Eric A. Simmons

Robert Martin

Microsoft Windows 7: 70-680

25 January 2016

Check Your Digital Baggage

These days one would be hard pressed to find lucrative employment with a company that is not, to some extent, international. In order to maintain connections and communications, travel is inevitable. Living in the digital age requires much more planning than that of a 1970's business professional. Computers, cellular phones, and other mobile devices are more than just common place, they are somewhat essential. According to a study conducted by Flurry Analytics using data collected between January and March of 2014, the average American spent two hours and 45 minutes per day on a mobile device (Khalaf, 2014). With everyone leaning toward computers and mobile devices to pay bills, shop, and work on business projects, securing these devices and the information saved on them is paramount.

Traveling within the borders of the United States of America affords you certain limited rights to privacy, but when traveling abroad the laws vary greatly. For example, the USA's northern neighbors, Canada, may conduct searches of individuals entering the country including their baggage, parcels or devices such as laptops, blackberrys or cellphones. These searches can be conducted without warrants and the officers may examine a travelers photos, files, contacts, and other media (“Checking In”, 2014). The same is true of the United Kingdom and Australia (Hughes, 2014).

These laws can cause many travelers to be alarmed across several career fields. Consider any intellectual properties a designer might be proposing to a foreign branch, sensitive information being carried by a military service member, or simply intimate pictures belonging to

any traveler. With the necessity of international trips growing more prevalent in all industries, Information Technology professionals are being challenged with ensuring security of their employer's information while providing the users with sufficient access to the data and information resources they need.

The US Army has even published guidance on the use of commercial mobile devices. In the memorandum dated 11 September 2013, Lieutenant General Susan S. Lawrence states that an "Enterprise-Connected Device" is authorized to process and store up to Unclassified/For Official Use Only information and personally identifiable information (Lawrence, 2013). So it makes sense that a traveling military official would be less than excited to allow their device to be searched by foreign authorities.

In response to this concern, several companies use tools such as encryption software and the ability to wipe lost devices remotely. Additionally, there are more and more Virtual Private Network options becoming available to enable remote access to company resources. This can help to reduce the threat of compromised information since the data is not stored directly on the device. SSG Dick C. Funk, a U.S. Army Cyber Network Defender, also offered advice to travelers concerned about transporting their work and personal communication devices. He suggests utilizing "burner phones" and travel laptops and devices that only contain information needed for a specific trip. Subsequently, these devices can be securely wiped and reformatted for other trips. "You have to constantly do cost/benefit analysis and develop a threat matrix" (Funk).

Encryption of data is becoming a highly adopted standard, but it cannot protect you from searches by customs officials. While it protects your data should you lose your device, most countries have laws which mandate the disclosure of encryption keys on demand. A resistant traveler can see themselves charged with contempt of court in Canada or receive a maximum of two years in jail in the United Kingdom (Hughes, 2014).

The Electronic Frontier Foundation offers the following points to consider: your citizenship status; how much hassle you are willing to tolerate; how important it is to have access to the data while you travel; how good internet access will be; countries you plan to visit; and your history with law enforcement (Schoen, Hofmann, and Reynolds, 2011). These can all have a significant impact on the likelihood of you being searched and the impact a search can have on your travels.

In conclusion, every globetrotter should do the proper research and know their rights prior to takeoff. If taking a business related trip, ensure that you consult your IT administrator to get clear guidance on any applicable company policies. Always minimize risk to yourself and your employer and only bring what you need for that trip. If you wish to travel far and fast, travel light ("Cesare Pavese Quotes", 2016).

Works Cited

"Fact Sheet: Checking In - Your privacy rights at airports and border crossings" *priv.gc.ca*. Office of the Privacy Commissioner of Canada, Revised 26 June 2014. Web. 20 January 2016

Funk, Dick C. Personal Interview. 20 January 2016

Hughes, Matthew. "Smartphone & Laptop Searches: Know Your Rights" *makeuseof.com*. MakeUseOf, 14 August 2014. Web. 21 January 2016

Khalaf, Simon. "Apps Solidify Leadership Six Years into the Mobile Revolution." *Flurry Insights Blog*. Tumblr, 01 Apr. 2014. Web. 20 Jan. 2016.

Lawrence, Susan S. "US Army Guidance on the use of commercial mobile devices" *Department of the Army*. Office of the Secretary of the Army, 11 September 2013. Print

Schoen, Seth, Marcia Hofmann, and Rowan Reynolds. "Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices" *eff.org*. Electronic Frontier Foundation, December 2011. Web. 20 January 2016

"Cesare Pavese Quotes" *BrainyQuote.com*. Xplore Inc, 2016. Web. 25 January 2016