BARNES & THORNBURG LLP

A Little-Known Exception To The 4th Amendment: Is Your Company's Confidential, Proprietary Data Safe From Government Inspection When Entering The U.S.?

February 27, 2014 | | Privacy, The GEE Blog

You arrive home to the United States from an international business trip. Customs directs you to open your bags for an inspection. Unconcerned, you acquiesce. The Customs Agent goes through your bags and finds nothing of interest, except your work laptop. To your surprise, the Customs Agent asks you to turn it on. He randomly opens files and reviews their contents. To your further surprise, the Customs Agent informs you that he will need to temporarily confiscate your work laptop in order to conduct a forensic examination. He takes your computer and makes an image of all its contents. You think to yourself, "This *must* be a violation of my Fourth Amendment rights against unreasonable searches and seizure, right?" The answer: *maybe not*. A search warrant is not required if a law enforcement officer has the necessary probable cause to believe that there is criminal activity.

The U.S. Supreme Court has established that the Fourth Amendment's protections against unreasonable searches and seizures extends to electronic information contained on electronic devices, but there is one little-known exception to the Fourth Amendment's protections. Upon entering the United States, probable cause is not required to search individuals or to seize property. The "border search" exception may have dramatic commercial consequences for unsuspecting employees with confidential, proprietary data or trade secrets on their business laptops or other electronic devices. In the 1977 case *United States v. Ramsey*, the U.S. Supreme Court explained the border search exception to the Fourth Amendment. The Court deduced that the law distinguishes between the broad powers afforded Customs officials to search and seize goods and property coming into the country and the more limited authority of law enforcement to search and seize property within the country. In short, border searches are *presumed* to be "reasonable" simply because the individual is entering the United States from outside.

This exception to the Fourth Amendment also applies to travelers' electronic devices, but the extent of Customs' authority to search and seize electronic devices without reasonable suspicion is uncertain. Courts have acknowledged that the Fourth Amendment imposes some restrictions on the border search exception. Non-routine searches, such as physically intrusive searches or x-rays, require a heightened or "particularized" suspicion that criminal activity is occurring. But does temporarily confiscating and imaging a traveler's computer or electronic device constitute a "non-routine" search? Recent cases may provide some insight. In *United States v Cotterman* out of the Ninth Circuit, a defendant challenged a Customs Agent's forensic examination of his laptop. On appeal, the court confirmed that the government's power to search is "at its zenith" at the border, and the balance of interests is weighed heavily in the government's favor. However, it is not without limits. Although the Ninth Circuit ultimately determined that there was reasonable suspicion to justify the forensic analysis of the defendant's computer, the Court stated that the border search exception did not apply to seizures and forensic examinations of laptops because, "[t]he uniquely

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." Similarly, the Second Circuit in *United States v. Galpin* likened the search of a suspect's computer hard drive to searching their residence. The implication is that imaging and comprehensively analyzing the contents of an electronic device transcends the "reasonable" presumption afforded border searches. The Ninth Circuit and the Second Circuit are the only federal circuits that have addressed this issue, and there is no guarantee other circuits will reach the same conclusion.

What does this mean for companies that have employees who frequently travel abroad for business and may have confidential, proprietary data or trade secrets on their laptops or other electronic devices? It is not implausible to suggest, or even expect, that the government, upon imaging an employee's computer, may obtain and analyze data that should never be in the government's possession. Furthermore, there may be commercial implications in the event trade secrets are disclosed as a result of a Customs search and confiscation.

Customs regulations require a Customs Officer encountering business or commercial information in electronic devices to treat such information as confidential and protect it from being disclosed. But that does not protect the owner of such information from unintended disclosures by a government official. There are multitudes of ways to limit the potential harm caused by a border search. Simple steps, such as encrypting sensitive files, can help protect confidential data. Traveling employees might be instructed to forward proprietary data to their respective destinations and removing the forwarded data from their electronic devices prior to entering into the country.

Regardless of the protective measures employed, companies with employees who travel internationally should be aware of the border search exception to the Fourth Amendment, and consider proactive steps to protect proprietary data that may be contained in employees' electronic devices.

* *Neal Brackett provided assistance with this article*