VIRGINIA JOURNAL OF LAW & TECHNOLOGY

FALL 2014 UNIVERSITY OF VIRGINIA VOL. 19, NO. 01

Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection

SHARON K. SANDEEN†

© 2014 Virginia Journal of Law & Technology Association, *at* http://www.vjolt.net.

† Professor of Law, Hamline University School of Law, Saint Paul, Minnesota. Because I have been working on this Article for several years, I have many people to thank for their assistance with research and for critiques of earlier drafts of this article. The Research Assistants who have worked on this project include: Amelia Vnuk, Colin Thomsen, Jessica Alm, Michael Mangold, Lauren Dwyer, Nick Datzov, Selena Marchan, and Lisa Valatutti. I am also grateful for feedback from other members of the Trade Secret Scholars community, including Professor Elizabeth Rowe and Professor David S. Levine. I must also thank Professor Jeannie Fromer and Professor Sonia Katyal for inviting me to present an early version of this Article to their IP Scholarship class at Fordham in early 2010 and appreciate the feedback that their students provided.

ABSTRACT

This Article explores whether trade secrets lose their status as trade secrets by being uploaded to computer servers owned by cloud service providers. Although some think this question can be answered easily by determining if the information is subject to reasonable efforts to maintain its secrecy, due to the third party doctrine of trade secret law and the practices of cloud service providers, the answer is not so simple. The third party doctrine, although somewhat related to the reasonable efforts requirement, is a distinct concept that cannot be ignored. After first explaining the scope and purpose of third party doctrine and how it puts trade secrets stored in the cloud at risk, the author proposes a method of analysis for distinguishing between trade secrecy waiving "disclosures" and non-trade secrecy waiving "mere transfers." This Article also provides a classification scheme for the various types of disclosure under trade secret law.

TABLE OF CONTENTS

I. INTRODUCTION

Over the past ten years, "cloud computing" has evolved from a clever yet misunderstood term of art into a thriving industry featuring all of the big names in the computer industry, the Internet, and telecommunications —including IBM, Microsoft, Google, Amazon, Dell, and Verizon. Apparently first coined as a term for the next generation of computer services in 2005,[1] the meaning and scope of cloud computing has been debated.[2] Some

---

[1] RackSpace claims to have developed the idea in 2005 or at least, embraced the idea of two unidentified developers. *See About Us*, THE RACKSPACE CLOUD, *available at* https://web.archive.org/web/20090721020002/http://www.rackspacecloud.com/aboutus/story (last visited Oct. 19, 2014). At the Web 2.0 Summit in November 2006, Jeff Bezos announced Amazon's Electric Compute Cloud service. *See* Alan Sipress, *At Web 2.0 Summit, A Look at What's in Store (and Storage)*, WASH. POST, Nov. 9, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/11/08/AR2006110802094.html. Dell tried, unsuccessfully, to trademark the term in 2007. *See* U.S. Trademark Application Serial No. 77139082 (filed Mar. 23, 2007). A company by the name of NetCentric Corporation applied to register the term "cloud computing" for use in conjunction with educational services in 1997, but the application was abandoned for failure to file a statement of use. *See* U.S. Trademark Application Serial No. 75291765 (filed May 14, 1997).

[2] In a September 2011 report, the National Institute of Standards and Technology stated that "[c]loud computing is an evolving paradigm," but nonetheless defined cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COM., THE NIST DEFINITION OF CLOUD COMPUTING 1–2 (2011). The report goes on to explain the "cloud model is composed of five essential characteristics**,** three service models, and four deployment models." *Id.*

people define it broadly to include a range of computer services that are available over the Internet, with "the cloud" simply being a metaphor for the Internet.[3] Others use the term to differentiate their services from the broader Internet by, for instance, focusing on a pay-for-play payment structure or the provision of discrete services over the Internet, such a web-hosting, infrastructure-as-a-service, and software-as-a-service.[4] Still others refer to "the cloud" as a place to store, retrieve, and use vast amounts of information.[5]

The focus of this Article is on cloud-based services, however labeled, that offer businesses the ability to upload and store information and data remotely via the Internet (hereinafter "cloud storage services"). This might include back-up and processing services akin to earlier service bureaus or data centers that are specifically designed and marketed to allow customers to store data. It can also include services that appear (at least on the surface) to be more benign, such as

---

[3] *See* Vangie Beal, *Cloud Computing (The Cloud)*, WEBOPEDIA, http://www.webopedia.com/TERM/C/cloud_computing.html (last visited Oct. 19, 2014).

[4] *See, e.g.*, Amazon Web Services, *What is Cloud Computing*, AMAZON WEB SERVS., *available at* http://aws.amazon.com/what-is-cloud-computing/?sc_channel=PS&sc_campaign=AWS_Free_Tier_2013&sc_country=US&sc_publisher=Google&sc_medium=Nonbrand_Cloud_Computing_B&sc_content=36175397442&sc_detail=Clouds+computing&sc_category=aws_cloud_computing&sc_se (last visited Oct. 19, 2014) ("'Cloud Computing' … refers to the on-demand delivery of IT resources and applications via the Internet with pay-as-you-go pricing.").

[5] Examples of cloud storage services include Amazon's EC2 service and Google's Google Docs and GoogleDrive services, as well as companies that focus on providing storage solutions such as DropBox and RackSpace.

Gmail[6] and Sony's PlayStation Network.[7] Indeed, if you use modern-day technologies such as cellphones, cable television, and tablet computers, chances are that your service providers offer the "convenience" of storing a wide-variety of information that can be remotely accessed via those devices.[8]

As touted by many cloud storage services, businesses around the world can reduce the costs of acquiring and maintaining their computer systems by storing their documents and data in the cloud.[9] Significantly, instead of having to

---

[6] *See In re* Google Inc. Gmail Litig., 2014 U.S. Dist. LEXIS 36957, *26–27 (N.D. Cal. Mar. 18, 2014) (describing Gmail and the privacy concerns it raises).

[7] *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 950–51 (S.D. Cal. 2012) (describing the PlayStation Network and Sony's (then existing) privacy policies).

[8] *See Google Terms of Service*, GOOGLE, http://www.google.com/policies/terms (last visited Oct. 19, 2014) ("When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps).").

[9] *See, e.g.*, *Cloud Services*, AT&T, http://www.business.att.com/enterprise/Portfolio/cloud/?wtPaidSearchTerm=cloud&wtpdsrchpcmt=cloud&WT.srch=1&source=EENT44MECCekGpIV4&wtpdsrchprg=Enterprise+-+Cloud+Services&wtpdsrchgp=ABS_SEARCH (last visited Oct. 19, 2014) ("With cloud solutions, IT services are procured on an as needed basis, rather than procuring capital expense assets. Instead of investing in equipment, you buy access to cloud computing, cloud storage, platforms

acquire and maintain an expensive array of centralized servers, businesses can utilize the server capacity of another that promises to be available 24/7 and to provide scalable capacity for all of its clients' needs. An added benefit of these services is that the stored information can be retrieved anywhere in the world via the Internet, thereby facilitating the use, sharing, and editing of information among multiple persons and entities and across jurisdictional boundaries. What these services do not always promise, particularly with respect to the so-called "public cloud," is that the stored information will be maintained in confidence.[10] Rather, in order to limit potential

---

and other resources on demand over the network, likely reducing: capital investments; IT spend; lengthy turnaround times; service-contract terms").

[10] *See* SIMON BRADSHAW ET AL., QUEEN MARY UNIV. OF LONDON, SCH. OF LAW, LEGAL STUDIES RESEARCH PAPER NO. 63, CONTRACTS FOR CLOUDS: COMPARISON AND ANALYSIS OF THE TERMS AND CONDITIONS OF CLOUD COMPUTING SERVICES 21 (2010) ("Our survey found however that most providers not only avoided giving undertakings in respect of data integrity but actually disclaimed liability for it."). Perhaps responding to the need for more security and confidentiality in the cloud, many of the storage services are careful to differentiate between storage of information in the "public cloud" and the "private cloud." According to the National Institute of Standards and Technology, the varying cloud deployment models are defined as follows:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

liability, the form terms of services agreements used by cloud storage services often disclaim responsibility for the security of information stored by their customers and are careful not to make any express promises of confidentiality.[11] This raises the question: Assuming the information stored in the cloud includes some trade secrets, to what extent does the use of cloud storage services undermine the trade secrecy of that information?

Although businesses have been using third party vendors for decades to store hard-copies of business records and to back-up computer data (usually off-site),[12] no reported cases were found concerning the consequences of such actions on the trade secret status of the stored information.[13] This fact

---

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

MELL & GRANCE, *supra* note 2, at 3. Significantly for the purpose of this Article, all four deployment models may involve the storage of information on the servers of another, including third parties.

[11] BRADSHAW ET AL., *supra* note 10, at 21–22; *see also infra* Part III.

[12] *See infra* text accompanying note 44.

[13] A case was found involving competing time-share companies, but it concerned alleged trade secret misappropriation related to a business agreement to share software. *See* Com-Share, Inc. v. Computer Complex, Inc., 338 F. Supp. 1229, 1236 (E.D. Mich. 1971), *aff'd*, 458 F.2d. 1341 (6th Cir. 1972); *see also* Oshno Int'l Found. v. O'Neill, No. FSTCV106004365S, 2010 WL 3960802 (Conn. Super. Ct. Sept. 8, 2010)

may lead some to believe that the answer to the foregoing question is easy, but there are at least two reasons why the "old-school" (and continuing) practice of securing or "vaulting" business documents is not the same as storing them in the cloud.[14] First, the primary purpose of data vaulting is to store information in a remote location as a back-up copy of the same information stored elsewhere. Although the act of initiating back-up storage may involve some network connectivity via the Internet or a private network, it does not involve the "on demand self-service" and "broad network access" that the National Institute of Standards and Technology (NIST) says are essential characteristics of cloud computing.[15] In other words, as used herein, data vaulting does not allow

---

(involving information stored in a self-storage facility but the case was decided without discussing the third party doctrine).

[14] According to Webopedia, "vaulting" means "the process of sending data off-site, where it can be protected from hardware failures, theft and other threats" and is also referred to as "remote back-up services." *Data Vaulting*, WEBOPEDIA, http://www.webopedia.com/TERM/D/data_vaulting.html (last visited Oct. 19, 2014).

[15] MELL & GRANCE, *supra* note 2, at 2. As described in a 1981 article that detailed the early history of the computer industry, including the practices of service bureaus: "In many cases the data to be processed are transcribed on conventional paper forms and mailed or delivered to the service bureau on conventional paper forms them and returns the results. But access to the service bureau computer may be direct via 'modem.'" Walter E. Schmidt, *Legal Proprietary Interests in Computer Programs: The American Experience*, 21 Jurimetrics J. 345, 378 (1981). *See also* W. KUAN HON & CHRISTOPHER MILLARD, CLOUD COMPUTING VS. TRADITIONAL OUTSOURCING—KEY DIFFERENCES, SOCIAL SCI. RES. NETWORK, *available at* http://ssrn.com/abstract=2200592 (last visited Oct. 19, 2014) ("Current laws envisage traditional outsourcing and the stand-alone databases in use when they are drafted. They do not cater adequately for differences arising from service type, particularly with public shared[–]infrastructure IaaS and PaaS (i[.]e[.,] infrastructure services), or differences arising from individual services' designs." (footnote omitted)).

stored information to be accessed and used on a regular basis by either the customer or the storage service.[16] This is not the case with some cloud storage services, many of which reserve the right to access, and potentially use all or a portion of a customer's stored information.[17] Second, unlike many cloud storage services, companies that provide data vaulting services are usually willing to make express promises of confidentiality and security that do not implicate the third party doctrine of trade secret law, discussed *infra*.[18] Indeed, for companies that are under a legal obligation to secure data (including healthcare and financial institutions), it is the promise of adequate database security that usually drives the selection of a vaulting service.[19] In contrast, what often drives the selection of a cloud

---

[16] As discussed *infra*, this distinction also explains the limited applicability of the Stored Communications Act. *See infra* text accompanying notes 261 & 269.

[17] *See infra* text accompanying note 85.

[18] *See infra* Part II.C. Modern day companies that focus on providing back-up services or excess server capacity are willing to provide such promises but usually at an increased cost over free or low-cost cloud storage providers. *See* BRADSHAW ET AL., *supra* note 11, at 22 ("A small number of the providers surveyed give more positive assurances. For example, Salesforce CRM's T&C [Terms & Conditions] state that appropriate measures will be taken to safeguard customer data. It is interesting to note that two providers offering specific backup services, Symantec and Iron Mountain, make no mention of data integrity in their T&C. It may well be that both providers assume it to be implicit from the nature of their service.").

[19] For data security purposes (as opposed to trade secret and privacy purposes), legal and industry standards have been (and continue to be) developed by various private, semi-private, and public institution. *See, e.g.*, U.S. NAT'L SEC. AGENCY & U.S. CENT. SEC. SERV., INFORMATION ASSURANCE DIRECTORATE: CGS IA POLICIES, PROCEDURES, AND STANDARDS CAPABILITY (2012), *available at* http://iase.disa.mil/cgs/Documents/IA_Policies_Procedures_Standards_v.1.1.1.pdf; – *Payment Card Industry (PCI) Security Standards Council (SSC)*

storage service is the ability to quickly and easily access stored information and to make available or share that information with multiple individuals both inside and outside a business.[20]

While businesses obviously have an interest in maintaining the confidentiality of the information they possess, there is no general right to keep business information confidential. Rather, the general rule is that business information, like all information, is not protected if it is voluntarily (or in many cases, involuntarily) disseminated to others.[21] Businesses who want to maintain the confidentiality of their information can always engage in self-help in an effort to maintain actual secrecy, but if those efforts are insufficient and their information falls into the hands of another, then the

---

Data Security Standards Overview, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/ (last visited Oct. 19, 2014). Whether these measures also suffice for trade secret purposes would depend upon whether they are "reasonable under the circumstances" to protect the subject trade secrets.

[20] Dropbox is an example of a service that gives multiple people the ability to share information and collaborate on the formulation of information and where such collaboration is a key selling point. *See* DROPBOX, https://www.dropbox.com/business (last visited Nov. 3, 2014) (touting the benefit of collaboration).

[21] *See, e.g.*, RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939) ("The privilege to compete with others . . . includes a privilege to adopt their business methods, ideas or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition."); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1 cmt. A (1995) ("The freedom to engage in business and to compete for the patronage of prospective customers is a fundamental premise of the free enterprise system."); ROGER M. MILGRIM & ERIC E. BENSEN, 1 MILGRIM ON TRADE SECRETS § 1.05[2] (2014) ("The courts do not prevent or punish copying of another's disclosed ideas unless such copying is prohibited by valid contract, or under patent, copyright, or trademark law.").

only way to stop the further disclosure or use of the information is to seek relief in a court of law. Generally, this can be accomplished in one of four ways: (1) by demonstrating that the information is protected by patent or copyright law, in which case the use of the information is restricted in accordance with the exclusive rights of the patent and copyright owner;[22] (2) by proving that the other person is under a contractual duty to maintain the confidentiality of the information, in which case the information owner is entitled to remedies for breach of contract if the information is disclosed or used in contravention of the terms of the contract;[23] (3) by establishing that the other person is under a statutory, common law, or professional duty to maintain the confidentiality of the information;[24] or (4) by proving that the information is a trade secret that was misappropriated.[25]

This Article focuses on whether trade secret protection can be used to protect information that is stored in the cloud

---

[22] *See* 17 U.S.C. § 106 (2012); 35 U.S.C. § 271.

[23] *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 300 (1998); Sharon K. Sandeen, *A Contract by Any Other Name is Still a Contract: Examining the Effectiveness of Trade Secret Clauses to Protect Databases*, 45 IDEA 119, 124–25 (2005) (detailing the differences between trade secret protection and protection of information and ideas pursuant to contract). The area of law referred to as "idea-submission law" is based upon contract law. *See generally* Lionel S. Sobel, *The Law of Ideas, Revisited*, 1 UCLA ENT. L. REV. 9 (1994).

[24] *See generally* FED. R. EVID. 501; s*ee also* Goldman, Sachs & Co. v. Blondis, 412 F. Supp. 286, 288 (N.D. Ill. 1976) (standing for the proposition that "by a long established and honored rule of the common law, embodied in the statutes of many states, an attorney should not, and cannot be, compelled to, testify regarding communications made to him in his professional character by his client").

[25] UNIFORM TRADE SECRETS ACT § 1(2) (1985) [hereinafter UTSA].

when the trade secret owner voluntarily and intentionally initiates an act (or series of actions) that cause such information to flow[26] from its own database storage facilities to the database storage facilities of a third party.[27] The focus on owner-initiated acts distinguishes it from earlier articles that examined the issue of trade secrecy with respect to accidental disclosures and disclosures following alleged acts of misappropriation.[28] This Article is also distinguishable from

---

[26] In order not to pre-judge the degree of "disclosure" that occurs when information is stored in the cloud, the author use the term "information flow" throughout this Article as a neutral term to refer to the fact that information has moved from a trade secret owner to a third party. As discussed *infra*, whether an information flow constitutes a "mere transfer" or a "disclosure" depends upon the legal and factual analysis that is detailed in this Article. *See infra* Part IV. "Third party," as used in this Article, loosely means an individual or company that is not affiliated with the trade secret owner in such a manner that the law would consider their actions to be that of the trade secret owner. *See* MILGRIM & BENSEN, *supra* note 21, § 7.02 (defining third parties as "parties who are not in any legally cognizable relationship with respect to one another except to the extent that use or disclosure of a trade secret by one of the parties may be argued to be an actionable wrong by the other"). In reality, however, these so-called "third parties" are actually "second parties" to the extent they deal directly with the trade secret owner and, thus, they may be directly liable for trade secret misappropriation if they owe a duty of confidentiality to the trade secret owner.

[27] In addition to the definition in the preceding footnote, as used herein, "third party" refers to a person or entity that, in most cases, would not be one of the parties in a trade secret misappropriation case and, thus, is a "third party" vis-à-vis the litigants. Similar to what occurs in the Fourth Amendment context, typically the defendant in a misappropriation case will point to a third party's possession of information as destroying its trade secrecy.

[28] *See, e.g.*, Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1 (2007) (describing the risks posed to trade secrets by the Internet,

ones that discuss privacy and security issues related to the Internet and the cloud because it focuses on the acts of information owners in transferring valuable business information to a third party.

Although issues of privacy and security are obviously implicated by the practice of collecting information in digital form and storing it in remote locations such as the cloud, privacy and security issues generally concern the legal obligations that are (or should be) imposed on companies that create and maintain large databases of customer information.[29] While these companies would undoubtedly claim that some or all of the customer information they store constitutes "their" trade secrets, the stored information that is the focus of this Article is not limited to customer-related or personally identifiable information but includes any information that is within the theoretical scope of trade secret protection. Pursuant to the Uniform Trade Secret Act (UTSA), this can include any "information, including a formula, pattern, compilation, program, device, method, technique, or process . . . ."[30]

Pursuant to a well-established principle of trade secret law, in order to establish and maintain information as a trade secret, information owners must engage in efforts that are

---

particularly with respect to the acts of misappropriation that lead to posting trade secrets on the Internet).

[29] UTSA § 1(4). The number of articles and books on the subject of information privacy is too great to list here. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (N.Y. Univ. Press 2004) (providing a comprehensive overview of the legal issues related to information privacy, including the cases and scholarship related thereto); Kevin Cronin, *Best Practices and the State of Information Security*, 84 CHI-KENT L. REV. 811 (2010).

[30] UTSA § 1 (defining "trade secret").

reasonable under the circumstances to maintain the secrecy of the information.[31] What is reasonable when a company is attempting to protect information intra-enterprise is different from what is reasonable when a company wishes to share information extra-enterprise.[32] When trade secrets are "disclosed" to another, what is referred to herein as "the third party doctrine of trade secret law,"[33] there exists a requirement that the disclosure occur under circumstances that give rise to a duty of confidentiality. This principle of law presents a problem for cloud storage services which carefully avoid promises of confidentiality and disclaim responsibility and liability for the security of information they store. Without a binding promise of confidentiality, companies that own trade secrets arguably waive the trade secrecy of stored information.

This Article begins by exploring the practices of the cloud storage services and the current state of trade secret law in order to identify and explain the risks posed to trade secrets and other proprietary information stored in the cloud. It begins in Part II with an overview of the current (but ever-evolving) state of the cloud computing industry, including an examination of the terms of service agreements used by several cloud storage services, particularly as they relate to the confidentiality and security of stored information. A brief explanation of the requirements for trade secret protection is provided in Part III, with particular emphasis on the reasonable efforts requirement. Part IV then explains the third party

---

[31] *Id.*

[32] *See generally* MILGRIM & BENSEN, *supra* note 21, at §§1.04–05 (discussing the maintenance of secrecy intra-enterprise and the loss of secrecy through external disclosure).

[33] There is also a third-party doctrine of Fourth Amendment jurisprudence. *See infra* notes 206–214.

doctrine of trade secret law as applied to the information flows between trade secret owners and cloud storage services.

Because the analysis of the relationship between cloud storage services and their customers leads to the conclusion that, at least in the absence of an express or implied agreement to the contrary, no duty of confidentiality is established, Part V of this Article explores potential refinements and exceptions to the third-party doctrine of trade secret law. It begins by examining the scope of the third party doctrine under existing law. Next, the meaning of disclosure under various area of law, including current trade secret law, is explored. After concluding that no existing definition of disclosure provides a workable exception to the third party doctrine of trade secret law, it is proposed that the law officially recognize a distinction between trade secrecy destroying "disclosures" and non–trade secrecy destroying "mere transfers." Borrowing from recent scholarship concerning the third-party doctrine under the Fourth Amendment and Professor Daniel Solove's "taxonomy of privacy,"[34] a number of factors are identified for differentiating between "mere transfers" of information and "disclosures."

This Article concludes with a proposed four-step analytical process. First, it should be determined if information flowed to a third party. This may require an examination of the relationship between the trade secret owner and the recipient of the information and whether they are considered part of the same entity under applicable law. Second, using a number of factors identified in this Article, the circumstances, nature and

[34] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) (differentiating between information collection, information processing, information dissemination, and invasion).

scope of the information flow should be examined to determine if there was a "disclosure" or "mere transfer" of the information. If there was a disclosure of trade secret information, then the third and fourth steps require application of the standard analysis under trade secret law: (1) it must be determined whether a duty of confidence existed between the trade secret owner and the third party; and (2) whether the trade secret owner otherwise engaged in reasonable efforts to maintain the confidentiality of its information.

II. THE CLOUD COMPUTING INDUSTRY

A. A Brief History of the Computer Industry

Depending upon who you talk to, cloud computing is either a revolutionary development or the hyped-up, repackaging of pre-existing business models. Commenting on the rush to offer cloud computing services, Larry Ellison observed:

> The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?[35]

[35] Dan Farber, *Oracle's Ellison Nails Cloud Computing*, CNET NEWS (Sept. 26, 2008, 12:09 PM), http://news.cnet.com/8301-13953_3-10052188-80.html.

As Amazon's Jeffrey Bezos put it, "We make muck so you don't have to."[36] Richard Stallman, the guru of the open software movement, paints a more nefarious picture, arguing that cloud computing is just another way by which computer and Internet companies are trying to get businesses locked into expensive proprietary systems.[37] Actually, there is truth to all three perspectives.

Anyone who is familiar with service bureaus, time-sharing, and data centers knows that the use of remote computers to process and store information is not new.[38] When the computer industry began in earnest in the late 1950s, the focus of many computer companies was on the manufacture and sale of mainframe computers for data processing use.[39] Successful companies of the time, such as IBM and Sperry-Rand, made their money building computing systems that were purchased by large institutions and companies and by programming and servicing those computers to meet the particular needs of clients.[40] Given the large investment

---

[36] Sipress, *supra* note 1.

[37] Bobbie Johnson, *Cloud Computing is a Trap, Warns GNU Founder Richard Stallman*, THE GUARDIAN (Sept. 29, 2008, 9:11 AM), http://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman.

[38] Bruce Schneier, *Cloud Computing*, SCHNEIER ON SEC. (June 4, 2009, 6:14 AM), https://www.schneier.com/blog/archives/2009/06/cloud_computing.html ("[H]ype aside, cloud computing is nothing new. It's the modern version of the timesharing model of the 1960s, which was eventually killed by the rise of the personal computer.").

[39] *See* ROY A. ALLAN, A HISTORY OF THE PERSONAL COMPUTER: THE PEOPLE AND TECHNOLOGY, pt. 1, ch. 2.1 (Allan Publ'g 2001).

[40] *See* Christopher LaMorte & John Lilly, *Computer: History and Development*, JONES TELECOMMS. & MULTIMEDIA ENCYCLOPEDIA, http://www.dia.eui.upm.es/asignatu/sis_op1/comp_hd/comp_hd.htm

associated with the purchase of early computer systems, such transactions were usually documented in individually negotiated (or negotiable) contracts that specified such matters as required deliverables, applicable deadlines, intellectual property ownership, and maintenance requirements.[41]

Given the high costs associated with purchasing and maintaining mainframe (and mini-) computers, it did not take long for the computer experts of the time to realize that there was excess computing capacity within most computers that could be used by others, provided that the technological challenges of transmitting data between computers could be solved.[42] Thus, by the late 1960s, a new computer-related industry was born: the time-sharing industry (aka service bureaus and data centers), with pioneering companies like National CSS, Inc. allowing businesses to essentially rent the

---

(describing five generations of modern computers from 1945 to the end of the twentieth century) (last visited Oct. 19, 2014); *see also* Telex Corp. v. Int'l Bus. Mach. Corp., 367 F. Supp. 258, 267 (1973) (including factual findings that describe the "electronic data processing industry" in the late 1960s and early 1970s).

[41] *See generally* RICHARD L. BERNACCHI & GERALD H. LARSEN, DATA PROCESSING CONTRACTS AND THE LAW (Little, Brown and Co. 1974); RICHARD RAYSMAN & PETER BROWN, COMPUTER LAW: DRAFTING AND NEGOTIATING FORMS AND AGREEMENTS (L. J. Press 1984).

[42] *See* John McCarthy, *Reminiscences on the Theory of Time-Sharing*, PROFESSOR JOHN MCCARTHY: FATHER OF AI, http://jmc.stanford.edu/computing-science/timesharing.html (last visited Oct. 19, 2014) ("By time-sharing, I meant an operating system that permits each user of a computer to behave as though he were in sole control of a computer, not necessarily identical with the machine on which the operating system is running."); *see also* Schmidt, *supra* note 15, at 377–78 ("The service bureau concept was developed to allow users who had no requirement for a multimillion dollar mainframe computer or even a microcomputer with all the paraphernalia and skills entailed, to nevertheless partake, for a price, in their benefits.").

use of a computer. Like the relationships that existed between the sellers and purchasers of mainframe computers (and later minicomputers), the relationships between time-sharing companies and their customers were usually defined by negotiated written agreements that included promises of confidentiality and security.[43] Also, because the data was transmitted over old-school (albeit dedicated) telephone lines using modems or off-line in a variety of storage formats (e.g., magnetic tape and floppy discs), there were more choke points along the way that could be used to control the confidentiality and security of the transmissions.

Another industry that grew out of the development of mainframe computers was the computer data storage industry, including two types of companies: those that invent and provide the necessary equipment and technology, like StorageTek, and those that use the available equipment and technology to provide storage services to businesses.[44] Even before the advent of the cloud (and since), it was recommended that companies that utilized computers in their business routinely back-up (or "vault") their important data. In this way, if the original data was lost or compromised, it could be restored using the backed-up information. Generally, this could be done in one of two ways: internally using extra computer media or server capacity or externally using the services of various providers.

---

[43] *See generally* BERNACCHI & LARSEN, *supra* note 41; RAYSMAN & BROWN, *supra* note 41.

[44] *See* Kazou Goda & Masara Kitsuregawa, *The History of Storage Systems*, 100 PROCS. OF THE IEEE 1433 (2012), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6182574.

At the same time that the data processing and storage industries were developing, efforts were undertaken to develop computer terminals that could replace the punch card and paper tape systems of data entry and that would allow mainframe and mini-computers to be accessed remotely. Early computer terminals were typically "dumb terminals" in that they only allowed for data to be entered and seen, with the host computer providing the processing power and running the software.[45] As computer technology developed throughout the 1970s and 1980s, so-called "smart" or "intelligent" terminals were developed that allowed for some processing at the terminal in addition to the host computer.[46] The development of smart computer terminals, in turn, raised issues about how a user should interface with whatever computer processing unit they were using, be it located in their home or at a remote location.

Despite the emergence of the time-sharing and data storage industries, as early as the 1960s, technology companies recognized that future growth in the computer industry would hinge on making hardware accessible to individuals.[47] The era of personal computing officially began in 1974 when Micro Instrumentation and Telemetry Systems (MITS) introduced a

---

[45] *See Dumb Terminal*, WEBOPEDIA, http://www.webopedia.com/TERM/D/dumb_terminal.html (last visited Nov. 3, 2014).

[46] *See generally* ALLAN, *supra* note 39, at pt. 2, ch. 4.1 (discussing smart terminals); s*ee also* Ron Rader, *Slow to Develop, but . . . Big Screen, 132-Column Units Setting Trend*, COMPUTERWORLD, Oct. 26, 1981, at 41, 44 (discussing the evolution of computer terminals).

[47] EMERSON W. PUGH, BUILDING IBM: SHAPING AND INDUSTRY AND ITS TECHNOLOGY 317 (Mass. Inst. of Tech. 1995).

computer kit designed for hobbyists.[48] The personal computing industry experienced fast growth through the 1980s, particularly after the development of the IBM personal computer and the founding of Apple Computer and Microsoft.[49] As personal computer sales grew, new competitors rushed into the emerging and lucrative market and a shift from a hardware-focused industry to a software-focused industry occurred.[50] By the late 1990s, it was clear that Microsoft's software-based business model held more potential for future growth than the traditional hardware-based model.

As long as there was a need for better and faster personal computers and more software programs, there was a recurring market for new and improved computers, terminals, operating systems, and software. The need for faster and more dependable personal computers received a boost in the early 1990s due to three important developments: (1) the invention and ultimate implementation of the first web browser, the World Wide Web, as first detailed in a memorandum by Tim Berners Lee in March of 1989, titled "Information Management: A Proposal";[51] (2) the related development of Uniform Resource Locators (URLs), the Hypertext Transfer Protocol (HTP), and the Hypertext Markup Language (html);[52]

---

[48] ADAM OSBORNE & JOHN DVORAK, HYPERGROWTH: THE RISE AND FALL OF THE OSBORNE COMPUTER CORPORATION 6 (Idthekkethan Pub. Co. 1984).
[49] *See id.* at 10; PUGH, *supra* note 47, at 315.
[50] *See* ALLAN, *supra* note 39, at pt. 2; OSBORNE & DVORAK, *supra* note 48, at 11; Schmidt, *supra* note 15, at 351–53 (describing the "metamorphoses of a computer program").
[51] JAMES GILLIES & ROBERT CAILLIAU, HOW THE WEB WAS BORN: THE STORY OF THE WORLD WIDE WEB 180 (Oxford Univ. Press 2000).
[52] *Id.* at 206.

and (3) the decision by the Clinton Administration to open up the Internet to commercial use.[53]

Instead of simply using computers for word processing, accounting, or gaming purposes, individuals and businesses could use them for a variety of communication purposes. This not only resulted in greater demand for personal computers and software, but led to the dot-com boom and bust and the development of many of the Internet-based business models and delivery methods that we use today, such as Amazon, Google, Facebook and eBay. With the resulting increase in the use of computers by individuals and small businesses, sales of personal computers and related software naturally increased. Today, the heady days when consumers and businesses bought new personal computers and software every two or three years has disappeared to be replaced by the sale of the next generation of computing devices, such a smart phones, e-readers, and tablet computers.

B. The Emergence of Cloud Computing

In many respects, cloud computing is a natural progression for the computer, Internet, and telecommunications

---

53 Id. at 265. This was the brain-child of Vice President Al Gore and why he deserves some credit for enabling the commercial use of the Internet. Although he did not invent the technical aspects of the Internet, he did have the vision to see how a technology that was developed for use by the military and universities might be of use to business and the general public and advocated for the commercial use of the "information super-highway." See SUSAN R. HARRIS & ELISE GERICH, RETIRING THE NSFNET BACKBONE SERVICE: CHRONICLING THE END OF AN ERA, http://merit.edu/research/nsfnet_article.php (last visited Oct. 20, 2014) (detailing the shift from the NSFNET to the commercial Internet today).

industries. It takes three things that those industries have in common—server capacity, technical abilities, and customer service capabilities —and attempts to package them into saleable business and personal services that are not dependent upon the sale of hardware or software.[54] IBM described the circumstances leading to cloud computing and the development of its "smarter cloud" initiative this way:

> Despite enormous advances in computing power, the world's IT infrastructure—already under severe stress from today's computing tasks—could easily become overwhelmed by the onrushing complexity and unprecedented data generated by nearly a trillion instrumented and interconnected devices, objects, processes and people.
>
> Fortunately, help is at hand. It comes in the form of a new model called "cloud computing," in which processing, storage, networking, and applications are accessed as services over networks—public, via the Internet; or private, via intranets. It makes possible a new level of system intelligence—also known as "services management"—with the potential to secure, authenticate, customise and just plain keep up with the coming wave of data complexity and volume.[55]

As the foregoing suggests, cloud computing services can take many forms. [56]

---

[54] It also provides them with the opportunity to collect information and control its dissemination but that is a subject for another article.

[55] *Smarter Clouds on the Horizon*, IBM, https://www.ibm.com/smarterplanet/global/files/au__en_uk__cloud__visions_pdf.pdf (last visited Oct. 20, 2014).

[56] According to the World Privacy Forum, "cloud computing services exist in many variations, including data storage sites, video sites, tax preparation

Some of the services being offered in the cloud are undoubtedly new, but others are simply re-packaged. As previously noted, the service of storing and processing data on computers (or at least on computer-readable media) has been in existence for well over fifty years.[57] Another example of an old service being re-labeled for the cloud concerns the distribution, maintenance, and improvement of software over the Internet, also known as Software-as-a-Service (SaaS).[58] Instead of customers having to invest in an expensive suite of software, they can essentially rent the use of needed software, thereby sharing the costs with other companies with similar needs.[59] An added benefit of SaaS is that it is flexible and comes with technical support. According to the NIST, other cloud-based service models include Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), both of which involve a range of services previously provided before cloud computing.[60]

What is new about cloud computing is: (1) it is explicitly based upon network connectivity; (2) the potential

---

sites, personal health record websites, photography websites, [and] social networking sites." *WPF Resource Page: Cloud Computing and Privacy*, WORLD PRIVACY FORUM, http://www.worldprivacyforum.org/2011/11/resource-page-cloud-privacy (last visited Oct. 20, 2014).

[57] *See supra* text accompanying note 39.

[58] *See* MELL & GRANCE, *supra* note 2, at 2 (defining Software-as-a-Service).

[59] This is similar to the old-school use of mainframe computers where "dumb terminals" were used to access remote mainframe computers that had the desired processing capabilities, including computer programming (aka software) that was not transferred to the end user. *See Dumb Terminal*, *supra* note 45.

[60] *See* MELL & GRANCE, *supra* note 2, at 2–3 (defining Platform-as-a-Service and Infrastructure-as-a-Service).

scale and breath of its use, including the ability of users to access the cloud with devices that have limited data storage capabilities (such as smart phones and tablet computers); (3) the fact that it is touted as an "online" alternative for storing masses of business documents and personal information; and (4) the number and diversity of companies that have lined up to provide such services. In addition to traditional computer companies like Microsoft, IBM, and Dell, Internet and telecommunications companies such as Amazon, Google, Facebook, and Verizon are all involved in the cloud computing market. Some cloud computing services, like Google Docs and Dropbox, are primarily geared toward individuals and small businesses or are focused on providing functionality (remote document retrieval and editing) as much as storage. Other companies focus on more discrete services like web-hosting or software-as-a-service.[61] Some companies, like Amazon and IBM, offer a wide-variety of cloud-based services.

In one form or another, cloud computing services store bits of information on behalf of their customers.[62] Indeed, it is the promise of decreased hardware needs (in the form of server capacity) that is at the heart of much of the cloud computing hype. [63] Normally, a company needs to purchase hardware resources to create one or more tangible in-house or off-site

---

[61] DreamHost is an example of a webhosting service while Salesforce is an example of a software-as-a-service provider.

[62] *See* Eric Griffith, *What is Cloud Computing?*, PC MAG., (Mar. 13, 2013), *available at* http://www.pcmag.com/article2/0,2817,2372163,00.asp.

[63] *See, e.g., In-House vs. Cloud Servers*, XYFON SOLUTIONS, http://xyfon.com/house-servers-vs-cloud-servers (comparing in-house and cloud servers and noting that "[m]ost small to mid-sized companies have traditionally invested in on-site servers to host their applications, email, and file sharing") (last visited Oct. 20, 2014).

server farms.[64] In so doing, it must not only predict how much server capacity is needed on average but must also account for potential spikes in demand for server capacity. With cloud computing, companies can, in essence, rent hardware and software resources from others and create a virtual server that can be scaled up or down as needed.[65] Except when using a "private cloud" that is owned and operated exclusively by the consumer, the computer equipment utilized (and thus, the information stored) does not reside in-house but can consist of multiple servers located in various locations (possibly throughout the world).[66]

The actual and potential scale of cloud computing is important because it also marks another expansion (or shift) in the nature and wording of contracts that are used for back-office computer and Internet support services. In the early days of the computer industry, when the sale of mainframe computers, specialized programming, and related services were the focus of the industry, individually negotiated contracts were the norm.[67] As the personal computer, software, and the Internet markets developed, however, individually negotiated contracts were replaced by mass-distributed form contracts.[68]

---

[64] *See id.* (explaining that "[w]ith [an in-house server], you'll also need to refresh your hardware, renew software licenses, perform upgrades, and extend warranties every five to seven years").

[65] *See id.* ("Beyond this, [a cloud server] also provides an easily scalable solution that can accommodate changing business needs.").

[66] *See* MELL & GRANCE, *supra* note 2, at 3 (defining the four types of "clouds").

[67] *See* BRADSHAW ET AL., *supra* note 10, at 3 ("Traditional IT outsourcing arrangements typically involve negotiated contracts for narrowly specified data storage and processing facilities and services for a set period of time.").

[68] *See* Miles R. Gilburne & Ronald L. Johnston, *Trade Secret Protection for Software Generally and in the Mass Market*, 3 COMPUTER L.J., 211, 228

Given the sheer magnitude of the business being conducted over the Internet, it was no longer feasible to individually negotiate all license agreements and form click-wrap and browse-wrap agreements were used instead.[69] To a lesser extent, a similar shift has occurred in the cloud where there is now a mix of take-it-or-leave it terms of service agreements and form agreements with some negotiation or specialization allowed.[70] Generally, however, (as with Internet service providers (ISPs) before them) although cloud storage services are willing to make a lot of promises about the services they will provide, at least with respect to the public cloud and low cost or zero cost services (the so-called "freemium" model), they are not willing to accept the liability that might flow from the terabytes of information they agree to handle.[71]

C. Features of Cloud Storage Terms of Service Agreements

As the cloud computing industry has evolved and new products and services are offered, the contracts that are used in connection with such services have also evolved. When cloud computing began to come into vogue in 2009, many of the

---

(1981) (describing the use of shrink-wrap licenses to protect trade secrets embedded in mass distributed software).

[69] *See* Gilburne & Johnston, *supra* note 68, at 227 (outlining the history of the shift to mass-marketed software); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459 (2006) (describing shrink-wrap, browse-wrap, and click-wrap agreements, and the legal issues surrounding them); *see also* Christina L. Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAWYER 279 (2003); Sharon K. Sandeen, *The Sense and Nonsense of Web Site Terms of Use Agreements*, 26 HAMLINE L. REV. 499 (2003).

[70] *See* BRADSHAW ET AL., *supra* note 10, at 15.

[71] *See* discussion *infra* Part II.C.

services were offered with take-it-or leave it terms of service agreements similar to those posted by ISPs.[72] A review of such contracts in late 2009 revealed that cloud computing services appeared to be re-purposing form agreements that were developed in the early days of the Internet when the major concerns of ISPs were avoidance of liability for service interruptions and materials posted by others and the ownership of shared and posted content.[73] Then, as now, some of these contracts suffered from legal schizophrenia caused by attempts to address different legal risks in multiple and seemingly inconsistent agreements and policies. For instance, while a cloud service provider might disclaim responsibility for security in its Terms of Service Agreement, it may promise a particular level of privacy in its Privacy Policy.[74]

---

[72] *See* BRADSHAW ET AL., *supra* note 10, at 15; Sandeen, *supra* note 69, at 503.

[73] This observation is based upon the author's personal examination of various Terms of Service Agreements as referenced in her 2003 article, *The Sense and Nonsense of Web Site Terms of Use Agreements*, and her more recent review of cloud computing agreements, including Amazon Terms of Service Agreement, Terramark Terms of Service Agreement, OpSource Terms of Service Agreement, Rackspace Terms of Service Agreement, and Google Terms of Service Agreement. *See* Sandeen, *supra* note 69, at 499.

[74] *Compare Amazon Web Services (AWS) Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement (last visited Oct. 20, 2014), *with AWS Privacy Policy*, AMAZON WEB SERVICES, http://aws.amazon.com/privacy (last visited Oct. 20, 2014); *compare DropBox Terms of Service*, DROPBOX (Feb. 20, 2014), https://www.dropbox.com/terms, *with DropBox Privacy Policy*, DROPBOX (Feb. 20, 2014), https://www.dropbox.com/terms#privacy; *compare Google Terms of Service*, *supra* note 8, *with Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy (last updated Mar. 31, 2014) [hereinafter *Google Privacy Policy*].

As of early 2015, the nature and scope of cloud service contracts have become more varied, but they are often based upon form contracts and online Terms of Service Agreements.[75] Undoubtedly realizing the need to provide some measure of security for stored data, particularly for businesses that are under a legal obligation to comply with various information security laws, there is a noticeable increase in the willingness of cloud service providers to promise some level of security with respect to some of the services they provide.[76] For instance, many companies now allow their clients to limit

---

[75] *See* W. Kuan Hon et al., *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*, 16 STAN. TECH. L. REV. 79, 83–84 (2012) ("The starting point for cloud contracts is usually the providers' standard terms and conditions. . . . However, as many providers' standard terms are not suitable to accommodate enterprise users' requirements, cloud users have sought changes to make the terms more balanced and appropriate to their own circumstances. It appears that there has been some movement in this direction, particularly for large users. Nevertheless, our research indicates that some providers' negotiations are very process-driven, particularly at the lower price end of the market, where providers seemed unable or unwilling to accommodate differences such as corporate structures entailing (for users) separate localized contracts for non–United States affiliates.").

[76] *Id. Compare Dropbox Terms of Service*, DROPBOX, http://web.archive.org/web/20120504122034/https://www.dropbox.com/terms (last updated Mar. 26, 2012), *with Dropbox Terms of Service*, *supra* note 74. The previous reference to "Account Security" that placed all the burden of security on its customers is eliminated and in its associated Privacy Policy, Dropbox states: "Stewardship of your data is critical to us and a responsibility that we embrace. We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive." *Dropbox Privacy Policy*, *supra* note 74. However, the Dropbox Terms of Service Agreement continues to include a broad disclaimer of liability for "loss of data." *See Dropbox Terms of Service*, *supra* note 74.

the geographic regions in which their data will be stored.[77] The level of security promised, however, usually depends upon the needs of the customer and how much they are willing to pay. Thus, while sophisticated companies with significant resources may now be able to exact express promises of security from some cloud service providers, the lower cost (or free) cloud storage services used by individuals and small businesses often disclaim or limit their responsibility for security, thereby placing the burden for security on their customers.[78] Moreover, for trade secret purposes, the promises of security do not usually include a promise that stored documents will be kept confidential.

The Customer Agreement for Amazon Web Services (AWS) illustrates both the evolution and limitations of the form terms of service agreements used by some cloud storage services and the potential risks that they pose to trade secrets stored in the cloud. In late 2009, Section 7.2 (labeled "Security") of the AWS Customer Agreement read:

> We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly . . . you acknowledge that you bear sole responsibility for adequate security, protection and backup of your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from

---

[77] W. Kuan Hon et al., *supra* note 75, at 100 ("Some services allow users to choose locations of data centers used to process users' data, e.g., European Union–only, while providers are increasingly offering, albeit with exceptions, to restrict data to users' chosen locations as standard." (footnotes omitted)).

[78] *Id.* at 92 ("According to our research, providers state [disclaimers of] liability [are] non-negotiable, and 'everyone else accepts it.'").

unauthorized access (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.[79]

As of late 2013, in the AWS Customer Agreement last updated on March 15, 2012, the relevant provision read:

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and back-up of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. . . . [80]

In other words, although Amazon Web Services would provide its customers with some security tools, the implementation of those tools is up to the customer. This limitation is emphasized in Section 3.1 of the March 15, 2012 AWS Customer Agreement which, while seemingly promising security and privacy, actually places the burden of security squarely on the customer. It reads: "Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures *designed to help you*

---

[79] *AWS Customer Agreement*, AMAZON WEB SERVICES, *available at* http://web.archive.org/web/20090831034111/http://aws.amazon.com/agreement (last updated Aug. 26, 2009) [hereinafter *Aug. 26, 2009 AWS Customer Agreement*].

[80] *AWS Customer Agreement*, *supra* note 74.

secure Your Content against accidental or unlawful loss, access or disclosure."[81]

Provisions, such as the foregoing,[82] that expressly state that cloud storage providers are not assuming responsibility for the security of stored data are undoubtedly designed to prevent a finding of any implied security obligation. To be doubly certain that no liability will arise for security breaches, other provisions of both the circa 2009 and the March 15, 2012 AWS Customer Agreement contain additional limitations. For instance, in 2009, Section 11.2 of the AWS Customer Agreement read: "You represent and warrant . . . that you are solely responsible for the . . . security . . . of Your Content." Similarly, Section 11.5, disclaimed all warranties that "THE DATA YOU STORE WITHIN THE SERVICE OFFERINGS WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED," and Section 11.8 stated that Amazon shall not be liable for any damages resulting from "UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR CONTENT."[83] In the current agreement, Section 10 states, in part, that AWS makes "NO REPRESENTATIONS OR WARRANTIES . . . THAT . . . YOUR CONTENT OR THE THIRD-PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED."[84]

The terms of service agreement that Google uses (governing its Google Docs service, as well as other services such as Gmail) has also evolved over time and has been greatly

---

[81] *Id.* (emphasis added).
[82] *See supra* text accompanying note 81.
[83] *Aug. 26, 2009 AWS Customer Agreement*, *supra* note 79 (emphasis in original).
[84] *AWS Customer Agreement*, *supra* note 74.

simplified from previous agreements. What is interesting about its circa-2013 agreement in comparison with the agreements of other companies does not relate so much to the promises of security and confidentiality, or lack thereof, but to the broad uses that Google can make of stored information. In part, the agreement reads:

> When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones.[85]

Whether its customers understand this or not, the foregoing provision, among others, allows Google to use the information it collects from one of its services (say Gmail) for many other purposes. Critical to the current analysis is Google's asserted right "to use," "communicate," "publish," and "publicly perform" customer content, albeit for the "limited purpose" of using it with respect to any Google service now known or to be developed.[86] As is further

---

[85] *Google Terms of Service*, *supra* note 8.

[86] The reason that cloud storage services may want to obtain a right to "publicly perform" stored content is made clear by the U.S. Supreme Court's recent decision in American Broadcasting Co., Inc., v. Aereo, Inc., where the Court found that Aereo's system involved a public performance under the transmit clause. 134 S. Ct. 2498 (2014); *see also* 17 U.S.C. §101 (2012). Pursuant to this precedent, depending how a cloud storage service is designed, the storage of copyright protected information in the cloud, even

explained *infra*, this is not consistent with general notions of the confidential treatment of documents.[87]

While the broad and varied use of information stored in the various Google services is problematic enough, nowhere in the foregoing Google Terms of Service is the issue of data security addressed. Rather, like other agreements of its kind, the Google Agreement includes a disclaimer of responsibility for "lost data" and a disclaimer of implied warranties.[88] Significantly, Google does not promise that such use will be confidential or private. Indeed, (apparently since getting in trouble with the Federal Trade Commission for failing to abide by its own privacy policies)[89] Google now admits that it offers little or no privacy. In the "Information Security" portion of its Privacy Policy, Google states:

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

We encrypt many of our services using SSL.

---

at the behest of a consumer, may be considered an infringing "public performance." 17 U.S.C. §106(4).

[87] *See infra* text accompanying notes 153–57.

[88] *Google Terms of Service*, *supra* note 8.

[89] *See FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data*, FED. TRADE COMM'N (Mar. 30, 2011), http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *see also* Google, Inc., No. 102 3136 (F.T.C. 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf.

> We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.
>
> We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
>
> We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.[90]

In other words, while Google is willing to represent the level of security it provides for its system (which it reserves the right to change at any time), it is not willing to make the provision of security a binding commitment, promising only to "restrict access to personal information." Because of this, the absence of an express promise of confidentiality, and Google's broad rights to use stored data not amounting to personal information, the ability to protect stored information as trade secrets is compromised.

The desire of cloud storage services to avoid liability for the confidentiality and security of the information that they store is understandable given the sheer volume of information they handle. However, serious questions about the value of the business model being promoted are raised as a result. While, on one hand, the cloud is promoted as a cost-effective alternative to acquiring and maintaining internal server capacity, cloud

---

[90] *Google Privacy Policy*, *supra* note 74.

storage services still recommend that companies maintain back-up copies of the information and data that is stored in the cloud and that they institute necessary security precautions, including encryption. Moreover, for reasons that are explained *infra*,[91] these arrangements may undermine the trade secret status of information that is stored in the cloud due to application of the third party doctrine of trade secret law.

III. THE REASONABLE EFFORTS REQUIREMENT OF TRADE SECRET LAW

Trade secret law, like other areas of law, has evolved over a long period of time.[92] Today, the predominant source of trade secret law is the Uniform Trade Secrets Act (UTSA), which was first adopted in 1979 and has now been enacted in substantial part by forty-seven states and the District of Columbia.[93] According to the UTSA, in order to protect information as a trade secret, the information must meet three requirements:[94] (1) it must be secret, i.e., not generally known

---

[91] *See infra* Part III.

[92] *See generally* Sharon K. Sandeen, *The Evolution of Trade Secret and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 495 (2010).

[93] *See Trade Secret Act*, UNIF. L. COMM'N, *available at* http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act (listing jurisdictions that have adopted the UTSA) (last visited Oct. 23, 2014). It is often stated that North Carolina has not adopted the UTSA but has adopted a statute which is very similar and, thus, is often counted as a UTSA state. *See* N.C. Gen. Stat. §§ 66-152–57 (2013). The two states that have not yet adopted the UTSA are Massachusetts and New York.

[94] UTSA § 1(4) (1985); *see* Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 6–7 (2009) (explaining the reasonable efforts requirement under the RESTATEMENT (FIRST) OF TORTS and the RESTATEMENT (THIRD) OF UNFAIR COMPETITION).

or readily ascertainable;[95] (2) it must derive independent economic value from not being generally known or readily ascertainable;[96] and (3) it must be the subject of efforts that are reasonable under the circumstances to protect its secrecy.[97]

While early treatises on trade secret law were slow to use the term "reasonable efforts,"[98] from the very earliest trade secret cases, courts insisted on evidence that the plaintiff (and putative trade secret owner) engaged in efforts to protect the information claimed to have been misappropriated.[99] As a 1953 treatise on trade secret law explained, because the existence of a trade secret is "not passed on officially as is a patent or trade-mark registration," plaintiffs in trade secret cases have "the burden of proving that their alleged process is in fact a secret process."[100] In effect, the reasonable efforts requirement is a "formality" of trade secret law and evidence of the putative trade secret owner's expectation of secrecy.[101] One of the

---

[95] UTSA § 1(4)(i).
[96] *Id.*
[97] *Id.* § 1(4)(ii).
[98] *See* HARRY D. NIMS, THE LAW OF UNFAIR BUSINESS COMPETITION, (Baker, Voorhis & Co. 1909); RIDSDALE ELLIS, TRADE SECRETS (Baker, Voorhis & Co. 1953).
[99] *See, e.g.*, Hamilton Mfg. Co. v. Tubbs Mfg. Co., 216 F. 401, 404 (W.D. Mich. 1908) (refusing to grant an injunction to prevent the use of machines copied from plaintiff because "[t]here is no evidence that any secrecy was enjoined on any person employed in drafting designs, making patterns of construction, or assisting in the construction of any of the last-named seven machines").
[100] ELLIS, *supra* note 98, § 238 (quoting Fairchild Engine & Airplane Corp. v. Cox, 50 N.Y.S.2d 643 (N.Y. Special Term 1944)).
[101] The term "formalities" is borrowed from copyright law and generally refers to various requirements for obtaining and maintaining copyright protection, including registration and notice. *See generally* MILGRIM & BENSEN, *supra* note 21, § 1.06[6]. Although international copyright norms

principal elements identified as proof of plaintiff's ownership of protectable trade secrets was "that secrecy has been maintained either by non-disclosure or disclosure in confidence."[102] As further explained, "[t]he existence of a confidential disclosure may be proved by showing that precautions were taken against disclosure to more persons than necessary, the use of symbols in place of actual names of materials used, and so on."[103]

In 1939, when the American Law Institute published Volume IV of the Restatement (First) of Torts to restate the law governing unfair business practices, the reasonable efforts requirement was one of six factors identified as relevant to the determination whether a set of information should be treated as a trade secret.[104] As explained in comment b to §757 of the Restatement (First) of Torts, "a substantial element of secrecy must exist [in information sought to be protected as a trade secret], so that, except by the use of improper means, there would be difficulty in acquiring the information."[105]

In 1970, the National Conference of Commissioners of Uniform State Laws (NCCUSL, now known as the Uniform Law Commission) began drafting a uniform act to govern trade

---

have eliminated copyright formalities, the term is used herein with respect to trade secrets to highlight that trade secret protection is not automatic. *Id.* Trade secret owners are required to engage in reasonable efforts to maintain the secrecy of their information. *Id.*

[102] ELLIS, *supra* note 98, § 239.

[103] *Id.* § 248; *see also* Mycalex Corp. v. Pemco, 64 F. Supp. 420, 425 (D. Md. 1946) ("It is not sufficient in the law for one to say that this or that phase of research or experimentation, or this or that factor in production, is secret. It must in fact bear the indicia of secrecy . . . .").

[104] *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

[105] *Id.*

secrets, ultimately replacing the Restatement (First) of Tort's amorphous and flexible six-factor test with the three requirements set forth above.[106] Although the drafting history, wording, and structure of the UTSA make it clear that the reasonable efforts requirement is an essential requirement of the definition of a trade secret, there is a lingering misunderstanding about the importance of the reasonable efforts requirement and where it fits in the trade secret analysis. Some courts and commentators frame it as an issue separate and apart from the definition of a trade secret.[107] In two of the three states that have yet to adopt the UTSA (Massachusetts and New York), it continues to be a factor to be considered in determining whether information should be protected.[108] The Restatement (Third) of Unfair Competition places the reasonable efforts analysis under the misappropriation prong of a trade secret claim.[109] Wherever the issue is situated in the analysis of trade secrecy, the reasonable efforts requirement plays an important notice and due process function.

---

[106] *See* Sandeen, *supra* note 92, at 513.

[107] *See, e.g.*, Lemley et. al., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 49 (6th ed. 2012) ("Besides the existence of a trade secret, plaintiffs must show under the Uniform Act that they have taken 'reasonable measures' to protect the secrecy of their idea."); *see also* MILGRIM & BENSEN, *supra* note 21, at § 1.01 (treating reasonable efforts as an element of the "procedural" aspect of the trade secret definition, and contrasted with the "substantive" aspects).

[108] *See* Warner-Lambert Co. v. Execuquest Corp., 427 Mass. 46, 49 (1998) (quoting Jet Spray Cooler, Inc. v. Crampton, 361 Mass. 835, 840 (1972)); Ashland Mgmt. Inc. v. Janien, 82 N.Y.2d 395, 407 (N.Y. 1993) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)).

[109] *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40(b)(4) (1995).

A. The Notice Function of the Reasonable Efforts Requirement

Historically, the reasonable efforts requirement was recognized as serving a number of different functions depending on the circumstances and equities of a particular case. As noted above, some courts stated that it provides proof of ownership or legitimacy and, in effect, substituted for government registration.[110] Other courts noted that it provides evidence that the subject information had sufficient value to be worthy of court intervention.[111] With respect to dealings with third parties (including employees), some courts identified the notice function that the reasonable effort requirement serves in both pinpointing the claimed trade secrets and providing a potential basis for finding a duty of confidentiality.[112]

The first two of the historical functions of the reasonable efforts requirement (proof of ownership and value) are now reflected in the secrecy and economic value requirements of the UTSA. When a putative trade secret owner succeeds in proving that its information is secret and has independent economic value due to its secrecy, it establishes that it owns the information and that it is worthy of court intervention. Based upon this, the modern and now primary function of the reasonable efforts requirement is to put others

---

[110] *See supra* text accompanying note 100.
[111] *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991).
[112] *See, e.g.*, Aries Info. Sys., Inc. v. Pac. Mgmt. Sys. Corp., 366 N.W.2d 366, 367 (Minn. Ct. App. 1985) (stating that reasonable efforts of plaintiff technology company including contract terms and proprietary notice clearly establish that defendant employees were aware of trade secret status of contested software development).

on notice of the claimed existence of trade secrets.[113] By stating the reasonable efforts requirement of the UTSA separate and apart from the secrecy and independent economic value requirements, the UTSA is not merely concerned with whether the acts of a putative trade secret owner result in information becoming generally known or readily ascertainable; it is also concerned with whether another party should be subject to liability when the putative trade secret owner fails to act reasonably to protect its own secrets.

The notice function of the reasonable efforts requirement is particularly important in third party situations given that, unlike other intellectual property doctrines, trade secret misappropriation requires proof of knowledge (or reason to know) of both the existence and misappropriation of trade secrets.[114] According to the UTSA, there are three acts that can constitute misappropriation: the wrongful acquisition, disclosure, or use of trade secrets.[115] When a trade secret owner voluntarily transfers its trade secrets to another, a claim for wrongful acquisition is impossible because the information was voluntarily provided to the other. Thus, unless a contractual restriction exists to limit how the information can be accessed, the only way to prove trade secret misappropriation in most cases involving the voluntary sharing of information is to establish wrongful disclosure or use in violation of an express or implied duty of confidentiality. To establish such a claim, it is axiomatic that a third party must know or have reason to know that it possesses trade secrets that need to be protected.

---

[113] *See* Sandeen, *supra* note 92, at 526.
[114] UTSA § 1(2) (1985) (definition of "misappropriation").
[115] *Id.*

While the reasonable efforts requirement serves a notice function, providing notice of the existence of trade secrets is not its only function. It also serves to limit the scope of protectable information and, in this way, operates as a policy lever that prevents the under-protection of trade secret assets and over-assertion of trade secret rights.[116] As noted by Professors Robert Merges and John Duffy in their article about the history and background of *Graham v. John Deere*, the extent to which limitations on IP rights are needed depends in large part on the scope of exclusive rights that are granted.[117] The greater the exclusive rights, the harder it should be to acquire rights in the first place. This explains the stringent novelty and non-obviousness requirements of patent law and the relatively lax requirements of copyright law. Because patent protection precludes even independent invention, and therefore provides very strong rights, it makes sense to require a high hurdle of inventiveness. In contrast, because copyright law does not preclude independent creation and recognizes other "fair uses" of copyrightable material, the requirements for protection are fairly low. Trade secrets are more like copyrights in that they do not preclude independent creation or reverse engineering. Moreover, in order to avoid a conflict between federal patent law and state trade secret law, the U.S. Supreme Court has recognized the importance of both the requirements and limitations of trade secret law.[118]

---

[116] *See* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 42–47 (2007).

[117] John F. Duffy & Robert P. Merges, *The Story of* Graham v. John Deere Company*: Patent Law's Evolving Standard of Creativity*, *in* INTELLECTUAL PROPERTY STORIES, 109, 111–114 (Jane C. Ginsburg & Rochelle Cooper Dreyfuss eds., 2005).

[118] *See generally* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974). *See also* Gordon L. Doerfer, *The Limits of Trade Secret Law Imposed by*

B. What Constitutes Reasonable Efforts?

While the public policy of the United States and the UTSA make it clear that the reasonable efforts requirement is an essential part of the definition of a trade secret, what constitutes reasonable efforts in any given situation is not always clear.[119] Moreover, there are both legal and practical dimensions to the requirement. Legally, in most jurisdictions, information will not qualify for trade secret protection unless some efforts to maintain secrecy are proven.[120] However, as a practical matter, greater security measures are often needed to prevent the loss of trade secrecy.

If one views the reasonable efforts requirement as a continuum, with one end of the continuum being no efforts and the other end being extreme efforts, what is required to satisfy the requirement falls somewhere between the two ends. But neither the UTSA nor case law signals whether the line should be drawn closer to the no efforts or extreme measures side of the continuum; they only say that the line should be determined

---

Federal Patent and Antitrust Supremacy, 80 HARV. L. REV. 1432, 1462 (1967) (noting that "inevitable leaks, accidental disclosures, and efficient reverse engineering limit the effectiveness of any program of secrecy" and therefore limit potential conflicts between patent and trade secret law).

[119] *See* Rowe, *supra* note 94, at 8–9 (noting that the various sources of law on the reasonable efforts requirement do not provide guiding standards for determining what is reasonable); *see also* Andrew Beckerman-Rodau, *Trade Secrets–The New Risks to Trade Secrets Posed by Computerization*, 28 RUTGERS COMPUTER & TECH. L.J. 227, 239–41 (2002) (listing relevant factors).

[120] *See, e.g.*, *In re* Dippin' Dots Patent Litig., 249 F. Supp. 2d 1346, 1377 (2003) ("Because simple measures, such as identifying materials as trade secrets and using a written confidentiality agreement, are available to protect sensitive information, the Uniform Act will not imply a confidential relationship between the parties."); *see also* Rowe, *supra* note 94, at 1–2.

"based upon the circumstances."[121] Since compliance with the reasonable efforts requirement is an issue of fact, where the line is drawn depends upon where the trier of fact thinks it should be drawn.[122] In this way, the reasonable efforts requirement is the most flexible of the three requirements of trade secrecy and the factor most apt to be influenced by equitable considerations.[123]

The flexible and subjective nature of the reasonable efforts requirement is likely to be a great comfort to information owners who do little to protect their information, because it provides some hope of bringing a successful trade secret claim despite deficiencies in protection efforts.[124] Case law is replete with examples (particularly before the widespread adoption of the UTSA) of information owners who used the seeming unfairness of the acquisition or use of their information to override deficiencies in their ability to prove the existence of trade secrets.[125] However, the flexibility of the

---

[121] UTSA § 1(2) (1985) (definition of "trade secret).

[122] *See* SmithKline Beecham Pharms. Co. v. Merck & Co., Inc., 766 A.2d 442, 448 (Del. 2000) (noting that whether Merck took reasonable precautions to protect its trade secrets is a question of fact).

[123] Rowe, *supra* note 28, at 30 ("In particular, the most critical part of that inquiry should be whether the trade secret owner took reasonable steps to preserve the secrecy of the information.").

[124] *See* P.J. Whelan, *Trade Secrets—Problems of Acquisition*, 18 BUS. LAW. 539, 543 (commenting on the uncertain application of trade secret law before enactment of the UTSA: "[I]t would be unwise to brush aside the claims of a discloser no matter how preposterous they might be, because, if he could get his case into the right jurisdiction, he could likely find precedent which would lend some merit to his position").

[125] *See* Doerfer, *supra* note 118, at 1432 ("[I]n attempting to eradicate what is considered to be unconscionable conduct, there is a serious danger that courts may elevate principles of gentlemanly conduct to the status of legal

reasonable efforts requirement makes it difficult for business people who wish to protect their trade secrets to know what efforts they should engage in to ensure a finding of trade secrecy. A company that is careful to engage in efforts that it thinks are reasonable to protect its secrets may find that such efforts are considered insufficient in a court of law.[126]

As a practical matter, the smart business will always do something to identify and protect its trade secrets so that it can later argue that its protection efforts were reasonable. However, since trade secrets are lost once they become "generally known or readily ascertainable,"[127] it is important for businesses that own extremely valuable trade secrets to also engage in more intensive efforts. Businesses that utilize computers and the Internet have to be particularly concerned about the ease with which information can now be reproduced and shared.[128]

Without recognized standards to guide the way, currently, the best way to predict what efforts are needed to meet the reasonable efforts requirement is to identify the factors that previous courts have considered and to act in a manner that is designed to ensure actual secrecy. It has also been suggested that the nature and size of the putative trade

---

norms without considering the countervailing interests in rigorous competition . . . .").

[126] *See* Rowe, *supra* note 94, at 1–2 (noting the second-guessing nature of the reasonable efforts requirement).

[127] *See* UTSA § 1(2) (1985) (definition of "trade secret").

[128] *See* Rowe, *supra* note 94, at 14–26 (describing the threats to trade secrets posed by "the digital world"); *see also* Anita Ramasastry et al., *Will Wi-Fi Make Your Private Network Public? Wardriving, Criminal and Civil Liability, and Security Risks of Wireless Networks*, 1 SHIDLER J.L. COM. & TECH. 9 (2005).

secret owner's business should be part of the reasonableness analysis.[129]

IV. THE THIRD PARTY DOCTRINE OF TRADE SECRET LAW: REASONABLE EFFORTS AS APPLIED TO INFORMATION FLOWS TO THIRD PARTIES

While there is some debate among courts whether a putative trade secret owner can do little or nothing intra-enterprise and still establish the existence of trade secrets for purposes of a misappropriation claim,[130] there is no debate that the decision of a putative trade secret owner to share information outside the confines of its own business requires it to tread carefully.[131] Generally, when a trade secret owner

---

[129] *See* Rowe, *supra* note 94, at 29–30; *see also* Jermaine S. Grubbs, Comment, *Give the Little Guys Equal Opportunity at Trade Secret Protection: Why the "Reasonable Efforts" Taken by Small Businesses Should be Analyzed Less Stringently*, 9 LEWIS & CLARK L. REV. 421, 426 (2005).

[130] *Compare* Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 892, 903–04 (Minn. 1983), *with* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991) (reasonable efforts treated as part of the analysis but as a minor factor in cases where evidence of misappropriation by improper means exists). The differing approaches may be explained by a lack of appreciation for the fact that the UTSA was intended to ensure that courts would not find misappropriation without first finding the existence of a trade secret. The differing approaches may be explained by a lack of appreciation for the fact that the UTSA was intended to ensure that courts would not find misappropriation without first finding the existence of a trade secret. *See* Sandeen, *supra* note 92, at 496 (detailing the drafting history of the UTSA).

[131] *See* MILGRIM & BENSEN, *supra* note 21, § 3.03 ("[T]here can be no protection of a trade secret if disclosure of it is made in the absence of a confidential relationship, a contract or if disclosure is made in a way that does not meet explicit requirements of the parties' contract."); *see also* Silicon Image, Inc. v. Analogk Semiconductor, Inc., No. C-07-00635JCS,

voluntarily shares information with another, it risks waiving whatever trade secrecy may exist in such information even in situations where the information does not become generally known of readily ascertainable.[132] As summarized in an early article on trade secret law: "In by far the largest proportion of decided cases in which the courts have afforded protection to a trade secret or secrets the defendant is the one to whom the successful plaintiff had directly imparted the secret which is the subject of litigation."[133] This occurs, for instance: (1) when trade secret information is disclosed to employees; (2) when the owner of the trade secret is seeking to sell an idea or unpatented invention; and (3) when the owner of the trade secret discloses it for "other special purposes. However, pursuant to the doctrine of relative secrecy, trade secret owners can share their secrets with third parties without losing trade secret protection if the disclosures are limited and the persons

---

2008 WL 166950, at *17 (N.D. Cal. Jan. 17, 2008) ("[C]ourts have denied trade secret protection where allegedly confidential information has been revealed to third-parties without protections that are considered adequate.").

[132] *See* Flotec, Inc. v. Southern Res., 16 F. Supp. 2d 992, 1005–07 (S.D. Ind. 1998) ("Even if any of the information that Flotec disclosed to SRI qualified as a trade secret, the weight of the evidence presented here shows that Flotec's disclosure of that information to SRI was outside the scope of any confidential relationship, so that Flotec's disclosure destroyed the secrecy of all the information."); *see also* Taylor v. Babbitt, 760 F. Supp. 2d 80, 86 (D.D.C. 2011). As explained by James Pooley: "[T]he examination of secrecy as an element of the definition involves a dual path. One must of course be concerned with the extent to which the secret is known, or could be known with but a modicum of effort. . . . But one must also address the question of what the owner has done by way of self-help efforts to keep the secret held within its intended bounds." James Pooley, TRADE SECRETS § 4.04 (L.J. Press 2007).

[133] Mathias F. Correa, *Protection of Trade Secrets*, 18 BUS. LAW. 531, 532 (1963).

to whom such disclosures are made are under an express or implied duty of confidentiality.[134]

As explained by the court in *Humphers v. First Interstate Bank of Oregon*, a breach of confidentiality case: "The contours of [an] asserted duty of confidentiality are determined by a legal source external to the tort claim itself. A plaintiff asserting a breach of a nonconsensual duty must identify its source and terms."[135] As applied to trade secret cases, this means that a duty of confidentiality does not arise from the mere fact that the defendant possesses trade secrets but must be found in some other source of law. As the case law has developed, the circumstances that give rise to the requisite duty of confidentiality often fall into one of four categories: (1) an express agreement; (2) an agreement implied-in-fact; (3) an agreement implied-at-law (a "quasi-contract"); and (4) duties imposed by law either as specified in a statute (e.g., the attorney-client privilege) or based upon common law principles applicable to trust and fiduciary relationships.[136]

Because most trade secret disputes arise in the context of an employment relationship, courts are often quick to find that employees owe an implied duty of loyalty or

---

[134] *See* Rockwell Graphics Sys., Inc. v. DEV Indus., Inc., 925 F. 2d 174, 177 (7th Cir. 1991).
[135] Humphers v. First Interstate Bank of Or., 298 Or. 706, 718–19 (1985).
[136] *See* MILGRIM & BENSEN, *supra* note 21, § 7.01; RESTATEMENT (FIRST) OF TORTS § 757 cmt. on clause (b) (1939); Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763 (2014) (detailing the law of implied confidentiality and advocating for its application to better protect the privacy interests of Internet users); Herbert David Klein, *The Technical Trade Secret Quadrangle: A Survey*, 55 NW. U. L. REV. 437 (1960).

confidentiality to their employers.[137] Even in these cases, however, there is always an issue whether the defendant/former employee had adequate notice of the existence and identity of the claimed trade secrets.[138] The more difficult cases involve the voluntary disclosure of information to non-employee third parties. As the U.S. Supreme Court explained, "[i]f an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished."[139] The reason these cases are tough is because there is no settled definition of confidential relationships, and equitable considerations often play a big part in decisions that recognize an implied duty of confidentiality.[140]

Ideally, in all cases involving the disclosure of trade secrets to a third party, the trade secret owner will obtain an express confidentiality agreement from the third party before

---

[137] *See, e.g.*, L.M. Rabinowitz & Co. v. Dasher, 82 N.Y.S.2d 431, 435 (N.Y. Special Term 1948) ("It is implied in every contract of employment that the employee will hold sacred any trade secrets or other confidential information which he acquires in the course of employment.").

[138] *See, e.g.*, Furr's Inc. v. United Specialty Adver., Co., 385 S.W.2d. 456, 459 (Tex. Civ. App. 1964) ("Confidential relationship is a two way street: If the disclosure is made in confidence, the 'disclosee' should be aware of it. He must know that the secret is being revealed to him on the condition he is under a duty to so keep it."); *see also* RESTATEMENT (FIRST) OF TORTS § 757 cmt. m ("The actor is subject to liability under the rule stated in this Clause only if he has notice of both the fact that the information is secret and the fact that the disclosure by the third person is a breach of his duty.").

[139] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984).

[140] "Although the reported cases cover a multitude of situations where protected disclosure of trade secrets is recognized, these cases do not delineate the type of relationship under which such disclosures may occur." MILGRIM & BENSEN, *supra* note 21, § 7.01.

any disclosures occur.[141] In such cases, the source of the duty of confidentiality is a contract that can then be used as the basis for both a breach of contract claim and a trade secret misappropriation claim. In the absence of an express agreement, the trade secret owner may rely on contract principles to establish an implied-in-fact duty of confidentiality or argue that a statute or other independent body of law (such as the law of trusts)[142] imposes such a duty. Absent these sources of a duty of confidentiality, the trade secret owner's only recourse is to make the equitable argument that an implied-at-law duty of confidence exists by virtue of the nature of the relationship between the trade secret owner and the party to whom trade secrets are given and the circumstances surrounding the sharing of trade secret information.[143]This

---

[141] The language of the express confidentiality agreement must also specify required protections that are adequate in nature and duration. *See* Silicon Image, Inc. v. Analogk Semiconductor, Inc., No. C-07-00635JCS, 2008 WL 166950, at *17 (N.D. Cal. Jan. 17, 2008).

[142] "The concept of a confidential relationship is commonly employed in at least two branches of law: trusts and agency. Nonetheless, courts rendering trusts or agency opinions tend to characterize a relationship as being a 'fiduciary' one, or one of confidence without giving reasons for such conclusory positions." MILGRIM & BENSEN, *supra* note 21, § 3.03 (footnotes omitted).

[143] *See* Hartzog, *supra* note 136, at 763 (detailing the factors that are often considered in implied confidentiality cases). Before the adoption of the UTSA, courts (principally acting in equity) often founded successful trade secret claims upon a finding of a breach of confidence rather than an implied contractual duty of confidentiality. *See, e.g.*, Sun Dial Corp. v. Rideout, 108 A.2d 442 (N.J. 1954). With the adoption of Section 7 of the UTSA, which precludes all common law theories of recovery not based in contract or consistent with the requirements of the UTSA, arguably an action for breach of confidence is no longer viable. *See* John T. Cross, *UTSA Displacement of Other State Law Claims*, 33 HAMLINE L. REV. 445, 467–69 (2011).

requires a highly fact-specific inquiry that is by no means certain to result in a finding of the requisite duty.

In the absence of a clear definition of confidential relationships under the law, the best one can do in trade secret cases is to try to glean some general rules from previous cases and argue the equities of the situation in the hope that an obligation of confidentiality will be found "as a matter of law."[144] Often, a key feature of relationships that give rise to a duty of confidentiality in the trade secret context is that they involve the pursuit of a common business purpose where it is necessary for the trade secret owner to disclose all or a portion of its trade secrets in order to conduct its business.[145] For this reason, not every seemingly "close" relationship includes an implied duty of confidentiality.[146] Moreover, as noted in the Restatement (First) of Torts, "in all these cases A cannot impose a confidence on B without B's consent. . . . Likewise, the confidence does not arise if B has no notice of the confidential character of the disclosure."[147]

Based upon the foregoing, the mere disclosure (or transfer) of trade secrets to a third party does not create a confidential relationship; rather, the disclosure must at least be made under circumstances where the recipient of the information: (1) knows that it is receiving trade secret

---

[144] *See* Hartzog, *supra* note 136, at 763 (listing eleven relevant issues and practice tips for creating a confidential relationship).
[145] *See, e.g.*, Smith v. Dravo Corp., 203 F.2d 369, 373 (7th Cir. 1953).
[146] *Compare* Smith, *supra* note 145, *with* Smith v. Snap-On Tools Corp., 833 F.2d 578 (5th Cir. 1987), *and* Town & Country House & Homes Service, Inc. v. Evans, 150 Conn. 314 (1963) (short summaries of the cases omitted so that the reader knows what is to be drawn from each case)
[147] RESTATEMENT (FIRST) OF TORTS §757, cmt. on clause (b); *see also* MILGRIM & BENSEN, *supra* note 21, § 7.01.

information; and (2) understands and agrees to handle such information confidentially.[148]

When parties are dealing at arm's length, as they were when the drawing was sent to Coatings, the disclosure of the secret does not, by that fact alone, impose a confidential relationship. Where what is thought to be a trade secret is disclosed, the question posed is whether, under the circumstances, the recipient of the information knew or should have known that the information is a trade secret and that the disclosure was made in confidence.[149]

In the context of the cloud, as in other contexts, the necessary inquiry must be made on a case-by-case basis.

To date, no case decision has held that the relationship between a trade secret owner and a cloud storage service is in the nature of a trust or fiduciary relationship or that the relationship otherwise gives rise to a duty of confidentiality. This is consistent with the traditional definition of a fiduciary relationship[150] and with the law governing bailments, which

---

[148] The analysis is further complicated when information is shared with multiple third parties or if the person to whom trade secret information is disclosed is allowed to disclose the information to yet another person or entity.

[149] RTE Corp. v. Coatings, Inc. 267 N.W.2d 226, 232 (Wis. 1978); *see also* Mercer v. C.A. Roberts Co., 570 F.2d 1232, 1237 (5th Cir. 1978).

[150] The application of fiduciary duty principles is often unclear and confused. *See* John F. Mariani et al., *Understanding Fiduciary Duty*, 84 MAR FLA. B.J. 20 (2010); *see also* Deborah A. DeMott, *Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences*, 48 ARIZ. L. REV. 925 (2006); D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399 (2002). But generally, a fiduciary relationship requires something more than a relationship of trust and confidence (which obviously exists in most

imposes only limited duties upon bailees and which has consistently recognized that the bailor/bailee relationship is not a confidential or fiduciary relationship.[151] It is also consistent with the desire of cloud storage services to avoid assuming such responsibilities, as described *supra*.[152]

While some cloud storage services may be willing to provide an express promise of confidentiality, they often disclaim any responsibility or liability for the security of stored information.[153] This not only undermines the creation of an express promise of security, but also hampers the ability of the trade secret owner to prove an implied-in-fact promise since a well-established rule of contract law provides that implied obligations cannot be inferred where express obligations of the same nature are disclaimed.[154]Further, unlike other relationships where an implied-at-law duty of confidentiality has been found, the disclosure or use of trade secrets is not necessary to further a business relationship between a cloud storage service and its customers. Thus, although it is conceivable that a cloud storage service might be held to an implied-at-law duty of confidentiality under a special set of facts (even when it has expressly disclaimed liability for stored

---

contractual situations); it also requires that the alleged fiduciary act on behalf of another under circumstances that create a potential for abuse. Black's Law Dictionary defines a fiduciary as: "A person who is required to act for the benefit of another person on all matters within the scope of their relationship . . . ." BLACK'S LAW DICTIONARY 702 (Deluxe 9th ed. 2009).

[151] 8A AM. JUR. 2D *Bailments* § 1 (2014).

[152] *See supra* text accompanying notes 78–90.

[153] *Id.*

[154] 17A AM. JUR. 2D *Contracts* § 17 (2014) ("As a general rule, if an express contract between the parties is established, a contract embracing the same subject cannot be implied; an implied agreement cannot coexist with the express contract.").

data),[155] the chances are high that no such duty will be found. This is particularly so since the information that is being stored in the cloud is not likely to be stored in a manner that gives the cloud storage service notice of the existence of trade secrets.[156]

Without the existence of either an express or implied confidential relationship with its cloud storage service, a company that pursues trade secret misappropriation claims for information that is (or has been) stored in the cloud is likely to confront defense arguments that such information is no longer (or never has been) entitled to trade secret protection due to the fact that it was stored in the cloud. In this regard, the defendant will argue that it was not reasonable to store information in the cloud without first securing an express promise of confidentiality. In response, the trade secret owner may produce evidence of the efforts it engaged in to protect its trade secrets intra-enterprise, but such efforts are likely to be insufficient if the same information was shared with one or

---

[155] *See, e.g.*, Burten v. Milton Bradley Co., 763 F.2d 461 (1st Cir. 1985) (involving a rare case where an implied-at-law duty of confidentiality was found despite the information recipient's efforts to disclaim any relationship between the parties).

[156] Unless a company that is using the cloud has instituted procedures to identify and mark documents as "confidential" or "secret," it is unlikely that even persons under a duty of confidentiality (including those with official access to a company's piece of the cloud) would know of the existence of trade secrets. This is particularly true with respect to information that is being created and modified in the cloud, as opposed to pre-existing information that is simply being stored in the cloud. Since cloud storage services such as Google and Dropbox are touting the cloud as a place for collaboration, it is possible that new ideas will be generated in the cloud that amount to valuable trade secrets, but no one is charged with differentiating such information from the multitude of other, perhaps mundane, information that a company may store in the cloud on a day-to-day basis.

more third parties who were not under a duty of confidentiality. This is because no amount of intra-enterprise reasonable efforts is sufficient to prevent the loss of trade secrecy that results from a voluntary, non-confidential disclosure of trade secrets to third parties and it will be difficult to establish that extra-contractual duties of confidentiality exists. [157]

Some courts may be troubled by the foregoing analysis and may seek to liberalize traditional notions of confidential relationships in order to avoid the forfeiture of trade secret rights for information stored in the cloud.[158] Or they may interpret the Stored Communications Act or similar laws to

---

[157] As noted previously, certain information holders (such as attorneys) may be under a legal duty of confidentiality with respect to some information that they hold whether or not a contractual duty of confidentiality exists. *See supra* text accompanying notes 141–49. Whether cloud storage services are under a legal duty of confidentiality, particularly where they expressly disclaim such duty in their Terms of Service Agreements, depends upon application of the Stored Communications Act and similar state laws. For reasons that are explained more fully *infra*, it is doubtful that the Stored Communications Act imposes a legal duty on cloud storage services due to the interactive nature of such services. *See infra* text accompanying notes 261–269; *see also* William Jeremy Robinson, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1195–96 (2010).

[158] The early days of the Internet were marked by such efforts in the form of arguments that were designed either to "save" the Internet from the application of well-established legal principles that were perceived to threaten the development and use of new technologies and methods of doing business, *see, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (applying an expansive definition of mutual assent to shrink-wrap licenses), or to expand well-established legal principles to cover new perceived wrongs. *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (refusing to extend the tort of trespass to chattels to cover "otherwise harmless electronic communications," even though some other courts had done so).

impose a legal duty of confidentiality despite disclaimers to the contrary.[159] While these approaches might solve the problem of trade secrets stored in the cloud, however, an expansion of the definition of confidential relationships to cover relationships in the cloud could have deleterious effects with respect to other information flows, such as the law governing the unsolicited submission of ideas by so-called "idea-men." In other words, making it easier for information owners to establish confidential relationships to protect information stored in the cloud might make it easier for the holders of ideas to assert similar confidential relationships and successfully assert idea submission claims, something that the business community would generally abhor. Rather than making it easier for duties of confidentiality to be formed in the cloud, more attention should be paid to the proper definition of "disclosure" under trade secret law and a better taxonomy should be developed to differentiate between trade secret destroying "disclosures" and non-trade secret destroying "mere transfers."

V. POSSIBLE REFINEMENTS AND EXCEPTIONS TO THE THIRD PARTY DOCTRINE OF TRADE SECRET LAW

Given the potential harsh effects of the third party doctrine of trade secret law with respect to trade secrets stored in the cloud, the practical techniques and legal arguments that might be used to ameliorate or eliminate those effects are considered next, followed by a specific proposal for distinguishing between "disclosures" and "mere transfers."

[159] *See, e.g.*, *ProCD*, 86 F.3d at 1447; *Intel*, 71 P.3d at 296.

A. Segregate Trade Secret Information or Obtain an Express Agreement of Confidentiality

One simple and direct approach to avoid the harsh effects of the third party doctrine of trade secret law is for companies to ensure that any trade secret information is excluded from the body of information that is stored in the cloud. Or they can make the effort and take the time to obtain an express confidentiality agreement from their cloud storage services, if possible. The first strategy is the best course of action because, if followed, the trade secret owner would only have to worry about its own reasonable intra-enterprise efforts to maintain secrecy. With the second strategy, the trade secret owner needs to ensure that reasonable efforts are employed at both its own facilities and those of the cloud storage service.

B. Limit the Scope and Application of the Third Party Doctrine of Trade Secret Law

Admittedly, there are unresolved questions concerning the scope of the third party doctrine of trade secret law (as there are with the scope of the Fourth Amendment's third party doctrine, discussed *infra*).[160] This appears to be due to three factors. First, the meaning of disclosure under trade secret law is underexplored and under-theorized. This is important because the third party doctrine of trade secret law assumes a degree of revelation of trade secret information between the trade secret owner and the third party, but the extent of the revelation needed to trigger a waiver is not clearly defined or well understood. Second, because trade secret misappropriation cases often involve bad acts, including potential criminal

[160] *See infra* text accompanying notes 206–214.

activity, there is a tendency among triers of fact to find trade secrets where none exist under a strict application of trade secret principles in order to be able to punish the alleged wrongdoer.[161] This could happen, for instance, where a court focuses on the efforts of a trade secret owner to protect its trade secret intra-enterprise and finds them "reasonable" while ignoring facts that show the information was otherwise distributed to third parties with little or no protection efforts. Finally, disagreements about the proper scope of the third party doctrine often reflect a lack of understanding concerning the evolution of trade secret law and why some of its requirements have become more stringent and less flexible.[162] In this regard, reliance on cases that predate the adoption of the UTSA to define the scope of the third party doctrine is problematic given the critical importance of the notice function of the reasonable efforts requirement under modern trade secret law.[163]

The critical issue concerning the scope of the third party doctrine of trade secret law centers around the question of whether the sharing of information with a third party must

---

[161] The author is not advocating that wrongdoers should be able to avoid responsibility for their wrongs but that such wrongs do not always amount to trade secret misappropriation. Other theories of tort liability and criminal wrongdoing exist (or could be created) to address specific wrongful acts without having to pretend that trade secrets exist when they do not. *See* Sharon K. Sandeen *The Third Party Problem: Assessing the Protection of Information Through Tort Law*, *in* INTELLECTUAL PROPERTY PROTECTION OF FACT-BASED WORKS: COPYRIGHTS AND ITS ALTERNATIVES 278 (Robert F. Brauneis ed., 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1680546.

[162] *See* Sandeen, *supra* note 92, at 500.

[163] *See supra* Part III.A.; *see also* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others.").

result in the information becoming generally known or readily ascertainable for trade secrecy to be lost, or whether trade secrecy is lost when information is shared with another who is not under a duty of confidentiality. In their treatise on trade secret law, Roger Milgrim and Eric Bensen suggest possible limitations to the third party doctrine of trade secret law so that a trade secret owner's voluntary, non-accidental third party disclosures are not considered unreasonable efforts unless they result in the information becoming generally known.[164] Consistent with this limited view of waiver, they identify three principal ways that a trade secret owner can destroy its own trade secrets: (1) disclose the secrets to the world through publication, for instance, in a published patent application or trade journal or by posting the trade secrets on the Internet; (2) disclose the trade secrets in a marketed product or service that can be reverse engineered; or (3) disclose the trade secrets to another without an adequate promise of confidentiality.[165] Quoting the pre-UTSA and very early case of *Tabor v. Hoffman*, Milgrim and Bensen opine that "[t]he issue is whether the sale or other act in fact discloses the trade secret."[166]

There are at least three problems with the last statement. First, in order to apply the suggested rule correctly, the meaning of disclosure must be understood. Although it may seem obvious to the layperson what is meant by "disclosure," just as there are different definitions of the public domain under different areas of law,[167] various areas of law (including

---

[164] *See* MILGRIM & BENSEN, *supra* note 21, § 1.05[3].
[165] *Id.* § 1.05[1]–[3].
[166] *Id.* § 1.05[3] (citing Tabor v. Hoffman, 118 N.Y. 30 (1889)).
[167] *See* Pamela Samuelson, *Mapping the Digital Public Domain: Threats and Opportunities*, 66 *LAW & CONTEMP. PROBS.* 147, 148–49 (2003).

trade secret law) apply varying definitions of "disclosure" depending upon the circumstances of a particular case. In fact, the two concepts are interrelated; generally, the "public domain" refers to the body of information that is unprotected by a given area of law while "disclosures" refer to the various acts that can waive applicable protection. Judging from the cases that have considered the question of what constitutes disclosure in various contexts, there are public policy and equitable reasons why disclosure may be defined more or less broadly depending upon the underlying purposes of the applicable law and who initiated the disclosure.[168] Moreover, as is discussed *infra*, the real issue suggested by *Tabor* is whether the alleged disclosure (in that case the public sale of a good) actually revealed anything.[169]

Second, the rule suggested by *Tabor* can be applied broadly to essentially do away with the reasonable efforts requirement altogether. In this regard, the varying definitions of disclosure that are discussed *infra* usually apply the broadest definition of disclosure to the voluntary acts of an information owner in sharing information with another.[170] This makes sense since information owners are in the best position to control the dissemination of their own information. Thus, if the test of waiver of trade secrecy for owner-initiated actions is whether the information becomes generally known or readily ascertainable, why not apply the same test to "lesser" forms of disclosure? In other words, why not dispense with the

---

[168] As Judge Rich explained, "the term 'public domain' as a 'question-begging concept,' and application of the concept to the facts at hand requires recourse to 'all sorts of legal concepts.'" Mine Safety Appliances Co. v. Electric Storage Battery, Co. 405 F.2d 901, 902 n.2 (C.C.P.A. 1969).
[169] *See infra* text accompanying notes 171–172.
[170] *See infra* Table 1.

reasonable efforts requirement and make the test of trade secrecy depend solely on whether the information is generally known and readily ascertainable and has economic value?

Based upon the drafting history and language of the UTSA, the obvious response to the foregoing questions is that the reasonable efforts requirement is one of three statutory requirements of trade secrecy and should not be ignored by courts.[171] But the question highlights the third problem with the statement from *Tabor,* namely, that application of the principle would undermine the notice and due process functions of the reasonable efforts requirement; in effect, it would allow information owners to protect information without giving actual or constructive notice of the existence of trade secrets and an expectation of confidentiality. While a defendant in a trade secret misappropriation case involving such information could always argue that it did not have the requisite "knowledge or a reason to know" of the existence of trade secrets and the need to maintain them in confidence, it would be easier to prevail on a motion for summary judgment if a bright-line test of waiver is applied. Additionally, doing away with the reasonable efforts requirement altogether may lead to the under-protection and over-assertion of trade secret rights.[172]

---

[171] Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("The remedial significance of such efforts lies in the fact that if the plaintiff has allowed his trade secret to fall into the public domain, he would enjoy a windfall if permitted to recover damages merely because the defendant took the secret from him, rather than from the public domain as it could have done with impunity." (internal citations omitted)).
[172] *See* Risch, *supra* note 116, at 45.

C. Narrow the Meaning of "Disclosure" Under Existing Trade Secret Law

Arguments that the storage of information in the cloud should not necessarily or automatically destroy the trade secrecy status of stored information are often based upon assumptions that the stored information is not actually "disclosed" to cloud storage services. Unfortunately, the definition of disclosure under trade secret law is under-theorized and not well understood. While on the surface the issue seems to involve a simple factual question, as the definitions of "disclosure" under trade secret law and other areas of law reveal, the applicable definition of disclosure often involves important policy questions. Thus, the measure of "disclosure" is not just a de facto test; it is a de jure test. Because the various definitions of disclosure under the law reflect important policy choices, any effort to modify those meanings should consider the underlying policies. As categorized below, the definitions differ not only because of the policies underlying the applicable law but based upon the actor and the circumstances surrounding the purported disclosure.

As a preliminary matter, it is important to note that the issue of disclosure arises in trade secret cases in two different ways. First, "disclosure" is one of three potentially wrongful acts that may subject an individual or company to liability for trade secret misappropriation, the other two being acquisition and use.[173] Second, as discussed *infra*, the act of disclosure can also be a trade secret destroying (or disqualifying) act, whether engaged in by a misappropriator, the owner of the trade secrets,

[173] UTSA § 1(4) (1985).

or a third party.[174] Unfortunately, courts and litigants do not always differentiate between the different actors when discussing the applicable meaning of disclosure and, in fact, there is little discussion of a definition of disclosure. For reasons that are explained *infra*, in some cases, the underlying purposes of trade secret law demand a narrow definition of disclosure (for instance, when a misappropriator shares the trade secrets with only a few people), while in other situations, a broader definition is warranted.[175]

Where the wrongful acquisition of trade secrets is suspected, a trade secret owner should act quickly and fight hard to prevent any actual disclosure by obtaining appropriate injunctive relief because failure to do so may result in the loss of trade secrecy due to the dissemination of the information. If dissemination of information by a misappropriator does occur ("Type I disclosure"), it is appropriate for the trade secret owner to assert a narrow definition of disclosure in order to limit the loss of trade secrets. Courts are often reluctant to hold that the acts of misappropriators, even if resulting in the dissemination of trade secret information to some third parties, constitute trade secrecy destroying disclosures unless the trade secrets become generally known.[176] From a policy point of view, this narrow view of disclosure makes sense because it provides a small window of time in which a trade secret owner can attempt to protect its rights.[177] Moreover, the limited

---

[174] *See supra* text accompanying notes 176–193.
[175] *Id.*
[176] *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'ns Servs., Inc., 923 F. Supp. 1231, 1254 (N.D. Cal. 1995).
[177] *See* Rowe, *supra* note 28, at 14–15 (discussing cases of trade secrets that end up in the hands of third parties who are not the original misappropriators and proposing an analytical framework for preserving

definition of disclosure applicable to the acts of misappropriators does not undermine the reasonable efforts requirement because the trade secret owner must prove some measure of reasonable efforts as part of its prima facie case.

Another form of disclosure that tends not to be treated harshly under trade secret la, but that often results in the loss of trade secrecy, concerns accidental disclosures ("Type II disclosures"). According to longstanding trade secret doctrine in the U.S., a trade secret owner who accidentally discloses trade secrets to a third party may be able to avoid the trade secrecy disqualifying effects of his inadvertence if he acts quickly to prevent further dissemination of the information.[178] Pursuant to the UTSA, a loss of trade secrecy will not result, and the third party possessor of the accidentally acquired information may be liable for trade secret misappropriation, unless the third party changed its position before receiving notice of the accidental disclosure.[179] Significantly, in situations where notice is timely received by the third party, the actual transfer or disclosure of the information to the third party is not counted as a trade secrecy waiving event.[180]

The third type of trade secret disclosure ("Type III disclosure") relates less to the actor who caused the disclosure and more to the extent and public nature of the disclosure. Specifically, it examines whether the subject information was (at the time of the alleged misappropriation) "generally

---

those trades secrets in some situations where they have subsequently been disclosed).

[178] *See* RESTATEMENT (FIRST) OF TORTS § 758 (1939).

[179] UTSA § 1(2)(ii)(C); *see also* MILGRIM & BENSEN, *supra* note 21, § 7.02[2][b].

[180] *See* Heriot v. Byrne, 257 F.R.D. 645, 654 (N.D. Ill. 2009) (analyzing effect of inadvertent disclosure made in e-discovery context).

known."[181] Underlying this type of disclosure is the well-established principle that intellectual property laws cannot be used to protect information that is in the public domain.[182] An early recognition of this concept by the U.S. Supreme Court was in a patent case, *Graham v. John Deere*, where the Court stated: "Congress may not authorize the issuance of patents whose effects are to remove existent knowledge from the public domain, or to restrict free access to materials already available."[183] Under trade secret law, protection is not available for information that has already been disclosed to the public either by the putative trade secret owner or another, including a misappropriator.[184] Conceptually, Type III disclosures are broader than Type I or II disclosures because there is no recognized basis upon which to limit the consequences of broad disclosures of information, other than possibly to restrict what is considered "generally known."[185] However, under longstanding trade secret doctrine, "generally known" includes

---

[181] *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished." (citing Harrington v. Natl. Outdoor Adver. Co., 196 S.W.2d 786 (Mo. 1946)); MILGRIM & BENSEN, *supra* note 21, § 1.01[2].

[182] *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc, 489 U.S. 141, 156 (1989) ("[W]e have consistently reiterated the teaching of *Sears* and *Compco* that ideas once placed before the public without the protection of a valid patent are subject to appropriation without significant restraint.").

[183] Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 6 (1966).

[184] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475–76 (1974).

[185] *See* discussion *supra* Part V.C (discussing Type I disclosures); Rowe, *supra* note 28, at 16.

information that is not only made known to the general public but also that which is known within discrete industries.[186]

Another form of a trade secrecy disqualifying disclosure ("Type IV disclosures") relates to the "readily ascertainable" language of the UTSA and is another example of how the definition of disclosure under trade secret law is fairly broad in defining the categories of information that do not qualify for trade secret protection.[187] While lay definitions of disclosure are often equated with broad, public dissemination, the concept that information might be readily ascertainable is narrower and, therefore, results in more trade secrecy disqualifying disclosures. It recognizes that information may not be generally known by the public or within an industry but may still be "disclosed" for trade secret purposes if it can be easily found in publicly accessible materials, such as scientific journals, books, or on websites, even if no one has actually accessed the information.[188] Elizabeth Rowe has explained that, in practice, courts often conflate "readily ascertainable" with "generally known" and

---

[186] UTSA § 1 (1985) Comment ("The language 'not being generally known to the public or to other persons' does not require that information be generally known to the public for trade secret rights to be lost. If the principal person who can obtain economic benefit from information is aware of it, there is no trade secret. A method of casting metal, for example, may be unknown to the general public but readily known within the foundry industry.").

[187] *See* UTSA § 1(4)(i). Some states, most notably California, do not analyze the ascertainability of information as part of plaintiff's prima facie proof of trade secrecy, but rather, frame the issue as a defense. *See* CAL. CIVIL CODE § 3426.1(d). This distinction does not affect the current discussion, however, because it concerns the broader and more abstract issue of what constitutes "disclosed" information under trade secret law.

[188] UTSA § 1 (1985) Comment ("Information is readily ascertainable if it is available in trade journals, reference books, or published materials.").

that a good way to think about the two concepts is that information is disclosed under trade secret law when it is either "known or knowable."[189] Generally, the ease with which information is knowable is the dividing line between whether information loses its trade secret status immediately upon becoming ascertainable, or whether it only loses its trade secret status when it has actually been found or reversed engineered and thereafter becomes "generally known."[190]

The fifth type of disclosure ("Type V disclosure") concerns information that would otherwise be a trade secret except that it is disclosed through no fault of the trade secret owner by the "rightful" acts of others, for instance, if others acquire the trade secrets through reverse engineering or independent development.[191] If the acts of reverse engineering and independent development are followed by a disclosure of the resulting information in a manner that makes it generally known or readily ascertainable, then the putative trade secret owner's rights in the same information no longer exist. A key reason for this rule is that the ability of individuals and companies to engage in reverse engineering and independent development is what differentiates trade secret protection from patent protection, thereby preventing state trade secret law

---

[189] Rowe, *supra* note 28, at 16–18. The broad definition of "readily ascertainable" information to include information that is knowable but not yet generally known is similar to the "in a printed publication" standard of patent law—which applies a very expansive definition of prior art—holding that information counts as patent disqualifying prior art if it is "sufficiently accessible, at least to the public interested in the art, so that such a one by examining the reference could make the claimed invention without further research or experimentation." *In re* Hall, 781 F.2d 897, 899 (Fed. Cir.1986).
[190] *See infra* text accompanying note 191 (discussing Type V disclosures).
[191] *See* MILGRIM & BENSEN, *supra* note 21, § 7.02(1) (describing the non-liability of the "honest" discoverer).

from being preempted by federal patent law.[192] It is also consistent with the general goal of promoting the dissemination of information and the flourishing of the public domain. Because there is nothing "wrong" with the acts of reverse engineering or independent development (except with respect to patented inventions, and possibly breach of contractual restrictions), public policy does not demand a narrow definition of disclosure with respect to Type V disclosures, and disclosures of this sort are conceptually broader than the first four types of disclosures described above.

Lastly, as discussed in Part IV, the meaning of disclosure under trade secret law also arises with respect to owner-initiated disclosures ("Type VI disclosures"). While such acts might result in information becoming generally known (a Type III disclosure) or readily ascertainable (a Type IV disclosure), the public availability of the information is arguably not required when a trade secret owner voluntarily transfers information to a third party without first establishing a duty of confidentiality. This is because of the various functions of the reasonable efforts requirement, including the notice, due process, and legitimacy functions, discussed *supra*.[193] A broad definition of disclosure with respect to voluntary, non-accidental owner-initiated acts is also consistent with notions of fairness and judicial efficiency. If a trade secret owner is not willing to engage in reasonable efforts to protect its allegedly valuable information, why should society intervene to protect it? Limits on the scope of trade secret protection (and by extension broad definitions of disclosure) also help prevent the use of trade secret litigation for anti-competitive purposes. The fact that a company did not engage in pre-litigation efforts to

---

[192] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490 (1974).
[193] *See supra* Part II.A.

protect its alleged secrets can suggest that its lawsuit is being used as a means to stifle competition rather than as a means to protect valuable trade secrets.

The various definitions of trade secrecy destroying disclosures under existing trade secret law can be diagramed as follows in Table 1:

Type of Disclosure		Actor	Concept of Disclosure
I.	Wrongful	Misappropriator	Broad
II.	Accidental	T/S Owner	Broad
III.	Gen. Known	T/S Owner or Other	Broader
IV.	Read. Ascert.	T/S Owner or Other	Broader
V.	ID and RE	T/S Owner or Other	Broader
VI.	Voluntary	T/S Owner	Broadest

Table 1.

While the foregoing categorization of disclosure principles under existing trade secret law may seem harsh, it is consistent with the purposefully limited and fleeting nature of trade secret protection and similar definitions of disclosure in other areas of law. In particular, most other areas of law are similarly harsh with respect to the treatment of owner-initiated disclosures of information and, therefore, they fail to provide useful models for a narrower conception of disclosure under trade secret law.

For instance, the issue of disclosure arises in patent cases because of the essential rule that a patent will not be granted for an invention that already exists in the "prior art."[194] The underlying purpose of this requirement is to reward truly "new" inventions and to preclude information from being removed from the public domain. In this way, it is similar to

[194] *See* 35 U.S.C. § 102 (2012).

the generally known and readily ascertainable requirements of trade secret law. As Robert Merges detailed in a recent article, there are several different definitions of (patent-disqualifying) disclosure under patent law that range from "widespread dissemination" on one end of the spectrum of disclosure to merely "a move away from complete secrecy."[195] Which patent definition of disclosure applies generally depends upon who is engaging in the act of disclosure and the form and manner of the disclosure.

Although it remains to be seen whether the recently enacted Leahy-Smith America Invents Act (the AIA) will narrow patent law's conceptions of disclosure,[196] under longstanding patent doctrine known as the *Metallizing Engineering* doctrine, a patent owner's act of using an invention in private in a manner that does not actually disclose the invention to the public can forfeit patent protection.[197] As explained in *Metallizing Engineering Co. v. Kenyon Bearing & Auto Parts Co:*

> [I]t is a condition upon an inventor's right to a patent that he shall not exploit his discovery competitively after it is ready for patenting; he must content himself with either secrecy, or legal monopoly. . . . [I]f he goes beyond that [grace period without filing a patent application], he forfeits his right regardless of

---

[195] *See* Robert P. Merges, *Priority and Novelty Under the AIA*, 27 BERK. TECH. L.J. 1023, 1036 (2012).
[196] *See, e.g.*, Paul Morgan, *The Ambiguity in Section 102(A)(1) of the Leahy-Smith America Invents Act,* 2011 Patently-O Pat. L.J. 29, 30 (2011); Merges, *supra* note 195, at 1023.
[197] Metallizing Eng'g Co. v. Kenyon Bearing & Auto Parts Co., 153 F.2d 516, 520 (2d Cir. 1946).

> how little the public may have learned about the invention . . . .[198]

Similarly, in *Egbert v. Lippman*, the Supreme Court considered whether the use of corset-stays by the inventor's girlfriend for a period over two years constituted a patentability-destroying "public use" even though the invention was not actually visible to the public.[199] In finding that the acts of the inventor constituted a patent-barring public use, the Court in *Egbert* set forth the following three principles:

> [1.] [T]o constitute a public use of an invention[,] it is not necessary that more than one of the patented articles should be publicly used[;]
>
> [2.] [W]hether the use of an invention is public or private does not necessarily depend upon the number of persons to whom its use is known [; and]
>
> [3.] [S]ome inventions are by their very character only capable of being used where they cannot be seen or observed by the public eye.[200]

An underlying purpose of the foregoing principles is to prevent an inventor from "sleeping on his rights" while the knowledge in the field of the invention advances around him and then, after a year or more of use of the invention, claiming

---

[198] *Id.* (quoting Pennock v. Dialogue, 27 U.S. 1 (1829)).
[199] *See* Egbert v. Lippman, 104 U.S. 333, 336 (1881).
[200] *Id.*

a right to a patent.[201] In effect, the public use bar forces inventors to file their patent applications sooner rather than later so that the public can benefit from the disclosures that are made in the patent application. If inventors use their inventions, but do not wish to make disclosures that are accessible to the public, then they forfeit their rights to a patent unless a patent application is timely filed.[202]

Pre-1989 copyright law also demonstrates that courts have long been unsympathetic to claims that a broad definition of disclosure with respect to owner-initiated disclosures will result in a forfeiture of valuable intellectual property rights. First, as detailed by Diane Zimmerman, copyright law in the U.S. used to have an explicit disclosure requirement in the form publication or registration, the latter being due to the deposit requirement.[203] Also, before March 1, 1989, U.S. copyright law provided that copyrights would not attach to works of authorship that were published without the requisite

---

[201] *Id.* at 337.

[202] References in patent law to "secret prior art" concerns the impact of pending (and unpublished) patent applications and the prior inventions of others and not the "secret" uses made by an inventor himself. *See* C. Douglas Thomas, *Secret Prior Art—Get Your Priorities Straight!*, 9 HARV. J. L. & TECH. 147, 173–74 (1996). With respect to individuals who are not the inventors of a "secret" invention, patent law does not count such "secret prior art" as prior art unless it meets the statutory definition of "prior art." *Id.* Thus, such individuals may be able to obtain a patent for the invention, but the inventor who used it secretly cannot (at least under pre-AIA law). *Id.*

[203] *See* Diane L. Zimmerman, *Trade Secrets and the "Philosophy" of Copyright: A Crash of Cultures*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 299 (Rochelle C. Dreyfuss & Katherine J. Strandburg, eds., 2011) (discussing the traditional disclosure purposes of U.S. copyright law).

notice of copyright.[204] Like the notice function of the reasonable efforts requirement of trade secret law, one of the purposes of this requirement was to put members of the public on notice of copyrights so that they could avoid infringing those rights. This was a stringent rule with few exceptions, despite the resulting forfeiture of valuable rights.[205]

Another area of law where public policy considerations have operated to create a broad definition of disclosure with respect to the act of an information owner is under the third party doctrine of Fourth Amendment jurisprudence, which generally recognizes that there is no reasonable expectation of privacy in information that has been voluntarily disclosed to a third party.[206] This doctrine was first recognized with respect to oral communications in a series of cases decided in the 1950s

---

[204] 17 U.S.C. § 10 (repealed 1978).

[205] 3 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 6:36 (2014) ("Section 10 of the 1909 Act provided: 'Any person entitled thereto by this title may secure copyright for his work by publication thereof with the notice of copyright required by this title.' The word 'may' was not discretionary; absent application of the savings clause in Section 21 or judicial tolerance for immaterial errors, the omission, imperfection, or misplacement of the notice resulted in loss of protection." (internal citations omitted)).

[206] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (explaining and defending the third party doctrine of Fourth Amendment jurisprudence). *But see* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011) (urging a more nuanced view of the Fourth Amendment's third party doctrine); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011) (arguing against an "aggressive" view of the Fourth's Amendment's third party doctrine particularly with respect to the transfer of information to "Internet intermediaries."); *see also* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011) (urging that a distinction be made between disclosures to an automated machine and a human being).

and 1960s.[207] The first of these cases was *Hoffa v. United States*, in which the Court held that voluntary statements made by Jimmy Hoffa to a "secret informer" did not violate the Fourth Amendment.[208] Since *Hoffa*, the third party doctrine of Fourth Amendment jurisprudence has been extended to a variety of non-oral communications. In *U.S. v. Miller*, it was extended to personal documents and records.[209] In *Smith v. Maryland*, the Supreme Court relied upon the doctrine in finding that the use of a pen register to record all outgoing phone numbers on a telephone line was not an improper seizure of information.[210] More recently, the doctrine has been used as the basis for finding that there was no reasonable expectation of privacy with respect to e-mail to/from records,[211] personal online data,[212] ISP subscriber information,[213] and e-mails and other documents stored by an ISP.[214]

Finally, although there is strong public policy behind the attorney-client privilege, it does not provide absolute

---

[207] *See* Tokson, *supra* note 206, at 597 (citing Hoffa v. United States, 385 U.S. 293, 303 (1966); Lewis v. United States, 385 U.S. 206, 210 (1966); Lopez v. United States, 373 U.S. 427, 438–39 (1963); On Lee v. United States, 343 U. S. 747, 751–55 (1952))
[208] *See Hoffa*, 385 U.S. at 303.
[209] *See* United States v. Miller, 425 U.S. 435 (1976).
[210] *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979). *But see* Riley v. California, 134 S. Ct. 2473 (2014) (recognizing a privacy right in data stored in and accessible via a cellphone and finding no exception for a warrantless search of a cellphone incident to a lawful arrest).
[211] *See* United States v. Forrester, 512 F.3d 500 (9th Cir. 2008). *But see* Warshak v. United States, 490 F.3d 455 (6th Cir. 2007).
[212] *See* Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 183 (D. Conn. 2005); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).
[213] *See* United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008).
[214] *See* Rehberg v. Paulk, 598 F.3d 1268, 1282 (11th Cir. 2010).

protection for information shared between an attorney and his client. The holder of the confidential information can lose protection through either overt or inadvertent acts involving the sharing of information with third parties to the attorney–client relationship.[215] Under the "strict approach" of waiver of the attorney–client privilege, if protected information is provided to a third party, the attorney–client privilege is lost.[216] While there are exceptions to the strict rule, they are limited. First, disclosures that are made to necessary agents of the attorney do not necessarily waive the attorney–client privilege.[217] Second, for a waiver of the privilege to apply, the disclosures must ordinarily be knowing and intentional acts. If the disclosure of otherwise privileged or protected information was inadvertent, a waiver of protection will not be found unless it appears that the acts of the discloser reflect gross negligence or a failure to take reasonable precautions.[218] In places that follow the "lenient approach," the client's subjective intent to waive will be considered.[219] Courts that take a "middle ground approach" will examine the circumstances and generally consider the

---

[215] *See* EDNA SELAN EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 398–407 (5th ed. 2012); John T. Hundley, *Waiver of Evidentiary Privilege by Inadvertent Disclosure—Federal Law*, 159 A.L.R. FED. 153 (2000).

[216] *See* Vincent S. Walkowiak & Thomas J. Leach, *Loss of Attorney-Client Privilege Through Inadvertent Disclosure of Privileged Documents*, in ATTORNEY-CLIENT PRIVILEGE IN CIVIL LITIGATION: PROTECTING AND DEFENDING CONFIDENTIALITY 385 (Vincent S. Walkowiak ed., 2008); *see also* EPSTEIN, *supra* note 215, at 398–407.

[217] *See, e.g.*, Commonwealth v. Mrozek, 657 A.2d 997, 999 (Pa. Super. Ct. 1995) (finding that a lawyer's secretary is an attorney subordinate, with whom communications can be protected by attorney–client privilege).

[218] *See, e.g.*, *In re* Grand Jury Investigation, 142 F.R.D. 276, 279 (M.D.N.C. 1992) (holding that certain disclosures should be considered intentional when they result from gross negligence).

[219] Walkowiak & Leach, *supra* note 216.

following factors to determine if an inadvertent disclosure should count as a waiver: (1) the reasonableness of the precautions to prevent the inadvertent disclosure; (2) the time taken to rectify the error; (3) the scope of the discovery; (4) the extent of disclosure; and (5) the overriding issue of fairness.[220]

In summary, although a legal maxim states that the "the law abhors a forfeiture,"[221] longstanding principles of law in a variety of fields demonstrate that there are times when other policy considerations override concerns about the loss of confidentiality. Thus, applicable policy considerations should be taken into account when considering whether to narrow existing definitions of disclosure under trade secret law, particularly since such narrowing will result in less information being available for public use.

D. Distinguishing Between "Disclosures" and "Mere Transfers"

The foregoing examination of disclosure principles under various areas of law—including existing trade secret law—does not provide an obvious or immediate answer to the question of how disclosure is to be defined (or redefined) with respect to trade secrets stored in the cloud. If anything, it reveals a strong public policy in favor of the waiver of applicable protections whenever an information owner voluntarily discloses information to a third party. As with the description of the third party doctrine of trade secret law, discussed *supra*,[222] some may question the foregoing

---

[220] *See* EPSTEIN, *supra* note 215, at 442–52; Walkowiak & Leach, *supra* note 216.
[221] *See, e.g.*, CAL. CIVIL CODE § 1442.
[222] *See supra* Part IV.

categorization of disclosure principles and argue for a narrower definition of disclosure with respect to voluntary, non-accidental owner-initiated acts. However, even if such acts are categorized as Type I disclosures, there is still a risk that trade secrets will be lost when they are stored in the cloud, as the victims of alleged misappropriators know all too well.[223]

Another option is to create a new, narrower definition of disclosure that would apply to cloud-based information sharing (a Type <I disclosure, if you will).[224] Like the Internet service providers that preceded them, cloud storage services are apt to argue that a special definition of disclosure is needed to ensure the flourishing of the cloud computing industry, otherwise individuals and businesses will be reluctant to store their information in the cloud.[225] However, there is a risk that any change in the definition of disclosure that is designed to

---

[223] *See* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1353 (E.D. Va. 1995).

[224] *See generally* Rowe, *supra* note 28 (addressing the problem of disclosures over the Internet and proposing a test for limiting such disclosures); *see also* Bruce T. Adkins, Note, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151, 1193 (1996) (suggesting that a "right of privacy" should be recognized for certain disclosures over the Internet).

[225] The cloud computing industry joined together to make a similar argument in American Broadcasting Companies, Inc. v. Aereo, Inc., which was recently decided by the U.S. Supreme Court. In the majority opinion in *Aereo*, Justice Breyer suggests that the solution to the perceived concerns of the cloud computing industry is for it to petition Congress, citing the Digital Millenium Copyright Act as an example of an industry-sponsored solution to perceived problems posed by new technologies. *See* Am. Broad. Co., Inc. v. Aereo, Inc., 134 S. Ct. 2498 (2014); Brief of Computer & Communications Industry Association and Mozilla Corporation as Amici Curiae Supporting Respondents, Am. Broad. Co., Inc. v. Aereo, Inc., *available at* http://sblog.s3.amazonaws.com/wp-content/uploads/2014/04/13-461_resp_amcu_ccia-moz.authcheckdam.pdf.

solve the cloud storage problem will have broader implications for trade secret law and practice. In particular, as discussed *supra*, a change in the definition of disclosure could render the reasonable efforts requirement superfluous and undermine the important notice and due process functions of that requirement.[226] Additionally, while there is a greater "policy of disclosure" under patent law than trade secret law, the U.S. Supreme Court in *Kewanee* recognized a disclosure purpose in trade secret law.[227] Any narrowing of the definition of disclosure under trade secret law would, arguably, be inconsistent with that purpose.

On the other hand, the law does not exist in a vacuum and consideration must be given to technological developments that change how individuals and businesses interact. As Professor Katherine Strandburg explained in an article On the On the other hand, the law does not exist in a vacuum and consideration must be given to technological developments that change how individuals and businesses interact. As Professor Katherine Strandburg explained in an article concerning the third party doctrine of Fourth Amendment jurisprudence: "[C]ourts should adopt an approach of technosocial continuity, recognizing that intertwined technological and social changes require not only the protection of privacy in conventional social contexts against technological intrusions, but also the

---

[226] *See supra* text accompanying note 172.

[227] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 486 (1974) ("Another problem that would arise if state trade secret protection were precluded is in the area of licensing others to exploit secret processes. The holder of a trade secret would not likely share his secret with a manufacturer who cannot be placed under binding legal obligation to pay a license fee or to protect the secret. The result would be to hoard rather than disseminate knowledge." (citation omitted)).

adaptation of privacy protections to the evolution of social context and governing social norms."[228]

Similar observations can be made with respect to changing business methods. With respect to cloud computing, the capabilities and efficiencies that it provides may simply be too irresistible and important to individuals and businesses, thereby raising questions whether and how trade secret law should adapt to meet this new reality.

Borrowing from recent scholarship related to the Fourth Amendment's third party doctrine[229] and the idea of a "taxonomy of privacy,"[230] rather than change the existing definitions of disclosure under trade secret law, an expanded taxonomy for trade secret law is proposed, whereby a distinction is explicitly recognized between information flows that are "disclosures" of trade secrets and information flows that are "mere transfers" of trade secrets (both of which are defined *infra*).[231] Although this may seem like a distinction without a difference (i.e., merely relabeling a possible Type <I disclosure as a "mere transfer"), there are significant factual differences between "transfers" and "disclosures" that are

---

[228] Strandburg, *supra* note 206, at 680.

[229] *See* sources cited *supra* note 206; Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1 (2005); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007).

[230] *See* Solove, *supra* note 34, at 485 ("[T]he goal [of this taxonomy] is simply to define the activities [that affect privacy] and explain why and how they can cause trouble. The question of when and how the law should regulate can only be answered in each specific context in which the question arises.").

[231] *See infra* text accompanying notes 242–243.

likely to make the labels meaningful to lay people and that are consistent with common sense.

As the U.S. Supreme Court and other courts have begun to realize, new technologies—including new methods of conducting business and exchanging information—require careful consideration of how information flows.[232] Based upon recent surveys, it appears that a significant percentage of individuals expect privacy with respect to information that is stored on third party computer servers, particularly when they believe that such information will not be read or accessed by a human being.[233] For this reason, among others, it is argued that courts that attempt to apply the Fourth Amendment in the Internet context should be careful to distinguish between disclosures that are made to humans and those that are made to machines.[234] As the Supreme Court recently explained in a case involving the alleged unlawful search and seizure of text messages: "The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on Fourth Amendment implications of emerging

---

[232] *See, e.g.*, City of Ontario v. Quon, 560 U.S. 746, 758–59 (2010); Strandburg, *supra* note 206 (detailing U.S. Supreme Court and state court decisions where a more nuanced view of third-party disclosures for Fourth Amendment purposes); *see also* Henderson, *supra* note 229.

[233] *See* Tokson, *supra* note 206, at 621 ("Does all [the recent surveys of Internet users] mean that a large proportion of Internet users are indifferent to the privacy of their online data? This Article argues that is does not. Rather, while users perceive disclosure of their personal information to humans as a serious privacy harm, they do not consider disclosure to automated systems alone to be a significant harm.").

[234] *Id.*

technology before its role in society has become clear."[235] Likewise, courts must proceed cautiously to determine what uses of technology constitute disclosures to a third party that would trigger the need for a confidentiality agreement under trade secret law.

In a series of articles, Professor Stephen Henderson details recent critiques of the Fourth Amendment's third party doctrine and the cases (mostly state court cases) that have applied a more nuanced analysis.[236] Rather than simply advocating for abolishing the third party doctrine as some have done, he suggests a multi-factored test that would better account for advances in technology and the expectations of information owners when using such technology.[237] Borrowing

---

[235] *Quon*, 560 U.S. at 759.

[236] *See* Henderson, *supra* note 206 (setting forth a four-factor test); Henderson, *supra* note 229; Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 36 MERCER L. REV. 507 (2005) (setting forth a nine-factor test).

[237] Initially, Professor Henderson suggested a nine-factor test, but he has since reduced the number of proposed factors to four. Henderson, *supra* note 206, at 50–51. The four factors that Professor Henderson considers relevant in the Fourth Amendment context are: (1) the initial transfer of the information from the person to a third party is reasonably necessary to participate meaningfully in society or is socially beneficial, including freedom of speech and association; (2) the information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma is disclosed, and whether outside of the initial transfer to a third party it is typically disclosed only within one's close social network, if at all; (3) the information is accessible to and accessed by nongovernmental persons outside the institution; and (4) existing law restricts or allows access to and dissemination of the information or similar information. *Id.*

from Professor Henderson's list of factors, and after considering the nature of cloud storage services, the factors that seem most relevant to the question of whether the act of transferring information to the cloud should constitute a third party disclosure for trade secret purposes include:

1. Public policy considerations, including the importance of specific cloud services;
2. The purpose of the transfer;
3. The representations of the cloud storage service;
4. The objective and subjective expectations of the uploading party;
5. The automation and functionality of the cloud storage service, i.e., whether it is merely a conduit or passive recipient for stored information;
6. The ability of the cloud service provider to access the information and whether such access is by a human or a machine; and
7. Whether the information has actually been accessed and used.

While it remains to be seen how Fourth Amendment jurisprudence will develop with respect to information that is stored in the cloud,[238] the arguments that call for a more nuanced view of waiver with respect to such information can be applied to trade secret law as well. This is particularly true since courts have traditionally applied a stricter definition of

[238] The U.S. Supreme Court's recent decision in Riley v. California mentions the cloud and suggests that personal information stored in the cloud is deserving of protection akin to information maintained in one's house. 134 S. Ct. 2473 (2014).

waiver to trade secrets than to Fourth Amendment rights.[239] If it is generally easier for a trade secret owner to avoid loss of trade secrecy than it is for an individual to waive his expectation of privacy under the Fourth Amendment (principally because the interests of law enforcement are not involved), then the arguments for limiting application of the Fourth Amendment's third party doctrine are stronger when applied to the thirty party doctrine of trade secret law.

i. Public Policy

Earlier in this Article, the public policy that underlies the reasonable efforts requirement and the third party doctrine of trade secret law was discussed to explain why neither ignoring the reasonable efforts requirement nor creating a new definition of disclosure is recommended as workable refinements to the third party doctrine of trade secret law.[240]

---

[239] In Dow Chem. Co. v. United States, the Supreme Court held that Dow Chemical had no reasonable expectation of privacy with respect to "open areas" observable by aerial surveillance. 476 U.S. 227, 239 (1985). However, in the trade secret case of E.I. duPont deNemours & Co. v. Christopher, the aerial surveillance of a plant under construction was found to be an act of trade secret misappropriation. 431 F.2d 1012 (5th Cir. 1970). Similarly, in California v. Greenwood, the Supreme Court held that there was no reasonable expectation of privacy in information that was placed in a garbage can that was then placed on a public street for pick-up. 486 U.S. 35 (1988). In contrast, some courts have recognized continued trade secret protection for trade secrets placed in garbage cans. *See, e.g.*, Tenant Co. v. Advance Mach. Co., Inc., 355 N.W.2d 720 (Minn. Ct. App. 1985) (analogizing to California's Fourth Amendment jurisprudence). While such cases are probably best explained by the desire to punish the defendants' "bad acts" in acquiring, disclosing or using plaintiff's trade secrets, they signify that there are reasons to treat waiver under the Fourth Amendment different from waiver under trade secret law.

[240] *See supra* Parts III–IV.

The public policy considered here concerns whether a distinction between a "mere transfer" and a "disclosure" should be made to accommodate situations, like those existing in the cloud, where third parties are largely passive possessors of information. Obviously, the cloud computing industry has a great interest in this question because the failure to recognize such a distinction threatens to dissuade the use of the cloud and to increase transactions costs associated with specially negotiated confidentiality agreements. But the more important question concerns the delicate balance between protection of intellectual property rights and free competition that our intellectual property rights seek to achieve.[241] As Goldilocks would say, trade secret doctrine cannot be too loose or too strict, but must be "just right."

Because explicit recognition of a distinction between mere transfers of information and disclosures of information would result in more information potentially being protected as trade secrets, the purposes of trade secret law are furthered. But these same rationales also apply to proposals which ignore the reasonable efforts requirement and create a narrower definition of disclosure; thus, the policy argument in favor of a mere transfer test cannot simply be "because trade secret protection is good." Nor can the argument against such a test be "because the disclosure of ideas and information is good." Rather, while acknowledging the underlying purposes and limits of trade secret law, the key question is: What are the additional policy arguments that tip the balance in favor of the proposal?

---

[241] *See, e.g.*, Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 150–51 ("The federal patent system thus embodies a carefully crafted bargain for encouraging the creation and disclosure of new, useful, and nonobvious advances in technology and design in return for the exclusive right to practice the invention for a period of years.").

One argument is that the proposed new test would best reflect reality and the fact that the operative "acts" are different. In this regard, the common dictionary definitions of disclosure and transfer reveal important differences that we should assume inform the actions of the lay public. According to Black's Law Dictionary, "disclosure" is defined as "the act or process of making known something that was previously unknown; a revelation of facts."[242] In contrast, "transfer" is defined as "to convey or remove from one place or one person to another; to pass or hand over from one to another."[243] The key distinction between the two terms is that one necessarily involves the transfer of knowledge and one does not. In this regard, "revelation" is defined as something revealed, with "reveal" being defined as "to make known, manifest."[244]

Another argument in favor of a "mere transfer" test concerns a policy expressed by the U.S. Supreme Court in *Kewanee v. Bicron Oil* that asserts that trade secret requirements that are too stringent are against public policy because they prevent the desired leakage of information into the public domain and because they would force businesses to spend too much time and effort on protection efforts.[245] In his article, *Why Do We Have Trade Secrets?*, Michael Risch put this policy in economic terms and identified it as the true "incentive purpose" of trade secret law, namely, the ability of companies to allocate fewer resources to both the protection and appropriation of secret resources.[246] The latter benefit

---

[242] BLACK'S LAW DICTIONARY, *supra* note 150, at 531.
[243] *Id.* at 1636.
[244] The New Lexicon Webster's Dictionary of the English Language 851 (Encyclopedic ed. 1987).
[245] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).
[246] *See* Risch, *supra* note 116, at 5.

promotes trade secret leakage, which enhances the sharing of information, while the former benefit reduces the costs of protection efforts. It is a classic "win-win" as long as the balance is maintained. Because a "mere transfer" test would be limited (as described *infra*),[247] it should not upset the balance by causing either the under-protection of trade secrets assets or the over-assertion of trade secret rights.

Finally, explicit recognition of a "mere transfer" test would provide a label and analytical framework for a distinction that, apparently, has already been made with respect to "old-school" document storage practices.[248] While many of the pre-cloud data storage practices involved express promises of confidentiality, the fact that there has not been more litigation on this issue suggests that the general public understands and respects the distinction between mere transfers and disclosures. Conceptually, such a distinction is also at the heart of the rule that trade secrets can be embedded in products that are mass distributed without the trade secret owner losing trade secret rights merely due to the mass distribution of the products.[249] The distinction is due to the fact that some mass-produced products (or services) are "self-disclosing" and some

---

[247] *See infra* Part V.D.ii.

[248] *See* Goda & Kitsuregawa, *supra* note 44.

[249] *See* Eric Douma, *Fair Use and Misuse: Two Guards at the Intersection of Copyrights and Trade Secret Rights Held in Software and Firmware*, 42 IDEA 37 (2002). As noted previously, the relevant distinction with respect to embedded trade secrets relates to the difference between information that is readily ascertainable and that which must be reverse engineered in order for trade secrets to be gleaned therefrom. *See supra* text accompanying note 84; *see also* Gilburne & Johnston, *supra* note 68, at 233 ("The issue of trade secret protection for ideas embodied in products distributed widely without restriction on use or disclosure would thus seem to turn on how difficult it is to 'reverse engineer' the product.").

are not.[250] Thus, the mere transfer or sale of a product in which trade secrets are embedded does not act as a trade secrecy destroying disclosure unless the trade secrets are actually revealed to members of the general public or to experts in the field.

ii. Purpose of Transfer

As previously described, the cloud computing industry is still evolving and the nature of services it offers vary greatly.[251] For this reason, it is not proposed that a mere transfer test automatically apply to all instances where information is stored in the cloud; such an application would be too loose. Instead, in the same way that the reasonable efforts requirement of trade secret law requires a case-by-case assessment of the circumstances, whether the mere transfer test should apply in any given case will depend on the facts, including the purpose of the transfer.

Although individuals and companies who use cloud storage services may simply want a place to store or back-up digital files, others may use the cloud for purposes that involve collaboration and the sharing of information. If the people who are sharing and collaborating are all employees of the same company or are otherwise under duties of confidentiality with respect to the shared information, then the trade secret analysis should focus on the reasonable efforts with respect to those individuals. If the sharing and collaborating involves third parties who are not under a duty of confidentiality, the nature

---

[250] *See* Katherine J. Strandburg, *What Does the Public Get? Experimental Use and the Patent Bargain*, 2004 WIS. L. REV. 81, 104–06 (defining "self-disclosing" products).
[251] *See generally* Part II.

and extent of such sharing and collaboration must be closely examined to determine if there was trade secrecy destroying disclosures. This might involve communications or collaborations between a trade secret owner and representatives of a cloud computing service with respect to web-hosting or SaaS services. In other words, if the purpose of the transfer is to communicate knowledge from one human being to another, the same rules that apply to non-cloud communications should apply and such transfers should constitute disclosures that waive trade secret protection unless a pre-disclosure obligation of confidentiality is formed between the trade secret owner and the third party. However, if the purpose of the transfer is merely to move information from one place to another, for instance from an in-house server to a cloud server, the mere transfer rule should apply.

As a practical matter, the fact-specific nature of the required analysis means that companies still need to be careful about where and how they store their trade secrets and who is allowed to learn or see such secrets. The mere transfer test would give them the option of using some cloud storage services in limited ways that do not risk the loss of trade secrecy. In order to foster the growth of the cloud computing industry, it is recommended that cloud storage services design specific services that allow for mere transfers and the segregation of important trade secret and other proprietary information.

iii. Representations of Cloud Storage Services

For reasons that were previously explained, cloud storage services are often reluctant to promise security for

information that is stored in the cloud.[252] They are also apt to disclaim any liability for the loss of stored information and to guard against the creation of any express or implied duty of confidentiality. Thus, their representations are unlikely to serve as the basis of either a breach of contract or trade secret misappropriation claim unless sufficient facts exists to support a finding of an implied duty of confidentiality. This does not mean, however, that the representations of cloud storage services would not be relevant in determining whether a disclosure—as opposed to mere transfer—of trade secrets has occurred. Without forming the basis of a duty of confidentiality, the representations of cloud service providers might reveal important facts, such as whether and to what extent information that is stored in the cloud is accessed and used by employees of the cloud service provider or by others.[253] The representations of cloud service providers may also provide insights regarding the expectations of trade secret owners or, as a matter of fairness and equity, justify applying the mere transfer test in a given case.

In this age of ubiquitous click-wrap agreements and cyber-hacking activities, one can imagine a scenario where a company, desiring to comply with the mere transfer test, carefully investigates the nature of services provided by a cloud storage service to ensure that its stored information will not be used or accessed by third parties, only to find out later that the representations that were made by the cloud storage service were inaccurate. While the liability limiting provisions of the click-wrap terms of service agreement may make it difficult for the company to sue the cloud storage service for

---

[252] *See supra* text accompanying note 78–91.
[253] *See, e.g.*, *Google Terms of Service*, *supra* note 8.

breach of contract or trade secret misappropriation,[254] an equitable question arises whether any information that was revealed to others under such circumstances should lose its trade secret status. Like the Type I disclosures described above, assuming that the subject information did not otherwise become generally known or readily ascertainable, no information would be removed from the public domain by applying the mere transfer test in such a situation. Additionally, the notice and due process functions of the reasonable efforts requirement are not undermined because the company arguably engaged in reasonable efforts by first investigating the nature of the services provided by the cloud storage company and concluding that a confidentiality agreement was not required because of the mere transfer test.

iv. Expectations of the Uploading Party

On the surface, the "expectations of the uploading party" factor is similar to the just discussed "representations of the cloud storage provider" factor, but it comes at the issue from a slightly different angle. A rule of Fourth Amendment jurisprudence is that information should not be protected when the information owner does not have a subjective expectation of privacy.[255] In other words, there is a difference between what an individual actually believed and what he could reasonably expect based upon applicable social norms.

---

[254] Obviously, the company would have a fraud or false advertising claim against the cloud storage service, but the fact that third parties accessed or used information when they were not under a duty of confidentiality also presents problems with respect to the trade secret status of the information.

[255] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

Pursuant to Fourth Amendment jurisprudence, it is only if it is first established that a person had a subjective expectation of privacy that the subsequent question of whether the expectation of privacy was reasonable according to prevailing social norms can be asked.[256]

The third party doctrine of trade secret law also reflects subjective and objective aspects. The reasonable efforts requirement looks for objective evidence in the form of affirmative efforts to maintain secrecy as evidence, among other things, of an expectation of secrecy. Pursuant to the independent requirement of a duty of confidentiality, however, it also demands that both parties to the information transfer have the subjective understanding that the information will be kept confidential.

In the case of alleged "mere transfers" of information to the cloud, objective evidence of reasonable efforts to maintain secrecy will continue to be important both intra-enterprise at the trade secret owner's facilities and within the cloud. Thus, trade secret owners who choose to store information with a cloud storage service should investigate the level of security that is provided and take advantage of the various security tools that are available for stored information. What is conceptually different under a "mere transfer" test is the necessary subjective understanding of the cloud storage service. If a disclosure of trade secrets does not occur, a trade secret owner should not have to demonstrate that the cloud storage service had a subjective understanding that the information should be kept confidential. However, the subjective belief of a putative trade secret owner would be relevant. For instance, if the putative trade secret owner did not care whether information

---

[256] *See id.*

stored in the cloud was kept confidential, then application of the mere transfer test is not needed to further an expectation of confidentiality. If a subjective expectation of confidentiality is shown, then a deeper analysis is needed to determine if there was an actual disclosure or only a mere transfer.

v. Functionality of Cloud Storage Services

How cloud services are established and whether they include tools to facilitate confidentiality and secrecy is another factor to consider. Although cloud storage services may be reluctant to contractually guarantee confidentiality and secrecy, they often offer functionality that could suggest the act of storage is a mere transfer of information rather than a disclosure. In fact, many cloud service providers label and otherwise differentiate their cloud services by focusing on functionality and, if a mere transfer test is recognized, they would be incentivized to engage in more of these efforts.

With respect to functionality, the critical distinction to be drawn between "mere transfers" and "disclosures" is akin to the distinction that is drawn between "passive" and "active" ISPs. In the early days of the Internet, questions arose concerning the liability of ISPs for the content posted on their websites, particularly user-generated content, and whether their online "presence" subjected them to personal jurisdiction in particular jursidictions.[257] In the same way that cloud storage services do not want to incur liability related to the terabytes of information that they store for their customers, ISPs did not want to be held liable for defamation, copyright infringement, and other torts related to the vast amount of content posted by

[257] *See, e.g.*, Zippo Mfg. Co. v. Zippo DOT Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (concerning alleged trademark liability of ISP).

their customers. An early theory that, in many cases, limited the liability of ISPs was that they should not be liable if the website was "passive" or the ISP was a "mere conduit of information.[258]

As argued by Mathew Tokson in *Automation and the Fourth Amendment*, this factor should also include an examination of whether the transfer of information involves human intervention and, if so, the nature and scope of such intervention. [259] In this regard, while many cloud services, particularly storage services, might be highly automated, others may depend on human interaction that may require knowledge of customer information. If knowledge is revealed through the storage of information, then arguably there is a disclosure rather than a mere transfer.

vi. Ability of Cloud Service Providers to Access Stored Data

For various reasons unrelated to wanting to use (or even read) stored data, cloud computing services typically reserve the right to access stored data under specified conditions.[260]

---

[258] *See, e.g.*, *Religious Tech. Ctr. v. Netcom On–Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1372–73 (N.D. Cal. 1995) ("[I]t does not make sense to adopt a rule that could lead to liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet.").

[259] Tokson, *supra* note 206, at 601–04 (describing automation on the Internet).

[260] One interesting example comes from a Rackspace blog: "It is Rackspace's policy that it will not access, transfer or deliver data stored on servers by Rackspace's customers in response to any government authorities *other than pursuant to a properly issued, lawful request from appropriate law enforcement officials or other order from a competent body from the country in which the servers are physically located.* This applies

Should the fact that stored data can be accessed be the test of disclosure for trade secret purposes, or should a disclosure that waives trade secret protection only occur when the information is actually accessed? Should the fact that government officials might be free to search and seize stored information, or actually search or seize such information, constitute a disclosure that waives trade secret protection?

To answer the foregoing questions, it is suggested that a distinction be drawn between: (1) transferred information that cannot be accessed by the transferee due to contractual or technical restrictions; (2) transferred information that can be accessed by the transferee but is not accessed; (3) transferred information that can be accessed by the transferee but only for limited purposes that does not involve the transferee's use of such information; and (4) transferred information that is accessed and used by the transferee. It is only the fourth type of transfer that would (in the absence of a duty of confidentiality) constitute a trade secret disclosing transfer.

The foregoing questions are also important with respect to whether a cloud storage service has a legal duty of confidentiality that may supersede any efforts by it to disclaim liability for the confidentiality or security of stored information. This is because the Stored Communications Act may impose a legal duty of non-disclosure with respect to some

---

to requests from law enforcement and includes those made under the Patriot Act. Our customers have full care, custody and control over their servers and the data that is stored on those servers —Rackspace does not have that control." Alan Schoenbaum, *Your Data is Your Data. Period.*, RACKSPACE (June 11, 2013), http://www.rackenspace.com/blog/your-data-is-your-data-period (emphasis added).

but not all of the listed types of disclosures.[261] Specifically, in cases where the Stored Communications Act applies, cloud storage services may be precluded from "knowingly divulging" stored information.

vii. Whether Access Has Occurred

When trade secret information is seen or used by another in such a way that the embedded knowledge is revealed to another human being, it is by definition "disclosed." Thus, while it is prudent to not designate any one factor as most important in the disclosure analysis, determining whether information has been accessed is the obvious first step in determining whether information was actually seen or used. It is also a critical factor in preserving the sieve-like quality of trade secret protection.[262] Although trade secret owners hate it when trade secrets are lost, trade secret protection is fleeting for important public policy reasons. If a company is careful, it can conceivably protect its trade secrets for decades, but they can also be lost in an instant due to no fault of the trade secret owner. Because of this reality a lot of resources can be wasted trying to protect information that others are likely to discover and disclose anyway. This should motivate companies to

---

[261] The Stored Communications Act is a Fourth Amendment–like statute that was designed by Congress to provide a measure of privacy for information that is handled by an "electronic communication service" (ECS) and a "remote computing service" (RCS). 18 U.S.C. § 2701 (2012). Where it applies, it prohibits the disclosure of information to law enforcement without a warrant or in response to a civil subpoena. *See* Crispin v. Christian Audiger, Inc. 717 F. Supp. 2d 965, 971–72 (C.D. Cal. 2010). Due to the specific and relatively narrow definitions of an ECS and an RCS, unless amended by Congress, it is unlikely to apply to all cloud storage services. *See* Robinson, *supra* note 157, at 1195.

[262] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490 (1974).

identify their most important trade secrets for special treatment and carefully limit access to that information, allowing other, lesser, trade secrets and proprietary information to potentially leak-out. This not only enriches the public domain, it reflects the balance that trade secret law seeks to achieve between free and robust competition and trade secret protection.

If the cloud storage service has not actually accessed, seen, or used the stored information, then the relationship between the trade secret owner and the cloud storage service is irrelevant. However, as noted above, the trier of fact would still have to examine whether the trade secret owner otherwise engaged in efforts that were reasonable under the circumstances to maintain the secrecy of the subject information.[263] With respect to information that is stored in digital form on a computer or other electronic devices, such efforts might include the use of passwords and encryption.[264]

E. A Proposed Analytical Framework

Although Fourth Amendment jurisprudence is not a model of clarity,[265] the bifurcated nature of its analysis provides a potential approach for applying the foregoing analysis and deciding whether a trade secret owner's act in storing information with a third party constitutes a "mere transfer" or a "disclosure." The bifurcated approach of Fourth Amendment jurisprudence first asks whether the challenged

---

[263] *See supra* Part V.A.
[264] *See* Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 366–68 (2009).
[265] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 528 (2007).

governmental action was a search.[266] If it was, the second part of the analysis asks whether the scope and manner of the search was reasonable. As explained by Orin Kerr, this bifurcated approach has the advantage of creating some predictability and clarity for law enforcement personnel. Importantly, "[d]ividing the Fourth Amendment into two stages provides considerable certainty by carving out a set of investigative steps that cannot lead to suppression."[267]

The analytical approach this Article proposes for use with respect to alleged trade secret information stored in the cloud involves a four-step process which, depending on how the parties and the court wish to structure the case, may precede or follow a determination whether the subject information is secret and has independent economic value.[268] The four steps are as follows:

Step 1: Did Information Flow to a Third Party?

Of course, the third party doctrine of trade secret law is not implicated unless the alleged trade secret information flows

---

[266] *See id.*
[267] *Id.*
[268] The plaintiff in a trade secret case has the burden of establishing both the existence of a trade secret and misappropriation. MILGRIM & BENSEN, *supra* note 21, § 16.01[3][a]. With respect to the first issue, the third party doctrine of trade secret law arises under the reasonable efforts requirement of trade secret protection, and thus, conceptually, it is the plaintiff's burden to prove that no trade secrecy destroying third-party disclosures occurred. This is not how the issue ordinarily arises, however. Usually, the plaintiff will present evidence of its intra-enterprise reasonable efforts to satisfy its prima facie case and then it is up to the defendant to find evidence of third-party disclosures. If such evidence is found, and the issue is raised in a motion for summary judgment brought by the defendant, then the issue may be decided before the plaintiff has to establish secrecy and economic value.

from the trade secret owner to a third party. Rather than attempting to define who is a third party for purposes of trade secret law, pre-existing law should be applied to determine this question. It is clear, however, that the transfer of information over a private network between servers owned by the trade secret owner would not count. Also, pursuant to the principles and policies underlying the Stored Communications Act and the Computer Fraud and Abuse Act, the use of the Internet (or another shared network) to transmit information between servers owned by the trade secret owner should not count.[269] Even though third party facilities are used for the transfer of information, the transient nature of such transfers should not trigger the third party doctrine of trade secret law.

More difficult issues may arise with respect to the flow of information between a trade secret owner and affiliates. Some affiliates may be closely enough related to the trade secret owner so that the transfer of information between such affiliates and the trade secret owner should not trigger the third party doctrine at all, such as information flows between employees of a company or between a parent company and its subsidiaries. However, the third party doctrine would be triggered when information flows between independent businesses.

Step 2: What Were the Circumstances, Nature, and Scope of the Information Flow?

It is at Step 2 where the multi-factored factual analysis that is discussed above should be applied. If it is concluded that the information flows only involved "mere transfers," then skip

[269] *See* The Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012); *see also* The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

to Step 4. It is only when a "disclosure" to a third party occurs that the third party doctrine of trade secret law applies to require a duty of confidentiality, discussed in Step 3.

Step 3: Did the Third Party Owe a Duty of Confidentiality to the Trade Secret Owner and Comply with It?

Although this Article is focused on voluntary, non-accidental, owner-initiated disclosures (described as Type VI disclosures), in other cases, it may be necessary under this step to determine if the principles governing a different type of disclosure apply. With respect to Type VI disclosures, the question to be examined at this stage is whether the third party is under an express or implied duty of confidentiality. If a duty of confidentiality exists, then it must be determined if the third party complied with that duty by engaging in reasonable efforts on its end to protect the shared trade secrets. If it did not comply, the trade secret owner may have a claim against the third party, but any disclosures by that third party may have destroyed the trade secrecy status of the information going forward. If there was no duty of confidentiality, then for the reasons set forth above, the "disclosure" of information to the cloud storage service waived the trade secrecy of stored information.

Admittedly, there is an odd circularity to the order of the analysis here because, if an express or implied duty of confidentiality exists, the distinction between "mere transfers" and "disclosures" is not needed to preserve the trade secrecy of stored information. Thus, in some cases it may make sense to consider the existence or non-existence of a duty of confidentiality first. In other cases, the distinction between "mere transfers" and "disclosures" may be important even if a duty of confidentiality exists, for instance, to define the scope and nature of the third party's duty.

Step 4: Did the Trade Secret Owner Otherwise Engage in Reasonable Efforts to Protect Its Trade Secrets?

Regardless of the choices that a trade secret owner makes concerning the flow of its information, the configuration of its computer systems, and the nature of its business relationships, applicable law requires that it institute reasonable precautions if it wants to protect its trade secrets. Step 3 requires an examination into the reasonable efforts that are engaged in by a third party when trade secret information is disclosed to a third party who is under a duty of confidentiality. In no event, however, do the obligations of a third party, if any, excuse a trade secret owner from exercising reasonable efforts of its own. Whether the flow of information to a third party is considered to be a "mere transfer" or a "disclosure," these efforts should include affirmative steps that are reasonable under the circumstances to ensure that the transfer and storage of information is secure through the use of encryption, passwords, and similar strategies.

VI. CONCLUSION

New technologies and new methods of conducting business always present challenges for the business community, their legal advisors, and the legal system. The emergence of cloud computing is no exception. Luckily, companies are willing to proceed with innovation despite uncertainties, and lawyers are willing to support their clients' aspirations by helping them to understand and manage the associated risks. The goal of this Article was to provide both an understanding of existing trade secret law and a proposed solution to the third party doctrine of trade secret law that will enable better risk management and that will assist courts in analyzing trade secret disputes that arise in the cloud. Some trade secrets are bound to be lost in the cloud, but with

planning, others may be preserved. Hopefully, the analytical framework set forth above will enable legitimate trade secrets that are stored in the cloud to be protected while still respecting both the purposes behind the reasonable efforts requirement of trade secret law and the balance between trade secret protection and free competition that underlies existing trade secret doctrine.