Presented:
2021 Nonprofit Organization Fundamentals and Institute

January 20-22, 2021
Austin, Texas

Cybersecurity and Data Protection Considerations In Work-From-Home Policies

Jason S. Boulette
Gilbert Nwaopara

Author contact information:
Jason S. Boulette
Gilbert O. Nwaopara
Boulette Golden & Marin LLP
Austin, TX

jason@boulettegolden.com
512-732-8901
gilbert@boulettegolden.com
512-732-9902

TABLE OF CONTENTS

I. INTRODUCTION

Since March of 2020, employees and employers have faced a new reality: working from home. With the threat and uncertainty of COVID-19, everything from elementary schools to television stations to Fortune 500 companies has shifted to working and delivering services from home.

While working from home may be a business necessity in the near-term (and a possible work-life benefit in the long-term), it does present unique risks with respect to the practical and legal protection of confidential business information, customer information, and trade secrets. Employers are now forced to balance their employee's ability to work effectively from home with the need to safeguard and protect their trade secrets and other confidential information outside the office.

This paper will provide an overview the impact of work from home arrangements on trade secret protection under the state Texas Uniform Trade Secret Act and the federal Defend Trade Secrets Act, as well as a discussion of the circuit-split with respect to the meaning of "unauthorized access" under the federal Computer Fraud and Abuse Act.

II. PROTECTING TRADE SECRETS WHILE WORKING FROM HOME

In an office setting, a number of trade secret safeguards result from the simple fact employees are accessing and dealing with the company's trade secrets in a controlled space. The company generally knows who is in the space, is able to physically co-locate teams that need access to similar information to limit the likelihood of inadvertent "over the shoulder" disclosures, and can create physical spaces of employee-specific restricted access.

In a remote work setting, these protections disappear. An employer has no idea who may be standing over an employee's shoulder or have access to an employee's laptop or company documents being used at the employee's home or other remote work location. Likewise, the company has no assurance that the network the employee is using to access the company's information is secure or that it is even the employee's own network as opposed to an unsecured public network. Indeed, the employer does not even truly know *where* the employee is when he or she is using a device to access the employer's network and information remotely. This simple reality has both practical and legal implications.

A. A "Trade Secret"

The state Texas Uniform Trade Secrets Act ("TUTSA") and the federal Defend Trade Secrets Act ("DTSA") both provide legal protection for "trade secrets." TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002; 18 U.S.C. § 1836. The TUTSA and the DTSA also use similar definitions of what it means to be a "trade secret" entitled to protection under the statute, both of which include taking reasonable steps to protect the information at issue. The TUTSA defines "trade secret" as follows:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, process, financial data, or list of actual or potential customers or suppliers, that:

> (A) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
>
> (B) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(6).

Similarly, the DTSA defines a "trade secret" thusly:

> [A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;

18 U.S.C. § 1839(3).

B. Reasonable Efforts

Under both statutes, a trade secret must (1) have independent economic value and (2) be the subject of reasonable efforts to maintain that information's secrecy. Of potential significance, however, the TUTSA requires such efforts be reasonable "under the circumstances," whereas the DTSA makes no explicit provision for "the circumstances." *Compare* TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(6)(B) with 18 U.S.C. § 1839(3)(B).

That said, federal courts often read in the "under the circumstances" found in most state Uniform Trade Secret Act statutes when assessing "reasonableness" under the DTSA. *See, e.g., Computer Sciences Corp. v. Tata Consultancy Services Ltd.*, 3:19-CV-970-X(BH), 2020 WL 2487057, at *4 (N.D. Tex. Feb. 7, 2020), *report and recommendation adopted*, 3:19-CV-00970-X, 2020 WL 1428941 (N.D. Tex. Mar. 24, 2020) (DTSA case) ("The owner must take 'reasonable measures under the circumstances to keep the information secret'"….); *Marek Brother Systems, Inc. v. Enriquez*, No. 3:19-CV-01082, 2019 WL 3322162, at *3 (N.D. Tex. July 24, 2019) (DTSA and TUTSA case) ("To establish entitlement to trade secret protection, the owner must take 'reasonable measures under the circumstances to keep the information secret.' …"); *Xavian Ins. Co. v. Marsh & McLennan Companies, Inc.*, 18CV8273(DLC), 2019 WL 1620754, at *5 (S.D.N.Y. Apr. 16, 2019) (noting the Uniform Trade Secret Act's requirement of "efforts reasonable under the circumstances does not appreciably differ from the DTSA's "reasonable

Title search: Cybersecurity and Data Protection Considerations in Work-From-Home Policies

Also available as part of the eCourse
Cybersecurity During a Pandemic: What To Do Help Protect Your Nonprofit Organization

First appeared as part of the conference materials for the
38th Annual Nonprofit Organizations Institute session
"Cybersecurity and Data Protection Considerations in Work-From-Home Policies"