CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 159 years

WEDNESDAY, SEPTEMBER 3, 2014

Chicago Daily Law Bulletin®

Volume 160, No. 173

# Companies need closer look at personal devices to protect secrets

From Russian programmers to South Korean technicians and Chinese engineers, U.S. trade secrets appear to be at the mercy of an increasingly sophisticated array of cyberthieves. This summer saw the first criminal indictment against foreign military officers for hacking U.S. entities to secure commercially valuable trade secrets.

Renewed attention to the strengthening of international protection measures for confidential business information triggered by this explosion of activity should help shore up present enforcement efforts. But such protection needs to be enhanced by addressing the most dangerous threat to a company's trade secrets — hardworking employees who take their work home.

Despite the present visibility of trade secret theft, government-sponsored economic espionage has had a long-lived history. In the 19th century, intellectual property laws were actually used to support such espionage. Britain granted patents to citizens who imported foreign technology. There was no obligation that such "importation" be acceptable to the country of origin.

Given this background, the first plurilateral treaty requiring trade secret protection did not appear until the 1994 Agreement on Trade-Related Aspects of Intellectual Property. Article 39 of TRIPS required member countries to prevent "undisclosed information" from being "disclosed to, acquired by or used by others without their consent." It set as the floor for prohibition acts "contrary to honest commercial practices."

The ultimate effect of this phrase was to place trade secret protection squarely within the domestic sphere. Consequently, most countries have created laws that provide some level of protection for trade secrets. But, as the OECD recognized in its February 2014 report on Approaches to Protection of Undisclosed Information (Trade Secrets), enforcement has lagged.

A flurry of international developments promises to fill the gap. The Commission of the European Union signaled in May its strong support for a new Trade Secret Directive that will harmonize protection throughout the European Union. New legislation was introduced in Congress in July, The Trade Secret Act of 1924, HR 5233, that will provide a civil cause of action under the federal trade secret statute — the Economic Espionage Act, 18 U.S.C. Section 1831. Even China is considering amendments to its trade secret laws.

These efforts will undeniably strengthen a trade secret holder's ability to combat thefts internationally. But they do not directly address the special issues that arise from the growing practice of employees' using their own smartphones, tablets and other personal devices at work.

*Retrieving copies of confidential data from personal devices becomes problematic, particularly when the owner of the device has left the company.*

According to a June 2012 McKinsey survey, more than 80 percent of smartphones and 67 percent of tablets used at work are employee-owned. Such bring-your-own-device practices may reduce employer costs, but BYOD also creates new enforcement problems directly related to the personal nature of such devices. These problems have yet to be addressed adequately by present international trade secret reform efforts.

Any storage of confidential data on a personal device necessarily makes that data more vulnerable because personal devices generally lack the encryption contained on employer-provided equipment. Theft of BYOD-stored data can occur from sophisticated third-party hacking or from the more mundane, but no less traumatic, physical loss of the device. Beyond these obvious dangers is the practical reality that personal devices may be used by family members in ways that open the data on the device to hackers who lurk on video gaming, file trading and other sites that lack strong encryption protection.

Better encryption technologies will not resolve all the problems posed by BYOD. Retrieving copies of confidential data from personal devices becomes problematic, particularly when the owner of the device has left the company. While technologies already allow remote removal of data from some devices, concerns over property and privacy rights may make the use of such technologies legally unavailing.

For example, among the remedies provided in the EU Draft Trade Secret Directive is the destruction or return to the trade secret holder of "any document, object, material, substance or electronic file containing or implementing the trade secret." Article 11(2)(e). Yet there is no measure that addresses the balance to be struck between such return-or-destroy remedies and the privacy interests of the holder of the device on which they are stored.

In *Scarlet Extended v. SABAM*, Case C-70/10, the Court of Justice of the European Union, the EU equivalent of the U.S. Supreme Court, overturned an injunction obligating the social networking site Scarlet to install a filtering system that would allow it to monitor and block end users' unauthorized file trading of specified copyrighted works.

The court held that protection of intellectual property rights in the EU must be proportionally balanced against personal privacy rights. Absent specific measures that alter this balance, there is no present guarantee that privacy interests will not trump trade secret interests in cases of BYOD.

Until international standards deal with the new problems posed by BYOD, there are several steps U.S. trade secret holders can take to reduce the threat to their confidential data. Reconsidering the cost-benefit analysis of employer-provided-encrypted devices is a critical first step.

If the analysis favors BYOD, trade secret holders should establish clearly articulated policies regarding the use of these devices. It should also provide sensitivity training for all employees regarding the need to secure critical data. A trade secret inventory should be conducted with a close eye to reducing access to critical data to those who truly have a need-to-know.

While law and technology will continue to provide a potent mix for protecting trade secrets internationally, corporations still need to start with the individual. So does international law.

It is time to marry the privacy concerns of cyberspace with the intellectual property protection concerns of the present trade secret reform. When that occurs, the walls of protection will be truly strengthened.

GLOBAL IP

**DORIS ESTELLE LONG**

*Doris Estelle Long is a law professor, director of the Center for Intellectual Property Law and chairwoman of the intellectual property, information technology and privacy group at The John Marshall Law School. She has served as a consultant on IPR issues for diverse U.S. and foreign government agencies, including as attorney adviser in the Office of Legislative and International Affairs of the USPTO. She can be reached at 7long@jmls.edu.*