Business Travel Security Holes – and How to Plug Them

BY ROBERT D. BROWNSTONE, ESQ.

Fenwick

FENWICK & WEST LLP

An oxygen-sucking hole ripped in an airplane's ceiling — though quite grave and potentially hazardous — should not be the only leakage concern of business travelers. Thunderous voices, loose lips, wandering eyes, lost portable devices and aggressive Customs officers are just some of the many circumstances that can compromise the confidentiality or privacy of information.

As a frequent traveler who also often advises clients and colleagues on information-security and data-leakage, I am hyper-sensitive – OK, call me just plain hyper. Over time, I have devised a series of routines to guard against disclosures of: client confidences and identities; my law firm's proprietary secrets; and private information relating to me and my family. Hopefully, whatever your walk of life, you will find these ensuing tips instructive. Do try them at home.

As soon as you leave your office or home, security measures should kick in. The first rule of thumb is one I learned from the former prosecutors with whom I first practiced law, back in the pre-smart-phone 1980's in New York City. They taught me about "location, location, location," namely that, when, out in public, never mention names of companies or individuals represented by you or involved in any way in a confidential matter on which you are working. I distinctly remember one of my mentors Bill Purcell (a former Manhattan D.A.) reminding me each time we got into a cab to go to court or a deposition to be careful. Bill would calmly mention something to the effect that "who knows who will hop into that taxi next and strike up a conversation with our cabbie." Then, we would transition into "code name" mode. If we had to talk about a case, we would refer to key players as "Mr. C" or "Ms. M" and omit as many atmospheric and factual details as possible.

Once on the way to one's destination, in today's high-tech world people's loose-lips tendency seems to have been exacerbated by the ever-present cell-phones – and even more so by the apparently requisite high volume of speech that accompanies use of same on a bus, train or plane. In the recent annals of publicly loud law-firm partners, there are now such widely recognized characters as "Amtrak Bob" and "Acela Jim." Each of them chatted noisily on a crowded train about a highly confidential personnel situation involving his respective law firm. According to news reports, Bob disclosed imminent layoffs that were not yet ready to be divulged; and Jim called a young partner at another firm and recited all the terms of an offer to try to entice the listener to jump ship and join Jim's firm.

Although the Information-Technology half of my persona wants me to keep bashing lawyers, attorneys are not the only negligent ones in this regard. Haven't we all experienced multiple occasions in an airport gate area or on a plane itself when we hear a salesperson or an IT administrator revealing names, numbers, troubleshooting steps and other confidential details? "Speed kills." The ostensible need to talk to someone that very instant often trumps the risk of damage that could ensue from revealing a trade secret or the identity of a company with whom one is negotiating or an inroad into a web network.

In addition to big voices, the wandering eyes of others are a factor, too, especially on long, monotonous flights. Every task undertaken and every bit of information possessed on behalf of a customer/client warrants protection. Attorney-client privilege, the even broader ethical-duty-of-confidentiality and all other lawyer and non-lawyer privacy obligations still apply at high altitudes. Thus, travelers should be especially careful about identifying customers or exposing other confidential information when typing on laptops on planes.

Before I go to the airport, I rename any laptop folders and document names that bear client names, typically only keeping the first letter of the client's company name. If there are a lot of documents in a folder that I plan to access on the flight, I use Better File Rename software to, with a few clicks, anonymize or pseudonymise all the pertinent file names. If I plan to edit a client-matter document that mentions a client name throughout, I run a Ctrl+H search-and-replace. Once I am back home or at my destination, it only takes another few clicks to undo those file-rename and search-and-replace temporary changes.

Laptops (and, whenever possible, other portable devices), once encrypted, enable one to reap two major benefits, one altruistic and one selfish First, the humane reward: in case the machine gets lost or stolen, whoever has the laptop will not be able to pull any data, let alone confidential information, off of the machine. As a result, confidential information, as well as private information as to co-workers, customers and others is protected. Second, the self-interest boon: anti-identity-theft statutes typically exempt lost or stolen encrypted personally identifiable information (PII) from triggering the duty of the data owner to give notice of breach. Thus, those who take precautions are spared the monetary costs and the PR-hit that inevitably flow from a notice-of-breach scenario.

But even if encryption protects files from getting into other hands, one's work has been for naught if he/she didn't back-up a document to another location. So, after each flight, a best practice is to make sure to copy new or newly edited documents back to the law firm's network. Our firm's IT Director Kevin Moore trained me years ago that the hard drive of a portable computer or device is like cash, but central storage on a network is like a credit card. The former, if lost or stolen, is lost for good. The latter is recoverable even if one local copy of it is lost or corrupted.

Along those same lines, go paperless as much as possible. Consider taking a portable scanner and scan all paper documents, receipts, handwritten notes that I create and gather on each trip. The scanner I use, the Visioneer Road Warrior, is about the same bulk as a light three-hole puncher. The only accoutrement it needs is a USB cable to attach to my laptop. As I find keeping track of physical objects increasingly distracting, I don't want to worry that I might have dropped — or left in the hotel room — a receipt or some notes or a prospective client's business card. Once scanned and saved to my work network, each such item is safe, secure and backed up. For business cards in particular, specialized user-friendly scanning software enables ready conversion into an electronic contact that can be saved right into, e.g., Microsoft Outlook or a webmail Contacts list.

Assuming one has been careful en route, what of the urge to surf the web on a big screen during down time at a hotel lobby or café computer? If you do check e-mail over a browser on a public computer, presumably you are not logging into a work email system via, for example, Outlook Web Access? If, however, you feel you must check work mail (or a personal webmail account Inbox) in this fashion, then at least make sure not to save the login/password or to download any confidential files.

On one cross-country trip, while waiting to do a workplace information-security presentation, I checked my personal Yahoo webmail on a hotel registration-desk PC. Once I had deleted the browser history and then closed the browsing window, I happened to notice something on the Desktop; it was called "[REDACTED FIRST AND LAST NAME]_Severance.doc". As soon as I hovered on that Microsoft Word file's icon, a yellow rectangular bubble appeared, displaying the company name and the first name of the original "Author" of the document – or of its parent or (great-)grandparent document. (According to some studies, 90% of electronic documents are created by editing a pre-existing document.) By right-clicking on the icon and then glancing at the "Properties" of the document, I was readily able to ascertain the original "Title" of the document. That Title reflected a different first and last name than the individual who was apparently about to be terminated via the current iteration of the document.

Without even opening the file, basic metadata allowed me to learn a fair amount of confidential information that was not meant to become public. I did delete the file and then emptied the Recycle Bin, such that only a computer forensics expert would have been able to resurrect the document from that machine. And I have never disclosed — and long since forgotten — the names I had stumbled upon. But the impact of that experience brought home to me how much more dangerous it is to lose a stray electronic document somewhere virtual than to leave a relatively one-dimensional piece of paper in a physical location. In the twenty-first century, inevitable human error can have much broader ramifications due to the many layers of information available in an electronic file.

Let's presuppose you made it through your trip without incident, physically and digitally. Now, what about the return trip home? Note that, if you travelled outside of the United States, hopefully you took special care at the beginning of your trip. Why? Under current Fourth Amendment law, upon anyone's return to the U.S. from overseas, the contents of his or her laptop — or other digital device — are subject to warrantless inspection at the discretion of Customs officials. No particularized suspicion of wrongdoing is required. Some courts have even ruled that a password and/or encryption/decryption key must be disclosed upon request.

Just last month, yet another federal appellate decision came down supporting the legality of warrantless border searches of laptop computers. So, what is a business traveler do? A multi-pronged work-around could be: use a loaner laptop that houses neither a full set of company-provided computer programs nor any confidential files/data; throughout the overseas trip, only do sensitive work over the Internet via a virtual private network (VPN) connection; store no newly created or modified confidential files on the local hard drive; and, before the return flight home, run an application such as powerful freeware tool CCleaner to "wipe" the hard drive.

Whether at home in your day-to-day routine or on the road, be circumspect about which information you store on a portable computer or device. When in doubt, leave the information in secure central storage from which you can access it remotely in a location-independent fashion. In general, remember the wisdom of the old "Hill Street Blues" cop-show Desk Sergeant Phil Esterhaus, who always urged his minions: "Let's be careful out there . . . ."

Robert D. Brownstone is the Technology & eDiscovery Counsel and the Co-Chair of the Electronic Information Management (EIM) Group at Fenwick & West LLP, a 300-attorney Silicon-Valley-headquartered law firm specializing in representing prominent high-technology and life-sciences companies. Known as "Law & Technology in One Brain" or "The Guru of Metadata," Mr. Brownstone is a nationwide advisor, presenter and writer on many law-and-technology issues, including privacy and information-security. He is often quoted in the press as an expert on electronic information and teaches eDiscovery Law & Process at two law schools. Mr. Brownstone can be reached at rbrownstone@fenwick.com or 650.335.7912. THIS ARTICLE DOES NOT CONTAIN LEGAL ADVICE.

Originally published as an article in the June/July 2011 issue of ExecutiveCounsel.