Cloud Computing Technology: Providing a Safer Way for Businesses to Protect Trade Secrets under the Defend Trade Secrets Act

HEATHER BOWEN*

INTRODUCTION

In this technological era, legal and business analysis is heavily focuses on the future and protecting interests that are traditionally revered by law. Some forms of technology are more prevalent than others, such as mediated communication, which includes email, text messaging, instant messaging, social networking, blogs, and video conferencing platforms (Skype, Oovoo, and FaceTime). Cloud computing is another example of mediated communication technology and is the prime focus of this paper. Today, society is extremely reliant on mobile phones and computers to retain and disseminate information to others for both personal and business purposes. This is an important fact because cloud computing technology is accessible from phones and computers. Well-respected scholars agree that technology has a strong, rather unfounded agency over individuals.[1]

Alvin Toffler articulated the three "waves" of technological innovation to be (1) agricultural, (2) industrial, and (3) informational.[2] Most relevant for the purposes of this paper is the latter - the informational wave of technology. The informational wave has transformed the business world to one in which individuals are heavily reliant and dependent upon not only computer communication technologies,[3] but also telephone and radio communication, and voice

* Heather Bowen graduated from Northwestern Pritzker School of Law in Chicago, Illinois, in May 2017. Heather holds a B.A. in Government and World Affairs, a B.A. in Music, and a minor in Criminology from the University of Tampa. She graduated *magna cum laude*, with honors in May 2014. During law school, Heather had the opportunity to perform with the Chicago Bar Association Symphony Orchestra, the Moody Church Orchestra, and the Chicago Philharmonic. In addition, she has served as a scholar of the Hispanic National Bar Association, Microsoft Intellectual Property Law Institute and the Intellectual Property Owners Association, and as a student ambassador of the International Trademark Association. Upon graduation, Heather returned to New York to start her transactional law fellowship with Start Small Think Big in Manhattan. She would like to thank her family, friends, colleagues, and professors for their endless support, knowledge, guidance, and encouragement in this process and throughout her life.

1. *See generally* Rias J. van Wyk, *Technology: A fundamental structure?*, 15 KNOWLEDGE, TECH. & POL'Y 14, 19–31 (2002).

2. ALVIN TOFFLER, THE THIRD WAVE 26 (William Morrow and Company, Inc. ed., 1980).

3. *See id.* (explaining that the Third Wave is radically changing the corporations of the

response systems. Toffler, along with his colleagues, Esther Dyson, George Gilder, George Keyworth, and Alvin Toffler provide a unique perspective on developing information and communication technologies, wherein he advocates for a "utopian" perspective on cyberspace.[4] Essentially, he advocates for free market competition in the information technology and communication sectors and for governmental units to abstain from controlling the advancement of the telecommunications marketplace.[5] Yoneji Masuda similarly advocated for a shift from the industrial society to the information society in order to result in an age that will provide both a new and unique period in human existence.[6]

This paper will focus on the particular technology of cloud computing, which has become so entrenched in the lives of individuals working in businesses, law firms, governmental institutions, and nonprofit organizations. Cloud computing technology has captured the attention of business leaders throughout virtually every industry, by providing businesses the opportunity to capitalize on speed, scale, and economics. Cloud computing is helping to serve everyday needs of the population[7] and should be considered as a non-neutral, continually-developing tool that has the ability to make broad social, cultural, and political impacts on the world around us. The expansion of this form of technology has brought about the ability to engage in more meaningful and knowledgeable undertakings in the workplace wherever we are in the world. Business entities, however, must acknowledge that cloud computing also sets a limiting parameter around what, how much, and in what way those entities may want to divulge one of their most protected assets - their trade secret proprietary information. This topic will be further addressed in later sections of this paper.

Businesses look to the law to protect trade secrets stored in the cloud. The intersection of law and cloud computing technology stems from the use of compartmentalized subject matter, such as intellectual property (patents, trademarks, copyrights, and trade secrets), biotechnological law, and telecommunications.[8] Part I focuses on how cloud computing technology has changed, how businesses generally protect their trade secrets, and how businesses also open themselves

---

future).

4. *See* Esther Dyson et al., *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age*, 12 THE INFO. SOC'Y 295, 295-308 (1994) (describing that the Third Wave and the new "electronic frontier" of knowledge will renew, and enhance the "American Dream" and humankind's future).

5. *See id.* at 305–06 (explaining that the regulation of telecommunication services, such as telephone, cable, satellite, should be regulated by antitrust law; therefore, moving away from natural monopolies and into a free market).

6. YONEJI MASUDA, MANAGING IN THE INFORMATION SOCIETY 3 (Basil Blackwell, Inc. ed., 2d ed. 1980).

7. *See* ANDREW FEENBERG, TRANSFORMING TECHNOLOGY: A CRITICAL THEORY REVISITED 5–6 (Oxford U. Press, 2d ed. 2002).

8. Arthur J. Cockfield, *Towards a Law and Technology Theory*, 30 MAN. L.J. 383, 387 (2004).

up to the risk of hackers stealing their information. This section will also frame the benefits and challenges in using cloud computing technology and maintaining the privacy of information. Part II focuses on pertinent recommendations for businesses to consider when using cloud computing technology, in light of the Defend Trade Secrets Act (DTSA),[9] to protect themselves against any trade secret misappropriation. Part III addresses future potential issues that cloud computing technology may have on business owners in protecting their trade secrets. These three parts all illustrate the overarching theme that cloud computing technology provides a safer way for businesses to protect trade secrets under the new implementation of the Defend Trade Secrets Act.[10]

I. THE RISE OF CLOUD-BASED DATA IN AN EFFORT TO PROTECT TRADE SECRETS

It has been over 25 years since the Internet first became available to the world.[11] Before the Internet, companies like CompuServe, Prodigy, and America Online, offered online-communication services, using telephone modems. Over recent decades, the Internet has increased the volume of both stored information and accessible information.[12] As modes of communication and methods for exchanging information continue to develop, so do the legal issues surrounding them.[13]

Trade secrets are arguably more important now than ever before because of the increase in computer storage, coupled with the use of the Internet. These factors have made it much easier to misappropriate trade secrets.[14] With it has come an increase in litigation, legislation, media, and scholarly attention due to digital technology, a mobile workforce, the rising value of intellectual property, an increase in international threats, and the continuing debate over whether to pursue patent protection over trade secret protection.[15] Businesses invest a lot of time and energy to bring ideas and new products to the marketplace. In most cases, the use of the Internet and technology has allowed businesses to forgo pen and paper or filing cabinets and bankers' boxes[16] as the main avenue for gathering and maintaining

9. DEFEND TRADE SECRETS ACT OF 2016, 18 U.S.C. § 1836(b)(1) (2016).

10. *Id.*

11. Sir Tim Berners-Lee, *On the 25th anniversary of the web, let's keep it free and open*, GOOGLE: THE KEYWORD BLOG (Mar. 11, 2014), https://blog.google/topics/internet-access/on-25th-anniversary-of-web-lets-keep-it/.

12. Sharon K. Sandeen, *Meatspace, the Internet, and the Cloud: How Changes in Document Storage and Transfer Can Affect IP Rights*, 12 DEPAUL BUS. & COMM. L.J. 437, 443 (2014).

13. *Id.* at 441.

14. *Id.* at 443.

15. David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091 (2012).

16. Sandeen, *supra* note 12, at 444.

important company information. Before the Internet, these hard-copy physical forms of documents would be locked in the basement of a secure manufacturing plant containing thousands of pages of blueprints.[17] The ease of digitally storing important and secretive information brings greater opportunity for information to be copied and shared among others within the industry, who should not be made privy to the information.

Cloud computing refers to a somewhat infinite online storage that is always accessible from multiple electronic devices, except when the connection to the cloud is severed.[18] The word *cloud* is more of a marketing term in advertising and media referencing the particular technology, and may refer to publicly available cloud applications or a cloud limited to a particular enterprise.[19] Cloud computing essentially seeks to increase the ease-of-use and flexibility of the benefits offered by engaging with technology.[20] When using a cloud service provider, information can be accessed from the Internet or private network on mobile devices, whenever the user needs it, making the software programs and accompanying data that much more attractive to businesses.[21] Businesses no longer rely on old methods of maintaining information in an off-storage location like inexpensive magnetic tapes used with large mainframe computers.[22] Cloud computing services allow businesses to "retrieve, edit[,] and store corporate records and information wherever they are in the world."[23] This sort of self-service, on-demand aspect of cloud computing means that information is not limited to being transmitted solely from point A to point B, like for example, sending information via the postal service.

In recent years, computer programs have been created to not only cure cancer, but to also solve the energy crisis.[24] Now, cloud computing technology is reshaping the way we live and work. It has also served as a driving force in the American economy, where businesses are more

17. Almeling, *supra* note 15, at 1098.

18. SunGard Availability Services, *White Paper Series: Security in the Cloud* 6 (2013), http://resources.idgenterprise.com/original/AST-0079600_cloud-services-security-in-the-cloud-CLD-WPS-057.pdf.

19. IAN C. BALLON, 5 E-COMMERCE & INTERNET LAW 50.02 (2d ed. 2001), Westlaw (database updated 2016).

20. W. Michael Ryan & Christopher M. Loeffler, *Insights Into Cloud Computing*, 22 INTELL. PROP. & TECH. L.J. 22 (2010).

21. *Id.*

22. *See* John Taffinder, *Mainframe tape backup: Vintage or outdated?*, COMPUTERWEEKLY.COM (Jun. 7, 2011), http://www.computerweekly.com/tip/Mainframe-tape-backup-Vintage-or-outdated.

23. BALLON, *supra* note 19.

24. *E.g.*, Amelia Heathman, *Microsoft wants to 'solve' cancer in the next 10 years using AI*, WIRED U.K. (Sept. 20, 2016), http://www.wired.co.uk/article/microsoft-solve-cancer-computer-science; *see also* Rinkesh Kukreja, *What is the Energy Crisis?*, CONSERVE ENERGY FUTURE BLOG, http://www.conserve-energy-future.com/causes-and-solutions-to-the-global-energy-crisis.php (last visited Dec. 11, 2017).

reliant on informational assets.[25] Subsequently, we should not be surprised that cloud computing has allowed businesses to improve system availability, bring technological products to market faster, make smarter decisions about inventory, and free up resources to invest in measurable outcomes for customers.[26]

In business environments, cloud computing certainly has its advantages over traditional software programs. First and foremost, it is easy to use.[27] Traditional software programs require a user to frequently update the software to keep the program operating smoothly.[28] In cloud services, vendors can install upgrades while the application remains "operating-system independent," so there is no worry about compatibility when using different computer operating systems.[29] Cloud computing can also be a cost savings mechanism for businesses that would otherwise have to purchase, install, and maintain rather sophisticated hardware and software for data storage. This is not to say that businesses will forego purchasing alternative back-up services because in reality, the information stored in the cloud should still be backed-up on an in-house server. Unlike traditional data storage programs, cloud computing allows businesses to log into a web browser for a monthly fee, as opposed to maintaining complicated software licenses.[30] Businesses can retrieve files from traditional storage devices and place them on networks such as, OneDrive, Dropbox, and iCloud, all of which provide the convenient storage of documents, media, and text files.[31] Businesses find cloud computing more appealing than traditional storage programs, because efforts to set-up and run the services are greatly diminished, allowing businesses more time for strategic planning and innovation.

Since the early 1970s, businesses have transitioned from storing information in physical "locked rooms . . . to magnetic tape, hard drives, floppy disks, jump drives,"[32] or a combination of devices. Businesses in possession of valuable trade secret information should ask themselves if now is the time to go back to the days of pen, paper, and locked boxes. The easy answer to this question is no because it is likely not feasible for many businesses of any size to operate on pen and paper from a purely economic standpoint.[33]

---

25. Almeling, *supra* note 15.

26. Philip Guido, *Three Companies That Transformed Their Businesses Using Cloud Computing*, FORBES (Nov. 3, 2014, 9:51 AM), http://www.forbes.com/sites/ibm/2014/11/03/three-companies-that-transformed-their-businesses-using-cloud-computing/#3d40530f326d.

27. Shawn L, Holahan, *Silver Lining in That Cloud*, 60 LA. B.J. 320 (2013).

28. *Id.*

29. *Id.*

30. *Id.*

31. BALLON, *supra* note 19.

32. Sandeen, *supra* note 12, at 444.

33. Robert D. Atkinson et al., *The Internet Economy 25 Years After .Com: Transforming Commerce & Life*, THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Mar. 2010), http://www.itif.org/files/2010-25-years.pdf (noting that over the past two decades,

Cloud computing, while extremely beneficial, does not come without its drawbacks. Business entities face a legal risk when engaging in a cloud service, whether public or private, to protect their proprietary trade secret information; "the digital world is no friend to trade secrets."[34] In the past, maintaining important information via pen and paper meant that businesses generally only needed to invest in a sturdy lock or a vault to protect trade secrets.[35] Subsequently, if anyone attempted to misappropriate the secret information, the thief would have to either gain the appropriate access or breach company trust and a duty of confidentiality by breaking into the locked facility.[36] That person could then easily copy, download or upload the materials, and smuggle them from the company.[37] Even if the company had a secure network, one who had legitimate access to the servers and misappropriated the information could post the company's confidential information on the Internet for all to see. Depending on where the information was posted, it could have severely negative repercussions for the business.

Since the turn of the century, the volume of hackers breaking into business' information generally stored in a cloud has been on the rise. In 2002, the FBI handled almost 1,500 hacking cases.[38] That number practically doubled in 2010, during which the FBI handled more than 2,500 hacking cases.[39] One of the biggest reasons for the increase in attacks is that it is difficult to catch and punish infringers. The majority of hackers are able to cover their tracks without leaving a single trace. Businesses must take all precautions in protecting their trade secrets from misappropriation. They must steer clear of potential security breaches, data corruption, or bugs in the information technology environment.[40] Businesses can never be too careful in assessing all possible risks. The following section provides recommendations to businesses in light of the Defend Trade Secrets Act[41] to protect their trade secret information.

---

information technology has made the U.S. economy over $1.2 trillion larger in terms of annual gross domestic product).

34. Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 361 (2009).

35. Sandeen, *supra* note 12, at 444.

36. *Id.*

37. Almeling, *supra* note 15, at 1098–99.

38. Devlin Barrett, *U.S. Outgunned in Hacker War* (Mar. 28, 2012, 10:31 AM), WALL ST. J., https://www.wsj.com/articles/SB10001424052702304177104577307773326180032.

39. *Id.*

40. Holahan, *supra* note 27.

41. 18 U.S.C. § 1836(b)(1) (2016).

II. PREVENTING MISAPPROPRIATION: RECOMMENDATIONS FOR BUSINESSES IN LIGHT OF THE DEFEND TRADE SECRETS ACT[42]

A business' trade secret may be protected without any procedural formalities. The other forms of intellectual property protection require registration, fees and/or some physical representation of ownership.[43] Generally, the only requirement for trade secret protection is the information must be kept secret, meaning it is not generally known among others in the industry and is not readily accessible.[44] Before there was a federal law regulating trade secrets, courts found that a plaintiff had satisfied the confidentiality requirement if efforts were "rigorous enough to force another to use improper, unethical or illegal means to discover or make use of one's trade secrets."[45]

Now, federal law governing trade secret misappropriation has been implemented. The Defend Trade Secrets Act of 2016 was signed by President Barack Obama on May 11th with the overwhelming support of Congress.[46] The DTSA allows a trade secret owner to file a civil right of action in a United States district court and seek relief for trade secret theft related to a product or service in interstate or foreign commerce regardless of the amount in controversy.[47] The DTSA is known as "the most sweeping change to the nation's intellectual property laws" since the Lanham Act for trademarks was passed in 1946.[48]

Enacting the DTSA ended the bipartisan effort to bring trade secret protection under the federal system of law. Under the Uniform Trade Secrets Act (UTSA), an entity could only bring civil actions in state court under state law for violations of trade secret rules.[49] The UTSA brought uniformity across the patchwork of state laws. Every state, with the exception of New York and Massachusetts has adopted some form of the UTSA.[50] The DTSA amends the Economic

---

42. *Id.*

43. *See generally* WORLD INTELLECTUAL PROPERTY ORGANIZATION, WHAT IS INTELLECTUAL PROPERTY? (2011), http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.

44. *See* Bret A. Cohen et al., *Explaining the Defend Trade Secrets Act*, AMERICAN BAR ASSOCIATION: BUSINESS LAW TODAY (Sept. 2016), https://www.americanbar.org/content/dam/aba/publications/blt/2016/09/trade-secrets-201609.authcheckdam.pdf.

45. David W. Slaby et al., *Trade Secret Protection: An Analysis of the Concept Efforts Reasonable Under the Circumstances to Maintain Secrecy*, 5 SANTA CLARA HIGH TECH. L.J. 321, 324 (1989).

46. *Defend Trade Secrets Act*, WIKIPEDIA, https://en.wikipedia.org/wiki/Defend_Trade_Secrets_Act (last updated Nov. 22, 2017, 4:59 PM).

47. 18 U.S.C. § 1836(b)(1) (2016).

48. David C. Berry & John Halan, *"Defend Trade Secrets Act" Signed Into Law Effective May 11, 2016*, BROOKS KUSHMAN (May 19, 2016), https://www.brookskushman.com/news/client-alerts/defend-trade-secrets-act/.

49. UNIFORM TRADE SECRETS ACT, 14 U.L.A. 539-40 Prefatory Note (1986), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

50. *Legislative Fact Sheet – Trade Secrets Act*, UNIFORM LAW COMMISSION,

Espionage Act of 1996[51] and attempts to harmonize divergent state laws by creating a single framework for trade secret misappropriation lawsuits and a uniform body of case law for trade secret disputes. Additionally, it underscores Congress's desire to align closely with the UTSA. The DTSA explicitly indicates that it does not eliminate or preempt state laws already conferring trade secrets protection, but instead strives to cause federal and state standards to co-exist as a supplement of one another, as is the case in wage-and-hour laws.[52] An additional provision of the DTSA is that it gives a broader definition of "trade secret," as information that the owner has taken reasonable steps to keep secret and from which value is derived because others do not know it.[53]

The presence of the DTSA as federal trade secret protection law by no accounts means that businesses can take their hands off the proverbial "security steering wheel" when engaging with a cloud storage medium. Businesses should instead view the DTSA with greater clarity and predictability across the United States. By engaging with cloud computing services, businesses must take extra precautions to protect their trade secrets against misappropriation by using a combination of passwords, firewalls, fingerprints, facial recognition, and encryption, among a variety of other security measures.[54]

Employers should strive to ensure that new employees, in addition to independent consultants and contractors, are well-educated about the importance of trade secrets, are aware of the respective business policies and procedures, and have signed confidentiality agreements prior to starting work. These policies include monitoring and limiting employee's access to cloud services that house trade secrets. Effective communication is of utmost importance in making sure that employees understand employers' expectations, and that each party gains mutual respect for each other.

Furthermore, businesses must take precautions in the event that an employee steals a trade secret and tries to disseminate it to members of the industry or general public. The DTSA allows a trade secret

---

http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited Dec. 11, 2017) (listing states that have enacted a form of the Uniform Trade Secrets Act; amended forms of the Uniform Trade Secrets Act were introduced in Massachusetts and New York in 2015).

51. ECONOMIC ESPIONAGE ACT OF 1996, 18 U.S.C. § 1831 (1996).

52. *See* Cohen et al., *supra* note 44, at 3.

53. *See* Cohen et al., *supra* note 44, at 1; *see also* 18 U.S.C. § 1839(3) (2016) ("The term "trade secret" means all 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.").

54. Sandeen, *supra* note 12.

owner to have law enforcement officials seize property of allegedly misappropriated trade secrets and the electronic devices in which trade secrets may be stored without advanced notice to the accused, in order to prevent dissemination of the trade secrets at issue.[55] For a court to issue a seizure of property, it must first meet the following three requirements: (1) a temporary restraining order or another form of equitable relief must be found to be inadequate,[56] (2) an immediate and irreparable injury will occur if seizure is not ordered,[57] and (3) the person against whom the seizure would be ordered has actual possession of the trade secret and any property to be seized.[58] The defendant-employee also has the right to challenge an improper seizure of property.[59] To combat the possible risk of abuse, this provision in the DTSA is constrained to serve as a high bar for plaintiff-employer, meaning that seizures are to be used only in defined "extraordinary circumstances," where a defendant-employee may flee the country or is planning to immediately disclose the trade secret to a third party.[60] The applicant requesting a seizure must show that the accused person would evade an ordinary injunction and that the accused person would destroy or hide the property if such person were given advance notice.[61]

Businesses with trade secret information should be cautious in assigning new employees to work on projects and assignments that are substantially similar to what they had worked on at their previous employer. This does not mean that incoming employees are restricted from using the particular skillsets, which make them valuable. Rather, businesses should make use of an employee's knowledge and capabilities, but not compromise the trade secret information that the employee may have acquired while working for the previous employer. Employees benefit from DTSA protections employees in the event that a previous employer files an injunction against them as a means to prevent them from engaging in work with the new employer. The DTSA provides that an employee may not be prevented from entering into an employment relationship solely on the basis of the information that the employee knows.[62] Instead, there must be evidence that the trade secret information at issue will actually be misappropriated.[63]

---

55. 18 U.S.C. § 1836(b)(2)(A)(i) (2016) (Items that may be seized include laptops, servers, storage devices, and papers, among a variety of other devices. The main requirement in this provision is that the seizure must be "necessary to prevent the propagation or dissemination of the trade secret.").

56. 18 U.S.C. § 1836(b)(2)(A)(ii)(I) (2016).

57. 18 U.S.C. § 1836(b)(2)(A)(ii)(II) (2016).

58. 18 U.S.C. § 1836(b)(2)(A)(ii)(V) (2016).

59. 18 U.S.C. § 1836(b)(1) (2016).

60. 18 U.S.C. § 1836(b)(2)(A)(i) (2016).

61. 18 U.S.C. § 1836(b)(2)(A)(ii)(VII) (2016).

62. 18 U.S.C. § 1836(b)(3)(A)(i)(I) (2016).

63. *Id.*

Without that actual or threatened piece of information, the injunction against the employee would fail.

The DTSA has measures in place in order to prevent against the dissemination of a business' trade secret information. The DTSA has a whistleblower / anti-retaliation provision, providing civil and criminal immunity to individuals who may need to disclose trade secrets.[64] The DTSA requires that employers provide notice of the immunity provision to their employees, consultants, and independent contractors in order to be able to take advantage of the full range of remedies.[65] These remedies include actual damages, exemplary damages, compensatory damages, unjust enrichment damages, injunctive relief, and reasonable attorney's fees for actions brought in bad faith[66] by looking at the "circumstantial evidence."[67] Employers may satisfy that obligation by cross-referencing a whistleblower policy that sets forth the protocol for reporting suspected violations of law in various documents and agreements, which are included in employee handbooks.

Employers should keep notes of the information that employees possess from previous employers to demonstrate that the knowledge used on projects at the new employer was acquired in the current job and not taken from a previous employer. In addition, employers should remind employees that they cannot take trade secret information with them when they leave the company. Employers should have a signed agreement of the employee's understanding in writing, so that the employee knows that the trade secret remains with the company once they leave. Furthermore, employers should update existing contracts to comply with the DTSA. For instance, they should make sure that the intellectual property agreements, employment agreements, consulting agreements, joint development agreements, and licensing agreements indicate what duties and responsibilities are expected of the parties. Lastly, employers should document trade secret information (for protection in the event of litigation), and be aware of the differences between federal law (i.e. DTSA) and state law (i.e. UTSA) remedies when deciding whether to bring a cause of action against a potential defendant-employee.

Businesses must be aware of the security offered by their cloud computing service providers and must fully understand the advantages and disadvantages compared to traditional non-cloud computing

64. 18 U.S.C. § 1833(b)(1–2) (2016) (An employee will not be "held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is made in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.").

65. *See* Cohen et al., *supra* note 44, at 2.

66. 18 U.S.C. § 1836(b)(3)(D) (2016).

67. *Id.*

services. Free service providers like Google Drive and Dropbox may put client information at risk in the event of lost data. Some service providers reserve the right to access their customer's stored content and are generally unwilling to enter into an express confidentiality agreement.[68] In the event that the business enters into an agreement with a free service provider, the free service provider would claim no liability, and there is the risk that trade secret information, placed in the free application, gets leaked to advertisers or third parties.[69] Herein lies the importance of businesses reading through the language of the terms of service and privacy policies with a fine-tooth comb. In addition, businesses must make sure that they encrypt client information and know which individuals in the business have access to the respective data. Businesses should have a reliable backup for data stored in the cloud, including but not limited to providers, such as Amazon S3, Rackspace, and SAS 70.[70]

Risk management is a top priority for businesses that choose to engage with cloud service providers. Businesses need to ensure that technical documents (ex. in regards to onboarding process) are regularly updated and tailored to their specific jurisdictions (ex. regarding punitive damages). They must consider what would happen if their cloud computing service provider goes out of business or declares bankruptcy. To this end, it would be useful to work with a cloud service provider that can provide local copies of data in the event of insolvency or if the service provider is served with a subpoena.[71] Another consideration is thinking about what will happen to information stored in the cloud in the event that the business decides to terminate its contractual relationship with the cloud service provider.

III. THE FUTURE OF CLOUD COMPUTING TECHNOLOGY TO PROTECT TRADE SECRETS

Trade secrets are produced by spending millions of dollars and many years on research and development. As such, the importance of protecting trade secrets in the United States economy has increased due to emerging technologies like cloud computing services, which allow users to access information from wherever they are. Individuals open valuable information up to theft when accessing cloud-based information on open Wi-Fi networks in places like Starbucks, Dunkin Donuts, Apple Store, Target, Barnes & Noble, and Best Buy or even more generally in larger public places like hotels, libraries, airports, gyms, parks, hospitals, and museums.

68. Sandeen, *supra* note 12, at 450–51.
69. Holahan, *supra* note 27, at 321.
70. Holahan, *supra* note 27, at 321.
71. Holahan, *supra* note 27, at 321.

When cloud computing emerged, businesses and attorneys analyzed the benefits and potential problems. The easy solution was to disregard cloud services for storing trade secrets because of the added level of effort required for protection. A trade secret holder would have to add protections to its own facility, as well as protections on the cloud computing facility. Businesses should look to the DTSA as an incentive to keep innovation moving forward. Under both the UTSA and the DTSA, courts should not force a company to make all possibly conceivable efforts to maintain secrecy. Rather, courts should defer to legislative text and historical precedent to require the trade secret holder to take reasonable steps under the circumstances to maintain the secrecy of the valuable information.

Developments like cloud computing certainly make it easier to create, store, and transmit information, in an electronic format, as noted in earlier sections. However, it can also cause data stored in a cloud to be more susceptible to trade secret theft.[72] Hackers, both nationally and internationally, are becoming more adept and present themselves as a constant threat to businesses, which is certainly likely to continue.[73] Hackers no longer need to be physically present in order to steal a trade secret from a locked combination box. Where sensitive trade secret data exists with more locations to store it, businesses should acknowledge that they fall into one of two categories: (1) companies that know they have been hacked or (2) companies who do not know it yet. In a study conducted by the computer security firm, Mandiant, researchers found that in cases involving Chinese hackers intruding into a firm, ninety-four percent (94%) of targeted companies were completely unaware of the breach until someone else told them.[74] What was worse was the length of time between when the breach happened and when businesses were actually notified of the breach. The median number of days between the two instances was 416.[75]

As international trade secret misappropriation continues to rise, the difficulty will be in enforcing the DTSA. U.S. courts may not be able to easily enforce the DTSA if misappropriation occurs in a foreign country.[76] President Barack Obama made the following statement

---

72. *Administration Strategy On Mitigating The Theft Of U.S. Trade Secrets*, EXEC. OFF. OF THE PRESIDENT OF THE U.S. GOV.T 8 (Feb. 2013), https://obamawhitehouse.archives.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

73. *Foreign Spies Stealing US Economic Secrets In Cyberspace*, THE OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC. 10 (Oct. 2011), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf; *see also Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats*, CREATE.ORG & PWC LLP 12 (Feb. 2014), https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

74. Barret, *supra* note 38.

75. Barret, *supra* note 38.

76. *See* TianRui Group Co. Ltd. et al. v. Int'l Trade Comm'n, 661 F.3d 1322 (Fed. Cir. 2011) (finding that the U.S. International Trade Commission had jurisdiction to address trade secret

concerning how China views the theft of trade secrets as an aid to their development:

> Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical advancement, and growth of the renewable energy sector. China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal trade secrets using removable media devices or e-mail.[77]

Not only is it difficult to obtain justice in a foreign country because of the variations in judicial procedures and trade secret protection, but enforcement itself can be a very complicated and an expensive burden that business may simply not be willing to take on.

CONCLUSION

In conclusion, trade secrecy involves legal knowledge, as well as knowledge of technology, politics, economics and other factors that affect the misuse of trade secrets.[78] With the technological advancements made, it is difficult to imagine going back to an era where businesses use pen, paper, and lock boxes as the standard method to protect trade secrets. Rather, with the continued development of software and cloud computing services the standard for operational excellence and accelerated innovation will continue to change. While cloud computing offers trade secret holders a viable storage medium to keep information away from competitors and misappropriation, businesses must make the ultimate decision of how much effort to invest in protecting its information stored on cloud services. Local, regional, and national laws are continuing to converge to create boundaries for protecting proprietary and trade secret information. With time, courts will become more comfortable with enforcing the DTSA, and this will likely incentivize businesses to file more federal trade secret cases. Businesses will continue to see the advantages in using cloud service providers as development of the cloud space increases, ultimately resulting in better and more reliable products and services. In the meantime, businesses should look to leading practices and investigate what procedures other competing and allied companies are engaging in to protect their information. The security of the businesses' proprietary information depends on it.

misappropriation that occurs in a foreign country, but in other situations, the presumption against extraterritoriality would govern).

77. *Foreign Spies Stealing US Economic Secrets In Cyberspace*, *supra* note 73, at 5.

78. Almeling, *supra* note 15, at 1117.