TO PROTECT TRADE SECRETS, COMPANIES MUST GET SMART ABOUT SMART PHONES

BY SHANNON S. PIERCE, ESQ. AND MATTHEW DIGESTI, ESQ.

Smart phones have changed the way that business is done. Today, property can be sold and contracts can be entered into with digital signatures scrawled across a smart phone touch screen. Companies have come to expect real-time communications with employees, vendors and business partners, all of whom are able to (and often do) check e-mail and voicemail around the clock. In short, smart phones are ubiquitous in business.

Thanks to technological advances in the last decade, virtually every person who walks through a company's front door is now armed with at least one smart phone, tablet or similar device. Thanks to Google Glass, voice-enabled (and web-linked) computers can now be mounted on a pair of glasses. Whether it is a company's customers, employees or visitors, most everyone has a way of instantly communicating – and transmitting – with the touch of a screen or a voice command.

While smart phones are an essential part of daily business, they also present ever-changing challenges to the protection of trade secrets. Consider the following scenarios:

Instant Photo and Video Capture:
An employee, seeking to exact revenge after a poor performance review, uses his or her personal smart phone to take photographs of highly confidential blueprints, product marketing plans or other sensitive data, which a co-worker left at his or her desk. That employee now has a shareable record of the company's trade secrets, and the company may have difficulty tracing how the employee accessed and recorded this information. Thanks to Apple's iPhone user interface, through which the camera feature is available without unlocking the phone itself, this theft could be accomplished in a matter of seconds.

Social Media:
A utility repairman overhears two employees discussing concepts for the company's next-generation products. On the way back to his work truck, he tweets the details for the world to see.

Voice Record:
Using the smart phone's built-in voice recording application, a mid-level employee of a company's business partner, who may or may not be aware of

the terms of the companies' mutual non-disclosure agreement, records a confidential planning meeting without anyone noticing. While this individual would need each party's consent to record such a conversation via telephone, the mere act of recording an in-person conversation may not, in and of itself, be unlawful. *See* NRS 200.650.

Regardless of whether a company is building unmanned aircraft, inventing new clean energy technologies, storing third-party data, developing the latest online gaming trend or engaging in virtually any other Nevada industry, every business can benefit from an analysis of the risks that smart phones present and how the company's policies and practices can be adapted to mitigate those risks.

Trade Secrets Are Only Trade Secrets If Companies Diligently Protect Them

If a company's trade secrets are stolen or threatened with theft, Nevada's Uniform Trade Secrets Act, which can be found in NRS Chapter 600A, enables the company to obtain immediate injunctive relief upon a showing of the following two elements: First, that the misappropriated information is likely a trade secret; and second, that such misappropriation will likely result in irreparable harm. NRS 600A.040(1); *Saini v. IGT*, 434 F.Supp.2d 913, 919 (D.Nev. 2006).

However, the determination of whether information qualifies as a trade secret depends on factors that are established long before the misappropriation occurs. Since trade secrets are defined as including only that information deriving value from not being generally known to the public and which is "the subject of efforts that are reasonable under the circumstances to maintain its secrecy" (NRS 600A.030(5)), the measures that companies take to protect their trade secrets before the theft occurs are a critical component of enabling a company to obtain injunctive relief once such data is stolen.

Courts often require companies seeking relief for trade secret misappropriation to demonstrate that they exercised eternal vigilance in protecting the information at issue. *Fail-Safe, LLC v. A.O. Smith Corp.*, 674 F.3d 889, 893 (7th Cir. 2012) (internal citations omitted); *see also Finkel v. Cashman Prof'l, Inc.*, 128 Nev. Adv. Op. 6, 270 P.3d 1259, 1264 (2012), *reh'g denied* (Apr. 27, 2012) (upon a claim of trade secret misappropriation, courts assess factors including the extent and manner in which the employer guarded the secrecy of the information). What measures are reasonable under the circumstances will vary depending on factors including the size and nature of the company involved, the data the company is trying to protect, how that data is stored and the limits the company places on disclosure of its sensitive information. Companies that fail to update their confidentiality policies and practices to remain current with technological

continued on page 10

TO PROTECT TRADE SECRETS, COMPANIES MUST GET SMART ABOUT SMART PHONES

continued from page 9

advances may, under certain circumstances, be deemed to have failed to exercise the requisite vigilance and forfeited trade secret protection that might otherwise apply.

Designing Strategies for Protecting Trade Secrets Against Modern Technological Threats

In light of these risks, companies should evaluate – on an annual or other periodic basis – their confidentiality policies and practices to ensure that they represent state-of-the-art protections against modern threats to corporate data. Among other things, companies should consider the following.

- ***Identify the Core Trade Secrets and Then Limit Opportunities for Access***: In any business, there are varying levels of sensitive data. By identifying the company's most sensitive data and periodically re-assessing this issue, companies can implement additional safeguards to protect this data, such as storing the data on a separate server, creating separate passwords to access such servers, and/or limiting access to portions of the company's premises where such information is stored. *See United States v. Chung*, 659 F.3d 815, 825-26 (9th Cir. 2011) ("[R]easonable measures for maintaining secrecy 'have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on [a] 'need to know basis', and controlling plant access.'") (internal citations omitted).

Companies should give careful consideration as to whether there are portions of their facilities that are so sensitive that even employees with proper access authorization should not be permitted to bring smart phones into such areas.

- ***Implement Premises Security Measures to Avoid Unintended Exposure to Trade Secrets***: Companies should consider involving their on-site security personnel in efforts to protect trade secrets. Careful coordination can enable security to identify individuals who are accessing sensitive areas of the company's facilities without authorization – including individuals who may be carrying smart phones or other data-transmission devices.

- ***Imposing Limitations on When and How Smart Phones Can Be Accessed***: Companies should give careful consideration as to whether there are portions of their facilities that are so sensitive that even employees with proper access authorization should not be permitted to bring smart phones into such areas. Once these decisions are made, companies should consider posting notices to employees and visitors, and revising employment policies to clarify not only where smart phones may be used, but also any smart phone capabilities (*e.g.*, audio recording) that are prohibited under certain circumstances. Prior to implementing any such policies, however, companies should consult with counsel experienced in employment matters to ensure that they do not run afoul of employees' right to engage in protected concerted activities, as set forth in the National Labor Relations Act (NLRA).

- ***Strengthen Contractual Protections to Address Smart Phone Usage***: Where appropriate, companies may also want to consider revising nondisclosure agreements to put corporate business partners on notice of appropriate and inappropriate use of technology during confidential business dealings.

- ***Label Data "Confidential" Before Someone Posts it Online***: Companies should advise employees as to how and when to label documents as confidential. Through consistent labeling of sensitive data, companies may be able to establish that the data at issue constitutes a protectable trade secret – even where (a) the company's other efforts to protect trade secrets may be found to be insufficient to address smart phones and other technological threats to trade secret protection and/or (b) company data is later stolen and published without the company's consent. *See* NRS 600A.032; *V'Guara Inc. v. Dec*, 925 F. Supp. 2d 1120, 1124 (D. Nev. 2013) (noting the rebuttable presumption that can be created where companies properly label sensitive documents); NRS 600A.055 (where companies adequately protect trade secrets, injunctive relief is available to preserve trade secret status of the data at issue and require that such trade secrets be removed from the internet).

- ***IT and Human Resource Strategies for Detecting and Responding to Theft***: Companies should consider training their IT and Human Resources personnel, among others, to identify and address suspicious use of technology – especially in sensitive portions of company facilities. For example, strategic use of computer forensic tools can enable IT personnel to identify and respond to indications of potential theft. Company Human Resources partners can also play a key role in detecting potential theft, including through well-designed initial hire procedures (e.g., up-to-date confidentiality and invention assignment agreements) and exit interview protocol.

Finally, if and when potential data theft is discovered, companies should immediately consult with counsel experienced in trade secret and employment litigation to ensure that the company is best positioned to pursue all available remedies and relief. ■

SHANNON S. PIERCE practices in employment, trade secret and commercial litigation with Fennemore Craig Jones Vargas, a leading southwest regional business law firm serving clients in the southwest. Pierce can be reached at (775) 788-2200 or spierce@fclaw.com.

MATTHEW P. DIGESTI practices in business and torts litigation with Fennemore Craig Jones Vargas. Digesti can be reached at (775) 788-2200 or mdigesti@fclaw.com.