Richmond Journal of Law & Technology

Volume 22 | Issue 3 Article 1

2016

# Addressing Employee Use of Personal Clouds

Philip Favro

# ADDRESSING EMPLOYEE USE OF PERSONAL CLOUDS

Philip Favro*

Cite as: Philip Favro, *Addressing Employee Use of Personal Clouds*, 22 RICH. J.L. & TECH. 6 (2016), http://jolt.richmond.edu/v22i3/article6.pdf.

## I. INTRODUCTION

[1] Cloud computing is one of the most useful innovations in the digital age.[1] While much of the attention on recent advances has focused on smartphones, tablet computers, and wearable technology, the cloud is perhaps unrivaled in its utility for organizations.[2] From simplified data storage to innovative software platforms, enterprise-grade cloud solutions provide cost-effective alternatives to acquiring expensive computer hardware and software.[3] Enterprise clouds also offer a collaborative work environment for a mobile and widespread work force, enabling businesses to maximize worker productivity.[4]

---

*Consultant, Discovery and Information Governance, Driven, Inc.; J.D., Santa Clara University School of Law, 1999; B.A., Political Science, Brigham Young University, 1994.

[1] *See* Joe McKendrick, *5 Benefits of Cloud Computing You Aren't Likely to See in a Sales Brochure*, FORBES (July 21, 2013, 9:04 PM), http://www.forbes.com/sites/joemckendrick/2013/07/21/5-benefits-of-cloud-computing-you-arent-likely-to-see-in-a-sales-brochure/#34a34b6e7d85, *archived at* http://perma.cc/ET8N-JKG5.

[2] *See* Edwin Schouten, *5 Cloud Business Benefits*, WIRED (OCT. 5, 2012), http://www.wired.com/insights/2012/10/5-cloud-business-benefits/, *archived at* https://perma.cc/7LJK-RP4M.

[3] *See* Jim Lynch, *What Are the Benefits and Drawbacks of Cloud Computing?*, TECHSOUP (Feb. 6, 2015), http://www.techsoup.org/support/articles-and-how-tos/what-are-the-benefits-and-drawbacks-of-cloud-computing, *archived at* https://perma.cc/9JYQ-AD93.

[4] *See id.*

[2] Organizations are not alone in reaping the benefits of cloud computing. Individuals have likewise discovered the value that cloud providers offer in their personal lives.[5] With increased storage for digital photos, music, and other files, personal cloud providers help users avoid losing personal data when a computer hard drive inevitably fails.[6] Furthermore, the transfer functionality afforded by personal clouds enables users to seamlessly move data between computers, smartphones, and other mobile devices.[7]

[3] With such utility at their fingertips, it should come as no surprise that individuals use personal clouds to facilitate work responsibilities.[8] Personal cloud providers like Dropbox, Box, and Google Drive can obviate clunky network storage options and simplify data sharing and teamwork among colleagues.[9] While employees of many organizations

[5] *See* Nicholas Lee, *Is Your Corporate Data Appearing on Personal Clouds?*, CLOUDTWEAKS (Sept. 9, 2015), http://cloudtweaks.com/2015/09/is-your-corporate-data-appearing-on-personal-clouds/, *archived at* https://perma.cc/HD3C-VDDX.

[6] *See* Zack Christenson, *Benefits of Cloud Computing*, AMERICAN CONSUMER INSTITUTE (Sept. 30, 2013), http://www.theamericanconsumer.org/2013/09/benefits-of-cloud-computing/, *archived at* https://perma.cc/9ATN-QEP2.

[7] *See* Bill Kleyman, *What Personal Cloud Means for Consumers and Enterprises*, DATA CENTER KNOWLEDGE (Sept. 10, 2013), http://www.datacenterknowledge.com/archives/2013/09/10/what-personal-cloud-means-for-consumers-and-enterprises/, *archived at* https://perma.cc/RK2Z-VE6L.

[8] *See* Louis Columbus, *How Enterprises Are Capitalizing on the Consumerization of IT*, FORBES (Mar. 24, 2014, 06:43 AM), http://www.forbes.com/sites/louiscolumbus/2014/03/24/how-enterprises-are-capitalizing-on-the-consumerization-of-it/#1af595ef6160, *archived at* https://perma.cc/38F9-KTQ6 ("79% [of surveyed enterprises] report that file sharing and collaboration tools including Box, Egnyte, Google Apps, Microsoft Office 365, GroupLogic, ShareFile and others are pervasively used today. 49% are with IT approval and 30% are not.").

[9] *See* Andrew Froehlich, *The Buck Stops at BYOC*, INFORMATIONWEEK (Jan. 29, 2014, 12:00 PM), http://www.networkcomputing.com/infrastructure/buck-stops-byoc/870595087, *archived at* https://perma.cc/K7BV-HPPL ("Employees are comfortable using services such as DropBox, Google Apps, and Carbonite at home. Because of that comfort level, they naturally want to use those same tools in their

could benefit from such functionality, it is particularly advantageous to workers whose employers lag behind the technology curve.[10]

[4] These and other features seem to make personal clouds an ideal tool for advancing business objectives within the corporate environment.[11] Appearances, however, can be deceiving. That is exactly the case with employee use of personal cloud applications in the workplace.[12] From information retention and information security to litigation readiness and cybersecurity, personal cloud use among employees implicates a range of troubles for organizations.[13] Indeed, the very aspects that make personal clouds so attractive–cheap and unlimited storage, simplified transfers, and increased collaboration–pose serious threats to the enterprise.[14]

---

business life."); Intermarine, L.L.C. v. Spliethoff Bevrachtingskantoor, B.V., No. 15-mc-80211-MEJ, 2015 U.S. Dist. LEXIS 112689, at *2 (N.D. Cal. Aug. 20, 2015) ("Dropbox provides a document storage and sharing service through which users can collectively save, share, and edit documents stored 'in the cloud.'").

[10] *See* Froehlich, *supra* note 9.

[11] *See id.* ("Lack of IT management and control will quickly put an end to BYOC, even though it has the potential to provide real benefits.").

[12] *See* Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915, at *22–24, *29 (E.D. Tex. Nov. 30, 2015) (discussing defendants' extensive use of Dropbox to remove vast amounts of proprietary information belonging to plaintiff).

[13] *See* Susan Miller, *New Risk on the Block: Bring Your Own Cloud*, GCN (May 23, 2013) https://gcn.com/articles/2013/05/23/new-risk-bring-your-own-cloud.aspx, *archived at* https://perma.cc/T7DM-3CD6.

[14] *See* Robert L. Mitchell, *IT's New Concern: The Personal Cloud*, COMPUTERWORLD (May 20, 2013, 7:00 AM), http://www.computerworld.com/article/2497860/consumerization/it-s-new-concern--the-personal-cloud.html, *archived at* https://perma.cc/XZN9-RSK8.

[5] Nevertheless, companies in many instances have taken few, if any, actionable steps to address the proliferation of personal cloud use among their employees.[15] Worse, some organizations have implemented "bring your own cloud" (BYOC) policies that officially sanction employee use of consumer-grade cloud applications in the workplace without sufficient corporate oversight.[16] A BYOC policy that lacks proper measures to ensure compliance may very well result in a disastrous outcome for the enterprise.[17]

[6] In this article, I address these issues by surveying recent court cases that exemplify the information governance and litigation challenges arising from personal cloud use in the business enterprise. In particular, I discuss the problems with BYOC practices that expressly or implicitly enable employee use of personal clouds. I also spotlight some of the troubles that stealth use of personal clouds creates for organizations. I conclude by suggesting some practices that can help organizations ameliorate these problems.

## II. LAISSEZ-FAIRE TREATMENT OF PERSONAL CLOUD USE IN THE CORPORATE ENVIRONMENT

[7] Employers are often directly responsible for the difficulties that have resulted from employee use of cloud applications.[18] That employers are at fault does not stem from this being a new trend. Indeed, personal cloud providers have been around since the 2000s,[19] with courts

[15] *See* discussion *infra* Part II.

[16] *See* Froehlich, *supra* note 9.

[17] *See id.* ("BYOC presents a nightmare scenario because data can be copied, duplicated, and ultimately lost or stolen via the various cloud services.").

[18] *See* Columbus, *supra* note 8.

[19] *See* Victoria Barret, *Dropbox: The Inside Story of Tech's Hottest Startup*, FORBES (Oct. 18, 2011, 8:30 AM), http://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/4/#1cace6c73a44, *archived at* http://perma.cc/C9Q3-

examining the troubles associated with cloud computing beginning in 2011.[20] Organizations previously overlooked the risks of this trend by authorizing their executives or employees to use personal cloud applications in the corporate ecosystem.[21] In addition, they ignored the hazards associated with the stealth use of personal clouds.[22] This Part examines cases that address these aspects of employee use of consumer clouds.

### A. Corporate Approved BYOC Accounts

[8] In many instances, organizations have openly welcomed the use of personal clouds by their employees.[23] Whether by policy or by practice, corporate IT departments have approved personal cloud use by expressly enabling its functionality.[24] Nevertheless, that is often the extent of corporate oversight.[25] Beyond requiring an employee to sign a perfunctory

465F; Jonathan Strickland, *How Cloud Storage Works*, HOWSTUFFWORKS.COM (Apr. 30, 2008), http://computer.howstuffworks.com/cloud-computing/cloud-storage2.htm, *archived at* https://perma.cc/5JTG-UZS3 (Web-based e-mail providers like Yahoo! and Hotmail have been providing their users with a quasi-cloud computing environment through e-mail since the 1990s).

[20] *See, e.g.*, Animators at Law, Inc. v. Capital Legal Solutions, L.L.C., 786 F. Supp. 2d 1114, 1117–18 (E.D. Va. 2011) (explaining that plaintiff's former employees accessed company files stored in a company Dropbox account through login credentials that plaintiff failed to disable after the employees left the company).

[21] *See* Columbus, *supra* note 8.

[22] *See* Boston Scientific Corp. v. Lee, No. 13-13156-DJC, 2014 U.S. Dist. LEXIS 66220, at *2, *4–7 (D. Mass. May 14, 2014) (enjoining defendant from using proprietary information that he had taken from his prior employer and which he stored both during and after his employment on Google Drive).

[23] *See* Selectica, Inc. v. Novatus, Inc., No. 6:13-cv-1708-Orl-40TBS, 2015 U.S. Dist. LEXIS 30460, at *2 (M.D. Fla. Mar. 12, 2015).

[24] *See* Columbus, *supra* note 8.

[25] *See* Froehlich, *supra* note 9.

non-disclosure agreement, little follow up effort is taken to prevent employees from transferring confidential information from company servers to a personal cloud.[26]

[9] Such corporate inaction can be challenging for cybersecurity initiatives, retention schedules, and preservation requirements in litigation. However, it can be especially problematic when an employee leaves the company with proprietary materials and begins working for an industry competitor.[27] The *Selectica v. Novatus*[28] and *PrimePay v. Barnes*[29] decisions are particularly instructive on the need for organizations to abandon their laissez-faire attitude toward employee use of approved BYOC accounts.

### 1. *Selectica v. Novatus*

[10] In *Selectica*, plaintiff (Selectica) filed suit against defendant (Novatus), claiming Novatus misappropriated various trade secrets.[30] In particular, Selectica alleged that four of its former sales personnel violated their respective non-disclosure agreements by sharing confidential pricing

[26] *See* Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915, at *7–9 (observing that defendants' former employer began investigating the possibility that defendants took proprietary company data in violation of their non-disclosure agreements only after one of the defendants mentioned that "she knew where too many bodies were buried.").

[27] *See* Toyota Indus. Equip. Mfg. v. Land, No. 1:14-cv-1049-JMS-TAB, 2014 U.S. Dist. LEXIS 99070, at *5–6, *9 (S.D. Ind. July 21, 2014) (explaining that defendant uploaded confidential information from his former employer to his Google Drive account before going to work for an industry competitor).

[28] *See* Selectica, Inc. v. Novatus, Inc., No. 6:13-cv-1708-Orl-40TBS, 2015 U.S. Dist. LEXIS 30460 (M.D. Fla. Mar. 12, 2015).

[29] *See* PrimePay, L.L.C. v. Barnes, No. 14-11838, 2015 U.S. Dist. LEXIS 65710 (E.D. Mich. May 20, 2015).

[30] *See Selectica, Inc.*, 2015 U.S. Dist. LEXIS 30460, at *4.

information with Novatus, their new employer.[31] Those agreements provided that the employees would maintain the confidentiality of Selectica's proprietary information and return all such materials to the company upon termination of their employment.[32]

[11] Despite those agreements, one of the employees (Holt) offered to share Selectica's pricing information to a member of Novatus' senior management team after joining Novatus.[33] Holt still had access to that information along with other data belonging to Selectica because he maintained it with Box, a cloud storage provider.[34] The Box account was not a stealth cloud drive concealed from Selectica.[35]

[12] Instead, Selectica expressly recommended and authorized Holt to store that data under a BYOC arrangement with Box: "While employed by Selectica, [Holt] had a company laptop computer which, *on Selectica's recommendation*, was configured so that it automatically synced to his personal cloud storage account at Box.com. This meant that when Holt saved a file to the laptop, the system pushed a copy to his Box account."[36] Despite having enabled the BYOC arrangement with Holt, Selectica apparently neglected to disable the Box account or remove any proprietary materials upon Holt's departure.[37] As a result, Holt had full access to the pricing information when he joined Novatus.[38]

---

[31] *See id.* at *2.

[32] *See id.* at *1.

[33] *See id.* at *3.

[34] *See id.*

[35] *See Selectica, Inc.*, 2015 U.S. Dist. LEXIS 30460, at *2–3.

[36] *Id.* at *2 (emphasis added).

[37] *See id.* at *2.

[38] *See id.* at *2–3.

[13] *Selectica* demonstrates the folly of a lax approach to personal cloud use within the enterprise. While Selectica enabled the Box account for backup purposes, it took no action to protect Selectica's interest in the corporate information stored in that account. For example, Selectica did not obtain Holt's login credentials to the Box account.[39] Nor does it appear that Selectica monitored Holt's use of the account while employed with the company.[40] Selectica did not disable the Box account when Holt left the company.[41] Furthermore, Selectica took no action to confirm that Holt had either returned or destroyed all proprietary company information before going to work for Novatus.[42]

[14] Any one of these steps—and certainly a combination of them—would likely have prevented the disclosure of Selectica's product pricing information to an industry competitor.[43] *Selectica* exemplifies the need for corporate oversight of approved BYOC accounts if organizations are to prevent their trade secrets from falling into the hands of competitors.

### *2. PrimePay v. Barnes*

[15] Another exemplary decision on these issues is *PrimePay v. Barnes*.[44] Like *Selectica*, *PrimePay* involves claims of trade secret misappropriation.[45] In *PrimePay*, the plaintiff (PrimePay) sued one of its

[39] *See id.* at *17.

[40] *See Selectica, Inc.*, 2015 U.S. Dist LEXIS 30460, at *2–3.

[41] *See id.*

[42] *See id.*

[43] *See* Tom Nolle, *Bring Your Own Cloud: The Movement Companies Can't and Shouldn't Stop*, TECHTARGET (Apr. 8, 2014), http://searchcloudapplications.techtarget.com/feature/Bring-your-own-cloud-The-movement-companies-cant-and-shouldnt-stop, *archived at* https://perma.cc/C478-7NCG.

[44] *See* PrimePay, L.L.C. v. Barnes, No. 14-11838, 2015 U.S. Dist. LEXIS 65710 (E.D. Mich. May 20, 2015).

former executives (Barnes) that established a competing business entity.[46] PrimePay moved for a preliminary injunction against the operation of Barnes' business, arguing that Barnes took several categories of confidential PrimePay information and stored it with cloud service provider Dropbox, along with other locations.[47] According to PrimePay, Barnes accessed the Dropbox-stored data to allegedly help start his competing company. He then allegedly destroyed those materials after the plaintiff warned him "to preserve any PrimePay electronically stored information that he possessed."[48]

[16] In response to these arguments, Barnes asserted that he never absconded with PrimePay's proprietary data.[49] Instead, Barnes explained that any PrimePay data in his Dropbox account was from work that he previously performed while at PrimePay.[50] According to Barnes, that data was mostly deleted at the time he left the company.[51] As for the origin of the Dropbox account, it was created far in advance of Barnes' departure from the company.[52] Its purpose was not to steal proprietary data, Barnes argued, but to allow him to complete work for PrimePay when he was away from the office.[53] Nor was this a stealth account; it was a company-approved BYOC:

---

[45] *See id.* at *2.

[46] *See id.* at *4–5.

[47] *See id.* at *2, *9–11.

[48] *Id.* at *8–9.

[49] *See PrimePay, L.L.C.*, 2015 U.S. Dist. LEXIS 65710, at *3.

[50] *See id.* at *11–13.

[51] *See id.* at *12.

[52] *See id.* at *11.

[53] *See id.*

> Barnes created the Dropbox [account] . . . so that he could transfer and access files when he worked remotely on PrimePay matters if he was away from the office, on vacation or elsewhere and needed access to the PrimePay files, all with the knowledge and approval of [PrimePay owner] Chris Tobin.[54]

[17] Given that Barnes' Dropbox account was a company-approved BYOC account, and in light of other evidence suggesting Barnes did not access the Dropbox files or other proprietary PrimePay information after leaving his position with the company, the court did not find evidence of trade secret misappropriation.[55] While the court ordered the destruction of PrimePay's remaining confidential information stored on the Dropbox, it refused to issue a preliminary injunction against the operation of Barnes' competing enterprise.[56]

[18] *PrimePay* reinforces the lesson from *Selectica* that a laissez-faire approach to personal clouds may lead to corporate disasters. Because PrimePay did not monitor or disable the Dropbox account, Barnes apparently left the company with a massive trove of proprietary company data. Even though the court accepted Barnes' explanation that he accessed little, if any, of that data after he left the company, PrimePay's evidence suggested otherwise.[57] While PrimePay may never know how much of its information was used to start Barnes' competing enterprise, it is reasonably certain that a more robust compliance program would have quarantined the proprietary data before Barnes left the company.[58] This may have obviated the legal expenses and opportunity costs of the litigation. Like *Selectica*, *PrimePay* ultimately teaches that organizations

[54] *PrimePay, L.L.C.*, 2015 U.S. Dist. LEXIS 65710, at *11.

[55] *See id.* at *64, 66.

[56] *See id.* at *106–08.

[57] *See id.* at *34–36, *100–01.

[58] *See* Lee, *supra* note 5.

should police approved BYOC environments to better safeguard proprietary corporate information.

### B. Stealth Use of Personal Clouds

[19] Beyond the problem of a poorly monitored BYOC ecosystem stands the equally troubling scenario of stealth use of personal clouds.[59] Such a scenario involves employees using their personal cloud accounts in connection with their work duties without express company approval.[60] While some employees do so in good faith to facilitate their work, others clandestinely use their cloud accounts to sabotage the organization or to gain a competitive advantage over their former employers after leaving the company.[61] A number of decisions demonstrate the problems with stealth—or "shadow"—use of personal clouds across the spectrum of corporate employees.[62]

#### 1. Operations-Level Employee

[20] Operations-level employees are often at the heart of stealth use of personal clouds. For example, in *Toyota Industrial Equipment Manufacturing v. Land*, a managerial level employee (Land) used Google Drive and other personal cloud applications to steal hundreds of critical

---

[59] *See* Danny Palmer, *CIOs Worried Cloud Computing and Shadow IT Creating Security Risks*, COMPUTING (July 27, 2015), http://www.computing.co.uk/ctg/news/2419409/cios-worried-cloud-computing-and-shadow-it-creating-security-risks, *archived at* https://perma.cc/39AR-LJ4F.

[60] *See* Thoran Rodrigues, *Cloud Computing and the Dangers of Shadow IT*, TECHREPUBLIC (Aug. 16, 2013, 12:48 PM), http://www.techrepublic.com/blog/the-enterprise-cloud/cloud-computing-and-the-dangers-of-shadow-it/, *archived at* https://perma.cc/Y5BG-PEQZ.

[61] *See, e.g.*, Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915, at *3–4, *8–9 (E.D. Tex. Nov. 30, 2015); Toyota Indus. Equip. Mfg. v. Land, No. 1:14-cv-1049-JMS-TAB, 2014 U.S. Dist. LEXIS 99070, at *10, *13–14 (S.D. Ind. July 21, 2014).

[62] *See* Rodrigues, *supra* note 60.

documents from his employer (Toyota) before going to work for an industry competitor.[63] Those documents included technical specifications reflecting the proprietary design of certain industrial equipment, along with related pricing and financial information.[64] While authorized to use that data during his employment, Land stored and kept shadow copies of these materials on his Google Drive account so they could be accessible after he left Toyota.[65]

[21] To facilitate the removal of Toyota's proprietary information, Land downloaded "GoogleDriveSync.exe" on his work computer.[66] Similar to the corporate-enabled Box account in *Selectica*, the GoogleDriveSync.exe program enabled Land to simultaneously save documents on his personal Google Drive account that he saved to his company-issued computer.[67] On the eve of his departure from Toyota, Land placed approximately 800 "files and folders" on Google Drive.[68] These actions—Land removing and then retaining Toyota's proprietary information after his departure from the company in violation of his non-disclosure agreement—resulted in an injunction preventing Land from working for Toyota's competitor.[69]

[22] Another case involving stealth cloud use by an operations-level employee is *RLI Insurance Company v. Banks*.[70] In *RLI*, the employee (Banks) used a Norwegian cloud provider (Jottacloud)[71] to upload "757

[63] *See Toyota Indus. Equip. Mfg., Inc.*, 2014 U.S. Dist. LEXIS 99070, at *3–7.

[64] *See id.* at *5.

[65] *See id.* at *5–7.

[66] *See id.* at *6–8.

[67] *See id.* at *6–7.

[68] *See Toyota Indus. Equip. Mfg., Inc.*, 2014 U.S. Dist. LEXIS 99070, at *8.

[69] *See id.* at *15–16, *22.

[70] *See* RLI Ins. Co. v. Banks, No. 1:14-CV-1108-TWT, 2015 U.S. Dist. LEXIS 9396, (N.D. Ga. Jan. 27, 2015).

customer claim files and other files containing proprietary information" belonging to her employer (RLI).[72] Banks initially tried to upload the files to her Dropbox account, but RLI's corporate network denied access to Dropbox.[73] RLI had employed a web filtering software blocking employees from accessing more commonly used cloud providers, such as Dropbox.[74] Undeterred, Banks researched "Dropbox alternatives" that could evade RLI's filtering protocol, opened a Jottacloud account, and used that service to remove proprietary RLI data in violation of her employment agreement.[75] RLI eventually discovered Banks' malfeasance, but only after offering her a severance package subsequent to her dismissal from the company.[76]

### 2. Company Executives

[23] Operations-level employees are not alone in their furtive use of personal clouds. Company executives can also be guilty of such conduct. Given the nature of access that executives often have to critical information, such conduct can be particularly problematic. The *Frisco*

[71] *See id* at *2; *see generally* JOTTACLOUD, https://www.jottacloud.com, *archived at* https://perma.cc/7HQJ-AYFR (last visited Mar. 17, 2016) ("Jottacloud is a cloud storage service for individuals and companies that lets you backup, synchronize, store and share files from all your devices. The uploaded data is protected by one of the worlds [sic] strongest privacy laws, with all your data stored in Norway.").

[72] *RLI Ins. Co.*, 2015 U.S. Dist. LEXIS 9396, at *2.

[73] *See id.*

[74] *See id.* at *1–2.

[75] *Id.* at *2.

[76] *See* Verified Complaint for Damages and Emergency Injunctive Relief at 15–16, RLI Ins. Co. v. Banks, 2015 U.S. Dist. LEXIS 9396 (N.D. Ga. Jan. 27, 2015) (No. 1:14-CV-1108-TWT) ("Not aware of Defendant's misappropriation of RLI's Customer Claim Files and Proprietary Information, RLI offered Defendant a severance package upon her termination. Defendant had not yet accepted the offer of a severance package when RLI discovered the misappropriation. Based on Defendant's misconduct, RLI revoked its offer of severance to Defendant by letter to Defendant.").

*Medical Center v. Bledsoe*[77] and *De Simone v. VSL Pharmaceuticals*[78] cases are instructive in this particular scenario.

[24] In *Frisco Medical*, the chief operating officer (Bledsoe) for a Texas hospital (Frisco) used Dropbox to obtain several classes of proprietary and patient information before leaving Frisco for a new position elsewhere.[79] More specifically, Bledsoe installed Dropbox on her work computer *after* she accepted her new position but *before* she resigned from Frisco.[80] With Dropbox enabled, Bledsoe then transferred "Frisco's confidential and proprietary information, trade secrets, peer review materials, and statutorily protected patient health information to her personal" cloud account in violation of her employment agreements.[81]

[25] Frisco did not suspect that Bledsoe surreptitiously removed proprietary information from its computer network until she revealed in an exit interview that "she knew where too many bodies were buried."[82] It was only then that Frisco began investigating Bledsoe's computer usage, discovered her use of Dropbox, and determined the extent of the information she had taken from the hospital.[83]

[26] In contrast to *Frisco Medical*, *De Simone v. VSL Pharmaceuticals* involved a chief executive officer (De Simone) who used Dropbox to

---

[77] *See* Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915 (E.D. Tex. Nov. 30, 2015).

[78] *See* De Simone v. VSL Pharm., Inc., No. TDC-15-1356, 2015 U.S. Dist. LEXIS 128209, at *2 (D. Md. Sept. 23, 2015).

[79] *See Frisco Med. Ctr., L.L.P.*, 2015 U.S. Dist. LEXIS 159915, at *8.

[80] *See id.* at *12.

[81] *Id.* at *11.

[82] *Id.* at *7.

[83] *See id.* at *7–9.

deprive his company (VSL) of corporate records.[84] De Simone, who served as VSL's chief executive for more than a decade, became embroiled in a dispute with investors over who rightfully owned VSL's intellectual property related to the probiotic drug sold by the company.[85] In connection with that dispute, De Simone transferred VSL's corporate records to his personal Dropbox account.[86] He then wiped the corporate network in order to eliminate any trace of the records and rejected shareholder requests to access the information.[87] After resigning his position as VSL's CEO a few months later, De Simone began working for a competitive enterprise that manufactured and sold a generic version of VSL's probiotic drug, taking the corporate records with him.[88]

### 3. Analysis of Cloud Jurisprudence

[27] The cases discussed so far generally involve harm to employers that likely could have been obviated had the organizations taken safeguards to prevent or detect stealth use of personal clouds.[89] Instead, like *Selectica*, the employers in *Toyota Industrial*, *RLI*, and *Frisco Medical* relied on non-disclosure and other employment agreements to protect their sensitive and proprietary information.[90]

---

[84] *See* De Simone v. VSL Pharm., Inc., No. TDC-15-1356, 2015 U.S. Dist. LEXIS 128209, at *48 (D. Md. Sept. 23, 2015).

[85] *See id.* at *1–2.

[86] *See id.* at *48–49.

[87] *See id.* at *18.

[88] *See id.* at *2.

[89] *See* discussion *infra* Part III.

[90] *See* Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915, at *3 (E.D. Tex. Nov. 30, 2015); RLI Ins. Co. v. Banks, No. 1:14-CV-1108-TWT, 2015 U.S. Dist. LEXIS 9396, at *2, *6 (N.D. Ga. Jan. 27, 2015); Toyota Indus. Equip. Mfg. v. Land, No. 1:14-cv-1049-JMS-TAB, 2014 U.S. Dist. LEXIS 99070, at *4–6 (S.D. Ind. July 21, 2014).

[28] On the one hand, those agreements successfully enabled the aggrieved parties to obtain injunctions, summary judgment orders, and damages against the cloud-wielding tortfeasors.[91] But at what cost? The employers incurred legal fees and costs for the investigations and court actions they undertook to address the theft of corporate information by their former employees. In addition to those expenses, the organizations sustained substantial opportunity costs. Personnel were likely redirected from business operations to ameliorate the harm caused by the loss of proprietary data. Moreover, industry competitors may have become acquainted with strategic plans, pricing information, design specifications, financial performance, and other proprietary data. All of this may have provided their competitors with an advantage in subsequent business dealings.[92]

[29] Simply put, the non-disclosure and employment agreements did nothing to stop the perpetrating employees from misappropriating company trade secrets.[93] Beyond the agreements, the only employer that apparently took anything close to a preventative step was RLI, which used a blocking program to prevent personal cloud use.[94] However, even that step proved inadequate as the employee easily circumvented the software filter by using a previously unknown cloud application.[95]

---

[91] *See Frisco Med. Ctr., L.L.P.*, 2015 U.S. Dist. LEXIS 159915, at *40–41 (granting Frisco summary judgment against Bledsoe on its trade secret claims); *Toyota Indus. Equip. Mfg., Inc.*, 2014 U.S. Dist. LEXIS 99070, at *21–22 (enjoining Land from working for his new employer).

[92] *See Frisco Med. Ctr., L.L.P.*, 2015 U.S. Dist. LEXIS 159915, at *2 (stating that beyond the problems with industry competitors, such unauthorized disclosures could violate regulatory schemes such as the Health Insurance Portability and Accountability Act, or HIPAA).

[93] *See* David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 WASH. & LEE L. REV. 323, 334–35 (2015) (observing that many companies prefer to litigate rather than protect their trade secrets).

[94] *See RLI Ins. Co.*, 2015 U.S. Dist. LEXIS 9396, at *1–2.

[95] *See id.* at *2.

[30] Just as in *Prime Pay*, none of the employers appears to have established a process to detect the possible use of personal cloud applications. This is evident from *De Simone*, as the company did not know that its chief executive used Dropbox to steal its corporate records.[96] That no such process was in place in *RLI* is confirmed by the company's initial offering of severance pay to Banks.[97] The *Frisco* employer only began its search of Bledsoe's computer activity after she carelessly suggested she knew where the "bodies were buried."[98] In *Toyota Industrial*, no efforts were made either to examine Land's computer activity or to verify his next work destination after he tendered his resignation.[99] Indeed, Toyota allowed Land to work for another two weeks at the company before his termination date.[100]

[31] With employees now regularly using consumer clouds in connection with their work responsibilities, organizations must be prepared to counteract their potential negative effects. As set forth in Part III, companies should develop proactive measures to address employee use of cloud applications and to mitigate any resulting harm.

## III. PROACTIVE STEPS TO ADDRESS PERSONAL CLOUD USE

[32] Despite the complexities that personal clouds now present for many organizations, they are not insurmountable. Enterprises can generally manage potential problems through a proactive, common sense

[96] *See* De Simone v. VSL Pharm., Inc., No. TDC-15-1356, 2015 U.S. Dist. LEXIS 128209, at *48 (D. Md. Sept. 23, 2015).

[97] *See* Verified Complaint for Damages and Emergency Injunctive Relief at 15–16, RLI Ins. Co. v. Banks, 2015 U.S. Dist. LEXIS 9396 (N.D. Ga. Jan. 27, 2015) (No. 1:14-CV-1108-TWT).

[98] Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915, at *7 (E.D. Tex. Nov. 30, 2015).

[99] *See* Toyota Indus. Equip. Mfg. v. Land, No. 1:14-cv-1049-JMS-TAB, 2014 U.S. Dist. LEXIS 99070, at *6 (S.D. Ind. July 21, 2014).

[100] *See id.*

approach to information governance. In this Part, I discuss some of the key aspects of an information governance program that can help address the challenges associated with employee use of personal cloud applications.

[33] A prefatory step that organizations can take in this regard is to create a data map identifying the locations—both on and off the corporate network—where their information resides.[101] While a data map is useful for both information retention and litigation purposes, it is essential for controlling ingress and egress to proprietary information—precisely the data endangered by personal cloud applications.[102] If a company cannot identify the precise areas where it has stored its trade secrets and other sensitive materials, it becomes difficult to establish that it used "reasonable steps" to safeguard that information.[103] In contrast, a current and accurate data map better enables organizations to reasonably account for proprietary records, along with other indispensable business

[101] *See* David Wetmore & Scott Clary, *To Map or Not to Map: Strategies for Classifying Sources of ESI*, INFORMATION MANAGEMENT (2009), http://content.arma.org/IMM/SeptOct2009/to_map_or_not_to_map.aspx, *archived at* https://perma.cc/CG8S-VACB.

[102] *See* R. Mark Halligan, *Protecting U.S. Trade Secret Assets in the 21st Century*, 6 LANDSLIDE, No. 1, Sept.–Oct. 2013, at 4, http://www.americanbar.org/publications/landslide/2013-14/september-october-2013/protecting_us_trade_secret_assets_the_21st_century.html, *archived at* https://perma.cc/FU3T-L4FW (urging companies to adopt "mapping" approaches to better safeguard trade secrets); *see also* Sterling Miller, *Ten Things: Trade Secrets and Protecting Your Company*, CORPORATE LAW ADVISORY (Apr. 27, 2015), http://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2015/04/27/ten-things-trade-secrets-and-protecting-your-company.aspx, *archived at* https://perma.cc/XH3L-WXRQ [hereinafter Miller] ("You need an inventory of all of the company's trade secrets . . . [a]n inventory helps you identify what steps are needed to keep those specific items confidential and protected and be clear with the business what items are not considered trade secrets . . .").

[103] *See* Boston Scientific Corp. v. Lee, No. 13-13156-DJC, 2014 U.S. Dist. LEXIS 66220, at *10, *12–13 (D. Mass. May 14, 2014) (finding the employer used "reasonable means to protect its trade secrets" despite contradictory evidence suggesting an employee openly used a personal Google Drive account to access and store confidential company information).

information.[104] Once the data map is in place, organizations can then proceed to develop policies that reasonably ensure the protection of corporate data.[105]

[34] Those policies should include actionable protocols that address employee use of personal cloud applications.[106] Those protocols should clearly delineate whether personal clouds are permitted and if so, what constitutes an authorized BYOC account.[107] Whether an enterprise chooses to ban the use of personal clouds or to adopt a BYOC-friendly environment, the policy should include audit and enforcement mechanisms to gauge policy observance.[108] At a minimum, those mechanisms ought to include the right to monitor, access, and disable employee use of personal clouds.[109] Related mechanisms will also be required for those organizations that proscribe BYOC use since employees

[104] *See* Halligan, *supra* note 102, at 4.

[105] *See*, *e.g.*, Philip J. Favro, *Getting Serious: Why Companies Must Adopt Information Governance Measures to Prepare for the Upcoming Changes to the Federal Rules of Civil Procedure*, 20 RICH. J.L. & TECH. 5, 25–35 (2014), http://jolt.richmond.edu/v20i2/article5.pdf, *archived at* https://perma.cc/SZ3M-3MNP (explaining that a comprehensive information governance plan would take various factors into consideration. They would likely include the length of pertinent retention periods, the ability to preserve data for legal matters, applicable data protection laws, cybersecurity initiatives, and use policies for smartphones and other mobile devices).

[106] *See* Philip Favro, *Do You Know Your BYOCs?*, LEGAL TECH. NEWS (July 13, 2015), http://www.legaltechnews.com/id=1202731897715?keywords=favro&publication=Legal+Technology, *archived at* https://perma.cc/QF6S-8KVW.

[107] *See* Miller, *supra* note 102.

[108] *See* Sophie Vanhegan, *Legal Guidance: Protecting Company Information in the Cloud-Era*, HRZONE (Apr. 23, 2013), http://www.hrzone.com/perform/business/legal-guidance-protecting-company-information-in-the-cloud-era, *archived at* https://perma.cc/8MGT-3QZG.

[109] *See id.* (observing that corporate policies must "allow company monitoring of employees' IT activity and work email accounts . . .").

will likely circumvent such a policy.[110] For example, blocking programs like the one used in *RLI*, while not foolproof, are a practicable first step to preventing some personal cloud use.[111]

[35] In a BYOC ecosystem, applicable protocols should additionally describe what company data can or cannot be transferred to the cloud.[112] Organizations should also require the disclosure of user login credentials for approved cloud applications to ensure appropriate policy compliance.[113] Upon an employee's termination, approved BYOC accounts should either be disabled or the company should verify that company data previously maintained in the account has been either returned or destroyed.[114]

[36] In like manner, non-BYOC organizations should consider examining terminated employees' computer activity and corporate devices to detect whether there was illicit use of personal clouds.[115] However, such a step may not be practicable for many organizations that lack the

---

[110] *See id.* ("Employers may also wish to consider . . . implementing IT measures to prohibit uploading of documents onto web-based applications."); *see also* RLI Ins. Co. v. Banks, No. 1:14-CV-1108-TWT, 2015 U.S. Dist. LEXIS 9396, at *2 (N.D. Ga. Jan. 27, 2015).

[111] *See, e.g.*, *RLI Ins. Co.*, 2015 U.S. Dist. LEXIS 9396, at *1–2.

[112] *See* Vanhegan, *supra* note 108 (explaining that policies addressing personal cloud usage should "expressly prohibit the removal of company documents and information outside the company's systems.").

[113] *See* Esther Schindler, *Protecting Corporate Data... When an Employee Leaves*, DRUVA BLOG (Oct. 13, 2014), http://www.druva.com/blog/protecting-corporate-data-employee-leaves/, *archived at* https://perma.cc/4GS5-QJ9H.

[114] *See* Rachel Holdgrafer, *Fix Insider Threat with Data Loss Prevention*, CLOUD SECURITY ALLIANCE (Dec. 10, 2015), https://blog.cloudsecurityalliance.org/2015/12/10/fix-insider-threat-with-data-loss-prevention/, *archived at* https://perma.cc/EU5U-2FZN.

[115] *See* Miller, *supra* note 102 ("Departing employees constitute one of your biggest risks for trade-secret theft.").

resources for a thorough review of every employee device. If a comprehensive sweep is cost prohibitive, organizations should consider conducting a review of those employees whose possible disclosure of corporate information carries the greatest risk to the enterprise.[116] The extent to which a company carries out this step likely depends on the role of the terminated employees, their position in the company, and the nature of the information to which they were privy.[117] Despite the expense of this procedure, such a step would likely have obviated much of the litigation that ensued in *Selectica*, *Novatus*, *Toyota Industrial*, *RLI*, and *Frisco Medical*.

## IV. CONCLUSION

[37] The challenges with personal cloud applications need not be an intractable problem. Following industry best practices like those suggested in Part III should help organizations address many of the troubles associated with approved BYOC accounts. They should also mitigate the harm created by stealth cloud use that may go undetected. While certainly not an elixir, adopting these practices should help companies avoid many of the worst problems associated with personal cloud use in the enterprise.

[116] *See id.*

[117] *See id.*; *see also* Frisco Med. Ctr., L.L.P. v. Bledsoe, No. 4:12-CV-37; 4:15cv105, 2015 U.S. Dist. LEXIS 159915, at *5 (E.D. Tex. Nov. 30, 2015).