SOCIAL MEDIA

AND

TECHNOLOGY IN THE WORKPLACE

JUNE 2012

JASON S. BOULETTE
MICHAEL GOLDEN

BOULETTE & GOLDEN L.L.P.
2801 VIA FORTUNA DR., SUITE 530
AUSTIN, TEXAS 78746

(512) 732-8900 | WWW.BOULETTEGOLDEN.COM

TABLE OF CONTENTS

I.
INTRODUCTION

This paper provides a brief overview of some of the issues associated with protecting confidential or trade secret information in the face of the rapid adoption of personal technological devices (*e.g.*, smart phones) by employees and service providers and the corporate implementation of technology that is changing when, where, and how work is performed.

It should be noted that this paper is written by an employment law specialist, not an intellectual property specialist and not an information security specialist. As with any sophisticated issue, a complete understanding of the security issues being created by the introduction and adoption of new technology requires input from multiple specialists representing a variety of disciplines. Even then, as Ray Kurzweil explains, there are limits to what we should expect anyone to be capable of predicting:

> The acceleration of paradigm shift (the rate at which we change fundamental technical approaches) as well as the exponential growth of the capacity of information technology are both beginning to reach the "knee of the curve," which is the stage at which an exponential trend becomes noticeable. Shortly after this stage, the trend quickly becomes explosive. Before the middle of this century, the growth rates of our technology—which will be indistinguishable from ourselves—will be so steep as to appear essentially vertical. From a strictly mathematical perspective, the growth rates will still be finite but so extreme that the changes they bring about will appear to rupture the fabric of human history.

Ray Kurzweil, The Singularity Is Near: When Humans Transcend Biology 9 (Penguin (Non-Classics) 2006) (2005).

II.
EMPLOYMENT LAW ISSUES

A. Employee v. Contractor

When it comes to the common-law protection of confidential information, there is a difference between employees and independent contractors. Every employee has a duty not to use, in a manner adverse to his or her employer, confidential or proprietary information acquired during the employment relationship.[1] This duty extends beyond termination and prevents a former employee from using confidential information or trade secrets acquired during employment.[2] By contrast, confidential information disclosed to an independent contractor may lose its "secret"

[1] *Gen. Insulation Co. v. King*, 2010 WL 307952, at *5 (Tex. App.–Houston [14th Dist.] 2010, no pet.) (citing *T-N-T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 21-22 (Tex. App.—Houston [1st Dist.] 1998, pet. dism'd)).
[2] *Id.*

status, absent a finding that the disclosure was made in confidence:

> One who does not wish to make disclosure of his secret in return for the term protection of the patent laws, or otherwise protect it specifically by contract, can still be protected if his disclosure is made in confidence so as to place the other party under a duty to keep his secret. It is a well-settled rule that equity will grant relief when one breaches his confidential relationship in order to unfairly use a trade secret. The owner of the secret must do something to protect himself. He will lose his secret by its disclosure unless it is done in some manner by which he creates a duty and places it on the other party not to further disclose or use it in violation of that duty.[3]

Notably, a "confidential relationship" may be inferred from the conduct of the parties, at least when it comes to determining whether there was evidence sufficient to uphold a jury finding that a particular item of information was a trade secret.[4] To be clear, the *unrestricted* disclosure of trade-secret information to third parties, *outside the context of a confidential relationship*, destroys the trade-secret status of the information.[5] Moreover, rational business actors rarely rely on the possibility of a favorable jury verdict as a means of protecting information, when it is relatively easy to impose contractual confidentiality obligations on contractors and thereby remove any doubt about whether the information is being disclosed in confidence. Indeed, contractual confidentiality obligations should be considered for employees as well, given that a contract can define "confidential information" much more broadly than the common-law defines a "trade secret."[6]

---

[3] *Furr's Inc. v. United Specialty Advertising Co.*, 385 S.W.2d 456, 459 (Tex. App.—El Paso 1964) *cert. denied*, *United Specialty Advertising Co. v. Furr's Inc.*, 382 U.S. 824 (1965) (citing *Luccous v. J. C. Kinley Company*, 376 S.W.2d 336 (S.Ct.1964); *Hyde Corporation v. Huffines*, 158 Tex. 566, 314 S.W.2d 763; *K & G Oil Tool & Service Co. v. G & G Fishing Tool Serv.*, 158 Tex. 594, 314 S.W.2d 782 (Tex. 1958)).

[4] *H.E. Butt Grocery Co. v. Moody's Quality Meats, Inc.*, 951 S.W.2d 33 (Tex. App.—Corpus Christi 1997) (fact that H.E.B. knew Moody's was "proud" of its fajita process and believed its process could provide H.E.B. an advantage was "some evidence" that Moody's disclosure of the process to H.E.B. was made in confidence and was thus capable of supporting jury's implied finding that Moody's disclosure of the process to H.E.B. did not destroy the trade secret status of the information).

[5] *INEOS Group Ltd. v. Chevron Phillips Chemical Co., LP*, 312 S.W.3d 843, 852 (Tex. App.—Houston [1st Dist.] 2009, no pet.) (citing *Numed, Inc. v. McNutt*, 724 S.W.2d 432, 435 (Tex.App.—Fort Worth 1987, no writ) (concluding that data not trade secret because owner had previously disclosed it in contracts to its customers); *Interox America v. PPG Indus., Inc.*, 736 F.2d 194, 202 (5th Cir.1984) (considering owner's past conduct of voluntarily giving third-party contractors manuals containing technical information to support conclusion that information not entitled to trade secret protection)

[6] *Trilogy Software, Inc. v. Callidus Software, Inc.*, 143 S.W.3d 452, 471 (Tex. App.–Austin 2004, pet. denied) (upholding summary judgment in favor of the defendant on the plaintiff's common-law misappropriation claim but reversing summary judgment in favor the defendant on the plaintiff's tortious interference with a non-disclosure agreement claim, noting that the operative definition under the non-disclosure agreement was broader than the common law definition of a trade secret).

B. Keeping Secrets

As the Texas Supreme Court noted 16 years ago, "We live in a world of high employee mobility and easy transportability of information."[7] As anyone with a smartphone can tell you, this statement is truer today than it was back in 1996. Technological advances have made the retrieval, transmission, and storage of phenomenal amounts of information simple, affordable, and efficient, even when done from thousands of miles away. Of course, the increased fluidity of confidential company information presents unique security concerns.[8] For example, even at the most basic level, cloud computing requires a fundamental leap of security faith, given that cloud data is stored off-site under the control of a third-party vendor, rather than in-house behind a company's own firewall.[9]

Indeed, the general increase in data fluidity presents at least two distinct risks to company confidential information: (1) the risk of inadvertent disclosure associated with the use of laptops, smartphones, and other mobile technologies; and (2) the increased risk of intentional theft of tremendous amounts of data through the use of common-place technology capable of accessing, transferring, and storing large amounts of data both remotely and locally.

1. All That Information in Your Pocket

One 2010 study found that only 35% of employees surveyed were provided smartphones by their employers.[10] Notably, the same study found that 66% of employees who were not provided a company-owned smartphone used their private smartphones for work.[11]

This little factoid is particularly significant, given the findings of the 2012 Symantec "Honey Stick Project." For those unfamiliar with the study, in early 2012 Symantec intentionally "lost" 50 smartphones in high traffic public locations (*e.g.*, elevators, malls, food courts, and public transit stops) in five cities: New York, Washington, D.C., Los Angeles, San Francisco, and Ottawa.[12] The smartphones, which were not password-protected, were equipped with monitoring software and loaded with simulated apps with recognizable names suggesting their function (*e.g.*, social media, banking, *etc.*).[13] Although the simulated apps had no true functionality, they

---

[7] *Computer Associates Intern, Inc. v. Altai, Inc*., 918 S.W.2d 453, 457 (Tex. 1996) (discussing the misappropriation of "a stack of 'greenbar' computer paper upon which the code was printed when [the employee] left the company.").
[8] *See, e.g.*, Mark Tickle, IDG Connect, *Securing a Growing Mobile Workforce* (May 5, 2011).
[9] Joe Dysart, ABA Journal, April 2011, *The Trouble with Terabytes*, p. 33; *see also* Kevin Townsend, *Securing the Public Cloud for the Mobile Workforce*, http://kevtownsend.wordpress.com/2010/10/29/securing-the-public-cloud-for-the-mobile-workforce/ (Oct. 29, 2010) (last visited May 15, 2011).
[10] iPass, *Mobile Workforce Report, Year End Review and 2011 Predictions* (www3.ipass.com/wp-content/uploads/2010/12/Mobile-Workforce-Report-yearend-2010.pdf) (Feb. 19, 2010) (last visited April 25, 2012).
[11] *Id.*
[12] Symantec, *The Symantec Smartphone Honey Stick Project* (www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf) (Mar. 9, 2012) (last visited Mar. 28, 2012)
[13] *Id.* at 6-5, 8.

mimicked functionality and were able to transmit event data to a central logging facility to indicate which app was activated and at what time.[14] Beyond that, some of the apps had simulated login pages that showed a pre-filled username and password.[15] In addition, an app called "Contacts" had a small number of manufactured contacts, one of which had the tag "Me" beside the name to enable a finder to identify the owner of the device relatively easily.[16] The findings suggest that the unexpected discovery of a smartphone presents a powerful temptation to snoop:

- Smartphone accessed – 96%
- Private photo app accessed – 72%
- Social networking and personal email accessed – 60%
- Online banking app accessed – 43%
- Corporate email app accessed – 45%
- File title "HR Salaries" accessed – 54%
- File titled "HR Cases" accessed – 40%
- "Remote Admin" app accessed – 49%
- File titled "Saved Passwords" accessed – 57%
- Attempt to click through the login and password reset screens – 66%;
- Average time following discovery before an access attempt was made – 10.2 hours
- Median time following discovery before access attempt – 59 minutes;
- Smartphones moved before being accessed – 32%
- Attempt to contact owner - 50%.[17]

At a minimum, these findings underscore the need for password protection and remote location and wiping capabilities. More broadly, these findings speak to the inherent security risks created when access to sensitive information is entrusted to a device as common as a phone and suggest

[14] *Id.* at 8.
[15] *Id.* at 10.
[16] *Id.*
[17] *Id.* at 12-13.

that executives are right to be concerned about the security implications associated with the proliferation of smartphones and social media.[18]

2. "Easy Access": A Euphemism for "Weak Control"

Texas law defines a "trade secret" as any "formula, pattern, device or compilation of information used in a business, which gives the owner an opportunity to obtain an advantage over his competitors who do not know or use it."[19] To state a common law claim for trade secret misappropriation under Texas law, a plaintiff must show (1) the existence of a trade secret; (2) breach of a confidential relationship or improper discovery of a trade secret; (3) use of the trade secret; and (4) damages.[20] Information such as customer lists, pricing information, client information, customer preferences, buyer contracts, market strategies, blueprints and drawings have all been afforded trade secret status.[21]

To determine whether information is a trade secret protected from disclosure or use, a court must examine six "relevant but nonexclusive" criteria: (1) the extent to which the information is known outside the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken to safeguard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[22]

Of course, to be entitled to protection, the information must be secret, or at least substantially secret.[23] The widespread adoption of remote and mobile technology thus presents an interesting

---

[18] *See, e.g.,* AT&T, *2011 Business Continuity Study, U.S. National Results* (www.att.com/Common/about_us/business_continuity/National_Business_Continuity_2011_Summary.pdf) (2011) (last visited April 25, 2012). (79% of executives responding indicated that they were "very/somewhat" concerned about the data security risk presented the increased use of social networking capabilities, while 82% reported being "very/somewhat" concerned about mobile networks and devices.)

[19] *Triple Tee Golf, Inc.*, 485 F.3d 253, 261 (5th Cir. 2007) (*quoting Taco Cabana Int'l, Inc. v. Two Pesos, Inc.*, 932 F.2d 1113, 1123 (5th Cir. 1991)).

[20] *Moncrief Oil Intern., Inc. v. OAO Gazprom*, 2010 WL 4813273, at *9 (Tex. App.–Fort Worth 2010, no pet.); *accord Tex. Integrated Conveyor Sys., Inc. v. Innovative Conveyor Concepts, Inc.*, 300 S.W.3d 348, 366–67 (Tex. App.–Dallas 2009, pet. denied); *Trilogy Software, Inc. v. Callidus Software, Inc.*, 143 S.W.3d 452, 463 (Tex. App.–Austin 2004, pet. denied).

[21] *Gallagher Healthcare Ins. Servs. v. Vogelsang*, 312 S.W.3d 640, 652 (Tex. App.–Houston [1 Dist.] 2009, no pet. hist.).

[22] *Gen. Universal Sys., Inc. v. Lee*, 379 F.3d 131, 150 (5th Cir.2004) (citing *In re Bass*, 113 S.W.3d 735, 739–40 (Tex.2003)); *T–N–T Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W.2d 18, 22 (Tex.App.-Houston [1st Dist.] 1998, pet. dism'd). All six factors need not be satisfied "because trade secrets do not fit neatly into each factor every time." *Gen. Universal Sys*., 379 F.3d at 150 (*quoting Bass*, 113 S.W.3d at 740).

[23] *SP Midtown, Ltd. v. Urban Storage, L.P.*, No. 14-07-00717-CV, 2008 WL 1991747, at *5 n.5 (Tex. App.–Houston [14th Dist.] May 8, 2008, pet. denied) (mem.op.) ("There is no cause of action for misappropriation of information that is not either secret, or at least substantially secret."); *see also Rimes v. Club Corp. of America*, 542

challenge as company secrets are increasingly moving outside company walls, making it increasingly important for companies to take specific steps to address the remote and mobile use of sensitive data.[24]

One seemingly simple step that employers can take to protect information is to limit access to the information to those who truly need to access it. In practice, however, limiting access to information can be exceedingly difficult, particularly in an age where a PowerPoint presentation being distributed via email may contain *bona fide* trade secrets. Fortunately, complete secrecy is not required for trade secret protection.[25] That said, whether a company limited access to information will likely be a key factor in determining whether a company took adequate measures to protect that information to make it entitled to protection under the common law.[26]

In *In re Union Pacific*, for example, the Texas Supreme Court held that Union Pacific met its burden of establishing that its rate structures are trade secrets, citing to affidavits from an Assistant Vice President who noted that rate information is not known by competitors, not known by customers, and "is not even generally known throughout the company."[27] Rather, the information was known only to a limited number of Union Pacific employees and certain management employees.[28] Likewise, in *Gallagher Healthcare Ins. Servs. v. Vogelsang*, the Court held that the employer had shown its confidential information was an interest worth of

---

S.W.2d 909, 913 (Tex. Civ. App.—Dallas 1976, writ ref'd n.r.e.); *American Precision Vibrator Co. v. National Air Vibrator Co.*, 764 S.W.2d 274, 277 (Tex. App.—Houston [1st Dist.] 1988, no writ).

[24] There are numerous trade secret cases where the company secret is kept literally under lock and key in a vault or other secured, physical location. *In Re Bass*, 113 S.W.3d 735, 742 (Tex. 2003) ("The data were kept in a secured, climate regulated vault that was accessible only to those who knew the combination."); *In re XTO Res. I, LP*, 248 S.W.3d 898, 902 (Tex.App.-Fort Worth 2008, no pet.) ("the data were kept in a vault accessible only to those who knew the combination, and employees needed a security card just to enter the work area"); *IAC, Ltd. v. Bell Helicopter Textron, Inc.*, 160 S.W.3d 191, 198 (Tex.App.-Fort Worth 2005, no pet.) ("Bell showed that it guards the secrecy of its data by storing the originals of its drawings and specifications in a vault, posting security guards at its plants, requiring persons entering the plant to identify themselves and wear identification badges, checking material going in and out of the plant, limiting access to data on its internal computer system to persons with appropriate system identification and passwords.").

[25] RESTATEMENT OF TORTS § 757, comment b (1939) (") ("It is not requisite that only the proprietor of the business know it. He may, without losing his protection, communicate it to employees involved in its use. He may likewise communicate it to others pledged to secrecy."); *see also H.E. Butt Grocery Co.v. Moody's Quality Meats, Inc.*, 951 S.W.2d 33, 36 (Tex. App.—Corpus Christi 1997, pet. denied)

[26] *In Re Bass*, 113 S.W.3d 735, 742 (Tex. 2003) (holding employer satisfied the second factor on the extent to which the information is known to employees with testimony that only four employees had access to the data, "including the company's geophysicist whose job includes analyzing such data for Bass.").

[27] *In re Union Pac. R.R. Co.*, 294 S.W.3d 589, 592 (Tex. 2009) (orig. proceeding) (per curiam).

[28] *Id.*

protection, pointing to evidence that the company shared the information with employees and agents of the company on a "need to know basis" only.[29]

In addition to increasing the likelihood that the information will enjoy trade secret status, limiting those capable of accessing sensitive information reduces the likelihood that the information will ever be compromised. The Wikileaks release of sensitive Department of State diplomatic cables is believed to have been largely caused by granting too many individuals access to the information, including, U.S. Army Intelligence Analyst Private First Class Bradley E. Manning, who was charged with the leaks in July 2010.[30] What was particularly suprising, apart from the actual information leaked, was Manning's alleged explanation of how he was able to do what he did, given what one would assume would be a highly secure environment. In online chats with a computer hacker, Manning is alleged to have described how he obtained the cables and other confidential information:

> "I would come in with music on a CD-RW labeled with something like 'Lady Gaga,' erase the music then write a compressed split file,"…. "No one suspected a thing and, odds are, they never will."…"[I] listened and lip-synced to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history," …. "Weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis … a perfect storm."[31]

Assuming the above is an accurate account of what happened, the Department of State debacle is at least in part a story about an employer's weak security measures. As Manning allegedly noted, "weak servers, weak logging, weak physical security," left his employer's confidential information vulnerable. While hindsight is obviously 20/20, the Department of State, the United States of America, and several high-profile governmental officials around the world could have been spared significant embarassment, if the Department had simply limited access to its cables to those who actually needed to be able to access them.

3. Keeping Your Secrets Secret

Although companies seem to comprehend (at a level) the security risks presented by mobile technology and social media, a recent PwC study found that only 43% of companies have a

---

[29] *Gallagher Healthcare Ins. Servs. v. Vogelsang*, 312 S.W.3d 640, 652 (Tex. App.–Houston [1 Dist.] 2009, no pet.); *see also Sharma v Vinmar Intern Ltd*, 231 S.W.3d 405, 425-26 (Tex. App. –Houston [14th Dist.] 2007, no writ) (citing to the "need-to-know" factor as evidence that employer "made concerted effort to maintain secret nature of its information.").

[30] *See, e.g.*, Ewen MacAskill, *Wikileaks cables: US tightens security*, THE GUARDIAN, Dec. 1, 2010; Ben Birnbaum, *WikiLeaks releases State Department cables*. THE WASHINGTON TIMES. Nov. 28, 2010. *available at*: http://www.washingtontimes.com/news/2010/nov/28/wikileaks-releases-state-reports/?page=1.

[31] Kim Zetter and Kevin Poulsen, *Army Intelligence Analyst Charged With Leaking Classified Information*, Wired Magazine, July 6, 2010. *available at*: http://www.wired.com/threatlevel/2010/07/manning-charges/.

security strategy for the use of personal devices, only 37% have a security strategy for mobile devices, and only 32% have a security strategy for social media.[32]

A discussion of the technical security solutions available to employers is far beyond the scope of this paper and the expertise of its authors. From an employment lawyer's perspective, here are a few basic strategies for safeguarding information:

- Require all devices containing sensitive information be password-protected;
- Require all mobile devices containing sensitive information be equipped with remote wiping software;
- Address BYOD, including whether employees may place particularly sensitive information on devices they own, whether a laptop, smartphone, or other device;[33]
- Prohibit employees and contractors from placing data on any device not owned by the company;
- Require employees to grant the company access to any device on which the employee places data (in violation of policy);
- Prohibit employees and contractors from working on sensitive material in public places, including airplanes and airports;
- Require employees and contractors to prevent third-parties (*e.g.*, roommates) from accessing their remote work areas or devices;
- Require that work devices be used only for work;
- Ban, limit, or monitor the use of thumb-drives, CDs, and other media devices;
- Block, limit, or monitor access to personal file transfer sites;
- Provide secure file transfer accounts for employees to use for file transfers, to ensure line of sight to anyone accessing the data contained in the account;
- Integrate a data loss prevention (DLP) solution with the company's secure file transfer system to enable the monitoring of sensitive content and its use;
- Install devices to monitor and track access to confidential information;

[32] PwC, *PwC's 2012 Global State of Information Security Survey*®, (http://www.pwc.com/gx/en/information-security-survey/giss.jhtml) (Sept. 2011) (last visited April 25, 2012).
[33] Note that this may be difficult with contractors, who more frequently provide their own equipment.

- Use confidential watermarks on confidential information;
- Require popup acknowledgements each time confidential information is accessed, noting the confidentiality of the information and reminding the employee of his or her non-disclosure obligations;
- Encrypt all computer hard drives, data storage devices, and electronic communications that contain confidential information; and
- Develop a relationship with local law enforcement.

This is by no means an exhaustive list, nor is it a list of must-do's. Rather, employers should recognize that there are steps that can be taken to safeguard sensitive information and consult true security experts to ensure their technical security programs are sufficiently robust given the specific nature of the data at issue.

4. Preparing For a Secret Getting Out

In addition to prohibiting the actual disclosure of information by employees and contractors who actually read and comply with them, agreements and policies offer "after the fact" mechanisms for dealing with employees who improperly access, retain, disclosure, or use company information. At a minimum, employees with access to confidential information should be required to sign non-disclosure agreements that broadly (but appropriately) define confidential information and specifically names any particularly important items of information. Again, a contract can define "confidential information" much more broadly than the common-law defines a "trade secret."[34] Moreover, evidence that the company required employees and contractors to execute non-disclosure agreements can be an important factor weighing in favor of trade secret protection for company information.[35]

Beyond non-disclosure agreements, an IT policy or acknowledgement that is properly drafted to limit access to information for legitimate company purposes can set up a claim (and possibly a prosecution) under the Federal Computer Fraud and Abuse Act ("CFAA").[36] Enacted in 1986, the CFAA prohibits anyone from accessing a protected computer without authority or by exceeding authorized access for purposes of obtaining information, causing damage, or

[34] *Trilogy*, 143 S.W.3d at 471 (Tex. App.–Austin 2004, pet. denied) (upholding summary judgment in favor of the defendant on the plaintiff's common-law misappropriation claim but reversing summary judgment in favor the defendant on the plaintiff's tortious interference with a non-disclosure agreement claim, noting that the operative definition under the non-disclosure agreement was broader than the common law definition of a trade secret).

[35] *Gallagher Healthcare Ins. Servs. v. Vogelsang*, 312 S.W.3d 640, 652 (Tex. App.–Houston [1 Dist.] 2009, no pet.); *Sharma v Vinmar Intern Ltd*, 231 S.W.3d 405, 425-26 (Tex. App. –Houston [14th Dist.] 2007, no writ.); *Gonzalez v. Zamora*, 791 S.W.2d 258, 265 (Tex. App.–Corpus Christi 1990, no pet.).

[36] 18 U.S.C. § 1030(a)(1)-(7) (2004).

perpetrating fraud.[37] Although the CFAA is a criminal statute, it also provides a private right of action.[38] The interesting issue raised in cases tied to employment has been whether the misuse by an employee was transformed into unauthorized use or use exceeding authorized access for purposes of the CFAA.[39]

In *United States v. John*, for example, the Fifth Circuit held that an employee of Citigroup exceeded her authorized access to her employer's computers when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud.[40] Likewise, in *International Airport Centers, LLC v. Citrin*, the Seventh Circuit reasoned that, regardless of whether an employee once held authorization to use company computers, that employee loses authorization when the employee violates a state law duty of loyalty. In essence, the employee's attempts to perpetrate a fraud on the company terminated the employee's authority to access company resources.[41]

Although these solutions neither prevent nor detect loss, they can provide a remedy once the loss is detected.

5. Dealing With Departure

Confidential company information is perhaps most vulnerable at the end of an employment or contractor relationship. This is especially true with remote and mobile workers, who literally may be thousands of miles away with an entire dataroom's worth of information stored off-site in their places of business or homes. Indeed, one of the reasons it is so important to own the devices on which sensitive information is stored is that ownership of the physical device is the

[37] *Id.*

[38] *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001) (referring to the private right of action under 18 U.S.C. § 1030(g)).

[39] *United States v. Nosal*, 2011 WL 1585600, at *2-3 (9th Cir. Apr. 28, 2011).

[40] *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

[41] *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Other courts have also joined this broader interpretation of the CFAA. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001) (holding that an employee likely exceeded his authorized access when he disclosed information in violation of a confidentiality agreement the employee voluntarily signed); *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (holding that an employee of Citigroup exceeded her authorized access when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud); *United States v. Batti*, 631 F.3d 371, 379 (6th Cir.2011) (although not addressing the issue of whether the employee's use was authorized or exceeded authority, the Court upheld a terminated employee's conviction and an award of restitution to his former company under the CFAA where the employee accessed the computer system to steal confidential data); *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir.2006) (holding that an employee loses authorization to use a computer even absent an express policy against fraudulent use when the employee violates a state law duty of loyalty because, based on common law agency principles, the employee's actions terminated the employer-employee relationship "and with it his authority to access the [computer]."); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (upholding the conviction of a former employee who used the employer's databases to obtain personal information about people he knew).

most certain means for ensuring forceable return of the data stored on it, if that becomes necessary. Put bluntly, the police may well assist in retrieving a company-owned laptop that a former employee or contractor has refused to return, but they are not particularly likely to assist in the forceable removal of company data from a laptop the employee or contractor owns.

It is also critical that an employer disable a departing employee's or contractor's network access as soon as practical and review the departing employee's or contractor's network activity in the days (or months, if circumstances warrant) leading up to his or her separation.[42] While these concerns are present with any departing employee or contractor, they are heightened when it comes to employees and contractors who work off-site, as they will be quite used to accessing the employer's systems remotely and more likely to have developed local copies of significant amounts of information.

Beyond that, departing employees and contractors should be required to return all company assets in an unaltered state (to permit forensic inventory and analysis as necessary) and reminded of their continuing obligations to protect the company's information. Departing employees and contractors should also be asked to sign an acknowledgment that they have not retained any company information, or any copy or derivation thereof, on any personal computers or electronic devices and a promise to deliver to the company any company information that later comes into their possession.

III.
CONCLUSION

Technology is advancing at an exponential rate and, as is usually the case, employers, employees, and third-party service providers are adopting it far more quickly than the law is addressing the implications of its use. While technology presents tremendous opportunity for companies who are able to implement it effectively, it simultaneously presents the opportunity for new and frequently unexpected legal risks for the uninitiated and seasoned alike. As a result, employers are well advised to give company counsel a seat at the table when discussing the adoption of new technologies to ensure that the risks presented by that technology are identified and at least mitigated, if not eliminated.

This paper is not intended as legal advice.

[42] *Gallagher Benefits Servs. Inc. v. De La Torre*, 2007 WL 4106821, *4 (N.D. Cal. 2007), *affirmed in part and vacated in part*, 283 Fed. Appx. 543 (2008) (employee alleged to have downloaded 150 files to his Blackberry the day prior to his resignation).