To BYOC or not BYOC? An Analysis of *PrimePay v. Barnes*

Information governance (IG) can be a lot like air. When everything is functioning properly, it is invisible and practically unnoticeable. But if something in the mixture is off, or worse, it is absent, the ramifications can be dire. Poor information control creates situations where important, confidential documents and other data can be lost or stolen due to accidents or the actions of bad actors. This scenario can be seen playing out in the 2015 Michigan case of *PrimePay, LLC v. Barnes et al*., an analysis of which reveals preventable gaps in the company's IG program and the issues that arose from them.

Background

PrimePay is a business support company offering services that include payroll, timekeeping, benefits administration, compliance, and human resources support ("About PrimePay"). Richard Barnes ran one of several independently-owned companies operating under the PrimePay name that were bought and folded into the company following a corporate reorganization in December 2013 (Borman 3). Barnes had worked for PrimePay for more than 15 years, but the consolidation meant his salary would be slashed from $210,000 to $80,000 per year ("IP Law Tracker"). He quit the following March, informing the company during his exit interview that he planned to set up a competing firm as there was no non-compete agreement in effect (Borman 3). That company, HighPoint Business Services, operates out of Clarkston, Michigan (HighPoint Payroll).

PrimePay sent a cease-and-desist letter to Barnes in April 2014 demanding "the return of a PrimePay laptop and files, including PrimePayQuickBooks files, that contained highly confidential client and employee-personnel related information that was stored on the laptop that Barnes used" (Borman 6). A forensic inspection of a laptop Barnes took with him from PrimePay, other computers in use at HighPoint, and a personal Dropbox account revealed several PrimePay files, as well as the deletion of files containing information such as sales contacts and financial data (6). At the time of Barnes' employment, Dropbox was a company-approved cloud service ("Personal Clouds" 14). Barnes said that the computer was his as he had purchased it from the owner of the PrimePay franchise before consolidation. He further stated the Dropbox account was set up to allow him to work even when away from the office, and the deleted files were ones he had used while employed with PrimePay. He maintained that he started working on

his own firm when he realized he could not afford to stay with PrimePay, that he "only worked on these plans on his own time and never used PrimePay information or documents in planning for, launching or operating HighPoint," and that he "undertook to delete all PrimePaymaterial from his laptop and in the Dropbox and confirmed that back up of all these files remained on the PrimePay server" (Borman 7). John Allen, PrimePay's vice president of information security and governance, said that the laptop was not the franchise owner's to sell (23), and court documents note that "much of the information retained on Barnes's laptop was PrimePay's confidential business information and even Barnes agrees that he should not have retained such information on his laptop as he set off to establishing [sic] a competing business" (40). PrimePay ultimately filed a lawsuit against Barnes alleging "misappropriation of trade secrets under the Michigan Uniform Trade Secrets Act…based on his retention of confidential computer files containing PrimePay accounting and customer information" ("IP Law Tracker"). The company said he used the information from PrimePay to help start his company before deleting the files (Favro 9). Barnes responded that nothing in his possession constituted trade secrets and that he had not "solicited any of Plaintiff's customers or used any of Plaintiff's proprietary information" (Borman 2). In its lawsuit, PrimePay sought an injunction to shut Barnes' new company down and bar him from the industry nationwide (43).

The court ruled that Barnes could not use or destroy any documents or information he obtained from PrimePay and had to allow the company time and opportunity to inspect and remove its files from his computers and cloud storage. In addition, he was ordered to return the digital assets along with any access information he still might have (Borman 66-67). The injunction was denied, however, as the court said PrimePay fell short "of explaining with any degree of clarity how this information, given this particular industry, has competitive value from not being generally known to every other payroll services company or how this type of information could be used by a competitor to steal customers" (42). The claim of trade secret misappropriation, the judge said, did not mesh with the fact that the company did not require any sort of non-compete agreement while Barnes was employed ("IP Law Tracker"), and evidence presented actually indicated that he never accessed the PrimePay files in his Dropbox account after leaving the company ("Personal Clouds" 14).

IG Issues

It should be noted that PrimePay argued that it took reasonable precautions to prevent the loss of information, including: a mandatory non-disclosure and proprietary information confidentiality agreement for all sales staff, a binding corporate privacy policy for all employees, password protection measures, storing confidential information in on a restricted server limited to need-to-know access, electronic pass keys to gain access to company headquarters, advanced firewalls, data encryption, and the use of continuous video monitoring. The company also alleged that policy dictated that "all of the confidential information to which Barnes was permitted access was to be stored on and accessed only fromPrimePay's secure drive" (Borman 5). While there were some active security measures in place, the bulk of the company's information protection depended upon people following policies, but the fact is that policies alone, even when coupled with "non-disclosure and employment agreements…[do] nothing to stop the perpetrating employees from misappropriating company trade secrets" (Favro 16). Policies and protocols are a good start, but information governance needs further development.

The use of personal cloud storage at work, known as bring-your-own-cloud (BYOC), has definite benefits. Cloud storage allows users to bypass physical storage limitations for a variety of digital documents, photos, music, and other files. It also allows them to easily move files between a variety of devices, from computers to phones to tablets and so on. At work, personal cloud storage "like Dropbox, Box, and Google Drive can obviate clunky network storage options and simplify data sharing and teamwork among colleagues" (Favro 2). Despite the upsides, BYOC environments, such as the one in the PrimePay case, can create severe gaps in attempts at maintaining information governance (IG). Many companies have taken a *laissez faire* approach to personal cloud storage, enabling access with little further oversight and "little follow up effort is taken to prevent employees from transferring confidential information from company servers to a personal cloud" (6). The attributes that make personal cloud storage beneficial – cheap, unlimited storage with simple transfers and easy collaboration – combined with weak internal regulation can result in a number of chinks in an organization's information armor, resulting in compromised trade secrets, poor information retention, information security leaks, and e-Discovery difficulties ("Polluting"; Favro 3). As the PrimePay case shows, "it can be especially problematic when an employee leaves the company with proprietary materials and begins working for an industry competitor" (Favro 6). While court documents suggest that the company

did not suffer any real catastrophic consequences, the public embarrassment does not help any organization, especially one that relies on a reputation of reliability to attract and maintain clients, as well as other indirect costs that can be difficult to enumerate. Not only did PrimePay have to pay for investigations, legal fees, and court costs, but there are also financial costs and losses in productivity as staff must be redirected to deal with the case as well as the loss of information itself. On top of that, there is also the fact that "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" (16). The risks of BYOC and the associated direct and indirect costs could be ameliorated with a more robust, mature IG program.

Possible Solutions

This instance shows two broad paths a company can take. One is to allow the use of personal cloud storage (BYOC), while the other is to proscribe its use (non-BYOC). For companies that elect to allow BYOC, policies need to be enacted that clearly delineate what platforms are allowable, what data can and cannot be transferred, what rights the company has to access and retain or destroy information in a personal cloud account, what rights the company has to disable BYOC access during or after a person's employment, what privacy rights employees have to data stored in their personal accounts, what audit and enforcement mechanisms will be in place to guarantee compliance, and what disciplinary measures may be taken for instances of noncompliance ("Personal Clouds" 14). Policy development should begin with a data map of all locations where a company's organization resides, whether onsite or off. The map is useful for retention of information and streamlining litigation discovery, but it is also "essential for controlling ingress and egress to proprietary information – precisely the data endangered by personal cloud applications" (Favro 18). A company can only develop solid policy once it knows where the data is, where it goes, and what the risks are.

Companies that disallow BYOC should maintain policies that explicitly forbid the use of personal cloud storage, define audit and enforcement mechanisms, and lay out consequences for noncompliance ("Polluting"). Non-BYOC organizations should also make use of electronic security measures to help make sure employees do not try to circumvent the policy, such as blocking programs, which "while not foolproof, are a practicable first step to preventing some personal cloud use" (Favro 20). Instead of multiple, personal accounts, a company could use

in-house or cloud-based collaboration software that "creates and maintains a secure collaborative workspace for interaction and information sharing by group participants" (Saffady 107). Such systems maintain a controlled platform where files can be shared and opened by authorized users without the risks associated with BYOC (107). Companies may also elect to provide cloud storage rather than relying on individuals to use their own accounts. This route provides remote access to a centralized repository without having someone copy files to less secure media or accounts, and it also "prevents duplication of information, provides access to the most current version of information, and stores information in an environment that only authenticated users can access" (Smallwood 340).

Regardless of whether a company decides on BYOC or non-BYOC, there are further steps that can help strengthen IG. For example, requiring two-factor authentication to verify login identity wherever possible can provide strong protection, as can actively monitoring and logging all network activity to identify fraudulent or illicit actions quickly (Smallwood 347). In particular, monitoring and examining the computer and network activity of terminated employees for illicit activities is a good standard practice when feasible (Favro 20). If such a review is financially impractical, an organization should still consider evaluating the activity of employees whose access poses a high risk to the company (21). Beyond this, there are a number of software tools that can benefit an organization:

- Enterprise content management (ECM) software allows an organization to create and maintain a repository of digital content (Saffady 96). These platforms often include security controls that "limit access to digital content on a need-to-know basis to prevent unauthorized retrieval of…confidential or sensitive information" while also maintaining "an audit trail of document-related activity" (98).
- Mobile device management (MDM) software – also known as enterprise mobility management – allows an enterprise to monitor, secure, and manage devices such as smartphones, tablets, and laptops remotely. The software allows the information technology (IT) staff to reach out to these devices "to add, upgrade, or delete software, change configuration settings, and ‘wipe’ or erase data, and make other security-related changes and updates" (Smallwood 324).
- Data loss prevention (DLP) software can help with data mapping by showing how information flows within and outside an organization, and those flows can in turn be

monitored and analyzed (Smallwood 26). A benefit of DLP systems is that they identify, monitor, and protect documents that are in use, in motion across the network, and at rest in storage. One downside is that DLP's monitoring is binary: access is allowed or it is not (263).

- Information rights management (IRM) systems provide more nuanced security than DLP and offer constant, persistent security to protected files that travels with the data whether at rest, in use, or in transit (Smallwood 265). The protections that IRM offers "prevent unauthorized viewing, editing, printing, copying, forwarding, or faxing. So, even if files are somehow copied to a thumb drive and taken out of the organization, e-document protections and usage are still controlled" (265).

Recommended Action Plan

The PrimePay case "reinforces the lesson…that a laissez-faire approach to personal clouds may lead to corporate disasters" (Favro 10). The company obviously had some form of IG in place, as evidenced by corporate policies, but it relied too much on the honor system, depending on people to do as they are supposed to rather than taking a more proactive stance. PrimePay is a sizeable company with about 615 employees ("Primepay Revenue") in offices across eleven states ("All PrimePay") and an estimated annual revenue between $128.3 million ("PrimePay – Overview") and $164 million ("PrimePay Revenue"). The spread-out nature of the enterprise mandates some kind of electronic collaboration capabilities. With that in mind, the following action plan is recommended:

- Maintain the BYOC environment.
- Map data across the company to get a complete picture of where it resides and how and where it flows. Use this information to inform the policy-revision process.
- Conduct a review of all relevant IG policies and procedures to identify weaknesses and gaps.
- Work with employees to rewrite existing policies and draft new ones as needed to clearly define the use of personal cloud accounts, including: what cloud storage platforms are allowed; what data can and cannot be transferred; what rights the company has to access, retain, and destroy information in an employee's personal cloud account; what rights the company has to disable BYOC access during or after employment; what privacy rights employees have to data stored in their personal accounts; what audit and enforcement

mechanisms will be used to monitor compliance; and what consequences arise from noncompliance.

- Review, procure, and implement enterprise content management, mobile device management, and information rights management systems, either as a turnkey platform or individual systems that can work together.
- Require two-factor authentication to verify login wherever possible.
- Actively monitor and log all network activity and review regularly for suspicious activity.
- Conduct training for all employees on the new policies, controls, and software, with potential extra training for those impacted the most by the changes.
- Manage the change process, taking advantage of opportunities to reiterate the importance of said changes and retrain as needed.

It must be noted that this action plan is not without its risks. BYOC exposes a number of potential weak points as noted earlier. Potential disinterest or even resistance to the proposed changes is also possible. Consistent communication *with* employees (rather than *at* them) and making use of their feedback is crucial to getting them on board, as is executive-level sponsorship and engagement. If leadership slacks off and/or does not seem to care about the process, staff will quickly follow suit. Another drawback is the financial commitment. Staff will need to dedicate time and resources to the necessary research and implementation of the various policies, controls, and software, to say nothing of the cost of the software itself.

That being said, however, the benefits outweigh the risks, which can be mitigated. First of all, this approach helps ensure employee buy-in. PrimePay already has an ingrained culture allowing for personal cloud usage. Attempting to change something deeply rooted in corporate culture can be costly and difficult, if not simply an exercise in frustration. Modifying something staff feels is beneficial rather than scrapping it increases the likelihood they will buy into the change, which is crucial for any new effort to take hold. Despite the costs involved, stronger IG has proven benefits over time, including improved collaboration between business sites, such as PrimePay's scattered offices. The data mapping and monitoring also helps to prevent future losses to internal and external threats (Smallwood 26). Improved IG also streamlines the e-Discovery process, reducing risk, liability, and cost while providing systematic, legally defensible methods of getting rid of information that is no longer needed (6). Reducing risk exposure, as well as improving e-document security and quality, "cutting out unneeded stored

information, and streamlining information technology (IT) development while focusing on business results add up to better organizational health and viability and, ultimately, an improved bottom line" (119). In addition to increasing efficiency of workers and less money spent addressing these issues, avoiding the loss of face from an embarrassing incident, as well as potential loss of competitive edge and even clients, all directly impacts the bottom line and the company's position in the industry.

Works Cited

"About PrimePay." *PrimePay*, https://primepay.com/about-us.

"All PrimePay office locations." *Indeed.com*, https://www.indeed.com/cmp/Primepay/locations

Borman, Paul D. "PrimePay, LLC v. Barnes et Al." *Justia Law*, 20 May 2015, https://law.justia.com/cases/federal/district-courts/michigan/miedce/2:2014cv11838/291212/35.

Favro, Philip. "Addressing Employee Use of Personal Clouds." *Richmond Journal of Law & Technology*, vol. 22, no. 3, Mar. 2016, pp. 1–21. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=lft&AN=116894861&site=eds-live&scope=site.

HighPoint Payroll. https://www.highpointpayroll.com.

"IP Law Tracker Docket Review - IV." *Brooks Kushman*, May 2015, https://www.brookskushman.com/insights/ip-law-tracker-docket-review-iv.

"Personal Clouds Can Present Security Problems." *Information Management Journal*, vol. 50, no. 2, Mar. 2016, p. 14. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=bth&AN=113586324&site=eds-live&scope=site.

"Polluting the Corporate Environment with Employee Use of Personal Clouds." *Innovative Driven*, 7 Jan. 2016, https://www.innovativedriven.com/blog/polluting-the-corporate-environment-with-employee-use-of-personal-clouds.

"PrimePay – Overview, News & Similar Companies." *ZoomInfo*, https://www.zoominfo.com/c/primepay-llc/31227916

"PrimePay Revenue and Competitors." *Growjo*, https://growjo.com/company/PrimePay.

Saffady, William. *Information Governance: Concepts, Requirements, Technologies*. ARMA International, 2017.

Smallwood, Robert F. *Information Governance: Concepts, Strategies, and Best Practices*. Second edition, John Wiley & Sons, Inc, 2020.