidance to give travelers with respect to supplying the passwords for the encryption to the CBP. In particular, if the traveler refuses to provide the passwords one assumes the device will be seized, but there could also be other remedies against the individual. If you refuse to reveal the password, you are likely to have the equipment seized and be refused entry to the USA if on arrival, or prevented from leaving, if on departure.

Many companies are reported to have now instituted a policy restricting the amount of sensitive or proprietary data that could be carried on a laptop; that number is expected to grow.

General advice is:

1) Do not carry any confidential, personal information that you do not want examined by third parties on your electronic device(s);

2) Limit the amount of proprietary business information you carry on your electronic device(s);

3) If you also use your for personal reasons, then get another one for travel purposes;

4) Make sure that you have a clear accompanying letter from your company's export control compliance manager to state what is on your electronic device(s);

5) Go to the cost of having an adequate stock of dedicated, travel specific electronic device(s), whose hard drives are completely clean and can be loaded up with whatever is required for a specific business trip, for re-wiping upon return from any trip overseas;

6) For Blackberries, it is suggested that best practice should be for anyone going to/from the USA to delete **ALL** e-mails from the in-box of their Blackberries on arrival, and then again on departure, and de-activating the wireless facility (by scrolling down and clicking on the "Turn Wireless OFF" button), so that US Customs can see that there is nothing on it at all when you are going through US Customs on arrival/departure. Once you have gone through US Customs and are leaving the Airport, you can turn your Blackberry on again and turn on its Wireless facility to start receiving e-mails again.

The message appears to be "do not take a laptop to the USA if it has any data that is not already in the public domain!"

Full advice on bureaucratic requirements for travelling to the USA is available from Brinley Salzmann, at the DMA ([b.salzmann@the-dma.org.uk](mailto:b.salzmann@the-dma.org.uk)).