Fourth Amendment Protection for Users' Information Stored in the Cloud: The Case of Mint.com

YENNY TENG-LEE*

I. INTRODUCTION

Dropbox, Google, Facebook, Twitter, YouTube, Mint, Salesforce, eBay, and Yelp all have something in common: they allow users to access software or upload data on-line through any computer with Internet access. They use a cloud-computing platform.

Despite this common feature, the definition of cloud computing is still subject to debate. The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as "on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)."[1] Cloud computing can refer to electronic storage space or software rented from a remote publicly or privately owned cloud provider.[2]

The use of cloud computing will expand in the foreseeable future.[3] In recent years, the world has witnessed the increased popularity of cloud computing: Facebook, Yelp, Zynga, Twitter, and Hulu are just a few examples of noteworthy web-based companies that utilize the technology. Experts believe that by 2020, cloud computing will change how people use computers: "most users will perform most computing and communicating activities through connections to servers operated by outside firms."[4]

This paper explores whether users' financial information stored in the cloud by Mint.com ("Mint") has Fourth Amendment protection against unreasonable search and seizure.

---

* J.D. Candidate, University of San Francisco School of Law, 2013; M.Sc. in Business Administration with Finance emphasis, San Francisco State University, B.A. in Accounting, University of Gadjah Mada, Indonesia. I thank Prof. Susan Freiwald for her invaluable guidance in writing this paper.

1. Harvard Law National Security Research Group, *Cloud Computing & National Security Law*, LAWFARE BLOG (Oct. 1, 2010), http://www.lawfareblog.com/wp-content/uploads/2010/10/Cloud-Final.pdf.

2. David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009).

3. *See* MKT. INTEL GRP., THE FUTURE OF VIRTUALIZATION, CLOUD COMPUTING & GREEN IT: GLOBAL TECHNOLOGIES & MARKETS OUTLOOK - 2011-2016 (2010) (estimating that cloud computing will grow to a $218 billion industry by 2016).

4. JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF CLOUD COMPUTING (2010), *available at* http://pewresearch.org/pubs/1623/future-cloud-computing-technology-experts.

A. MINT.COM

Launched in September 2007, Mint is a web-based service that consolidates and tracks its users' financial information in various financial institutions free of charge. The service is meant to assist users in organizing and managing their finances and is not intended to provide legal, tax or financial advice.[5] Intuit, Inc. ("Intuit") acquired Mint in 2009[6] and from 2010 to 2011[7] the service grew from three to five million users. [8]

The Mint Terms of Use and Privacy and Security Policy ("User Agreement") are agreements between Mint's parent company and its users, which must be adhered to in order for users to benefit from the information consolidation service provided.[9] For consistency, this paper will refer to Mint instead of Intuit unless Intuit's different role needs to be discussed.[10]

In its User Agreement, Mint specifies that users grant Mint the right to retrieve (and use) users' financial information maintained online by third party financial institutions, such as banks and credit card companies ("Users' Information" or "User Data").[11] Mint accesses users' financial information in the financial institutions under its contract with third party providers. Mint makes no effort to review the information for any purpose, including but not limited to accuracy, legality, or non-infringement. Subsequently, Mint stores users' financial data extracted from the third party financial institutions in its servers.[12]

1. The Trend in Cloud Computing and Privacy Concerns

Data privacy in cloud computing is one of the top five concerns in privacy issues.[13] The Fourth Amendment of the United States Constitution provides protection to persons in the United States against unreasonable

5. Mint—Terms of Use, § 3, https://www.mint.com/how-it-works/security/terms (last revised July 26, 2012).

6. Belinda Luscombe, *Intuit Buys Mint.com: The Future of Personal Finance?*, TIME.COM (Sept. 15, 2009), http://www.time.com/time/business/article/0,8599,1923290,00.html.

7. *Reading, Writing and Money Management: Mint.com Goes to School*, BUSINESS WIRE (Dec. 20, 2010), http://www.businesswire.com/news/home/20101220005460/en/Reading-Writing-Money-Management-Mint.com-School.

8. Steven Gianakouros, Response to *How Many Unique Users Does Mint.com Have?*, QUORA.COM (Jan. 29, 2011), http://www.quora.com/How-many-unique-users-does-Mint-com-have.

9. Mint—Privacy and Security Policy, https://www.mint.com/how-it-works/security/policy (last revised Feb. 19, 2010).

10. Intuit is known for its accounting products such as QuickBooks, payroll services, TurboTax, and others. *See* Intuit—Corporate Profile, http://about.intuit.com/about_intuit/profile (last visited Nov. 4, 2012).

11. *See* Mint—Privacy and Security Policy, *supra* note 9, § 2 (Mint may "make anonymous or aggregate personal information and disclose such data . . . to . . . organizations approved by Intuit that conduct research into consumer spending.").

12. Mint—Terms of Use, *supra* note 5, § 49.

13. Cynthia J. Larose, *Top 5 Commercial Data Security and Privacy Issues in 2012*, THOMSON REUTERS NEWS & INSIGHT (Jan. 30, 2012), http://newsandinsight.thomsonreuters.com/Legal/Insight/2012/01_-_January/Top_5_commercial_data_security_and_privacy_issues_in_2012.

searches and seizures by the government. On the one hand, it is a constitutional right of any individual in the United States to have protection from the government's overzealous penetrating inquiries. On the other hand, the government needs to perform its mandated police functions for the good of society. The tension between the two competing interests is ever evolving.

Technological development has arguably outpaced Fourth Amendment law. The United States Supreme Court has never issued a ruling clarifying the Fourth Amendment protection of cloud computing.[14] Only one federal appellate case has examined an unreasonable search and seizure in the cloud context.[15] The Sixth Circuit decided in *U.S. v. Warshak* that users' emails stored with an Internet Service Provider ("ISP") enjoyed Fourth Amendment protection, and that law enforcement agents must obtain a warrant before compelling an ISP to produce such emails.[16]

The legislative response has been equally underwhelming. The Electronic Communications Privacy Act of 1986 ("ECPA") covers electronic communications, but experts argue that it is already outdated.[17] For example, cloud computing was almost unheard of in the 1980s.[18] Users routinely downloaded emails to their computers instead of storing them with a third party.[19] In that context, it seems reasonable for ECPA to treat emails stored in third parties' servers over 180 days as abandoned.[20] However, with the expansion of cloud computing, third party storage became commonly used for storing emails or data due to its convenience, low cost, and huge capacity.[21] Thus, it is no longer reasonable for ECPA to treat emails stored over 180 days in third parties' servers as abandoned and without the statutory protection of a warrant requirement.

Between outdated legislation and relative judicial silence on the issue, the state of data privacy on the cloud is in flux. Fourth Amendment protection for cloud computing consists of a patchwork of judicial opinions and statutory provisions, and has left users, providers, and government agents confused with its application.

In Part II, this paper analyzes judicial precedents under the Fourth Amendment. In Part III, the paper applies the judicial precedents to the case of Mint by exploring and analyzing potential arguments by the government and Mint users. In Part IV, the paper scrutinizes whether users

14. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 3 (2007), *available at* http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

15. *Id.*

16. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

17. *ECPA Reform: Why Now?*, DIGITAL DUE PROCESS BLOG, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited May 22, 2012).

18. *See* Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1045 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1288344.

19. *Id.*

20. *Id.*

21. *Id.* at 1046.

have consented to access to their information by Mint such that users have no reasonable expectation of privacy vis-a-vis the government.

To summarize the arguments below, Part III of this paper discusses how users and the government have applied the Supreme Court's arguments: the third party doctrine, business records, business ownership, and a normative approach to Mint's case. Users and the government have equally strong arguments under the agency theory and the third party doctrine respectively, but precedents may favor the government. Under the business records argument, users may retain their reasonable expectation of privacy via an analogy between passwords and closed containers. Under the record ownership argument, the government has convincing arguments that the aggregated or anonymized data are users' data, and that Mint's selling of the data implies Mint's ownership. Under the normative approach, the court may find for users by recognizing that sending consolidated data to users via Mint's website is analogous to letters in P.O. boxes or email inboxes, and more importantly, that the case of Mint raises a broader issue of privacy concerns within cloud computing.

In Part IV, both the government and users have strong arguments about whether or not users have granted access to their information to Mint such that it would defeat a reasonable expectation of privacy in users' information. The court will likely decide in the government's favor because of users' ignorance. However, deciding a constitutional issue based on user agreements is unsound and goes against the fabric of our society.

The paper concludes that the User Agreement, which is effectively determined unilaterally by companies, should not be used to decide a constitutional issue such as Fourth Amendment protection. Finally, the application of judicial precedents demonstrates that both the government and users have equally strong arguments. Other factors, such as the importance of the issues in the arguments discussed in this paper or political wind in the courts may tip the balance.

II. FOURTH AMENDMENT PPROTECTION OF FINANCIAL IINFORMATION

The Fourth Amendment of the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[22]

Katz v. United States is the seminal case in which the Supreme Court established the test for Fourth Amendment protection.[23] Defendant Katz was using a public phone booth for illegal gambling, while an FBI agent listened to his conversation using an eavesdropping device placed on the

22. U.S. CONST. amend. IV.

23. Katz v. United States, 389 U.S. 347 (1967).

exterior part of the phone booth.[24] The Supreme Court held that a person has Fourth Amendment protection against an unreasonable search and seizure when: (1) that person has a subjective expectation of privacy in the subject of the search and (2) that expectation is reasonable from society's point of view.[25]

Miller v. United States is another major case determining the reasonable expectation of privacy in bank depositors' financial documents such as checks, financial statements, deposits, and loan records kept by banks.[26] Defendant Miller had an unregistered whiskey still and alleged intent to defraud the government of whiskey tax. Law enforcement agents compelled the banks that maintained Miller's accounts to disclose all account records to law enforcement.[27]

The Supreme Court found that depositors did not have a reasonable expectation of privacy in their financial documents for the following reasons. First, under the third party doctrine, depositors assumed the risk of leakage to the government when they revealed their records to banks, which were parties to their commercial transactions.[28] Second, the financial documents were not Miller's private confidential papers but rather the business records of the bank, because the financial documents were negotiable instruments that were exposed to the bank's employees in the ordinary course of business.[29] Third, the banks owned the financial documents because the documents were addressed to and from the banks, and the banks had a stake in the records' continued availability and acceptance.[30] Fourth, the Bank Secrecy Act requires banks to maintain records for criminal, tax, and regulatory investigations and proceedings.[31] Thus, Congress assumed the lack of any legitimate expectation of privacy concerning information retained in bank records.[32]

In the following section, both users and the government will use the Supreme Court's arguments above: the third party doctrine, business records, and record ownership, in order to argue whether Mint's users have a reasonable expectation of privacy in users' data stored by Mint.

24. *Id.* at 348.
25. *Id.* at 361.
26. United States v. Miller, 425 U.S. 435, 437 (1976).
27. *Id.*
28. *Id.* at 443.
29. *Id.* at 442.
30. *Id.* at 440.
31. *Id.* at 444.
32. United States v. Miller, 425 U.S. 435, 442–43 (1976). Statutory mandates, such as the Bank Secrecy Act, the ECPA, and the USA Patriot Act, are beyond the scope of this paper.

III. EVALUATING USERS' REASONABLE EXPECTATION OF PRIVACY IN MINT.COM

A. THIRD PARTY DOCTRINE

Under the third party doctrine, a person assumes the risk of leakage when he or she reveals information to another party in a communication or transaction.[33] In *Miller*, the depositors took the risk that the banks, as parties to their commercial transactions, would convey the depositors' information to the government. The depositors assumed the risk of leakage even if they revealed their information with the assumption that it would be used only for a limited purpose and that their confidence placed in the third party would not be betrayed.[34] The banks in *Miller* were parties to the commercial transactions with the depositors because the depositors voluntarily conveyed their records to the banks.

The government may argue that Mint's users have no reasonable expectation of privacy under the third party doctrine because Mint is a party to the transaction with the users and thus the users assume the risk of leakage. Mint is a party to the transactions because users voluntarily convey their information to Mint by allowing Mint to access to the users' accounts with various financial institutions. Mint, in return, provides users with a consolidated financial picture. Regardless of the limited purpose of the data in Mint's possession or the confidence placed in Mint, users assume the risk that Mint will reveal the information to the government. Under the third party doctrine, users do not have a reasonable expectation of privacy in their financial records stored with Mint.

Users may argue that they retain a reasonable expectation of privacy in their information because Mint is their agent rather than a party to their commercial transactions. Since Mint is not a party, users do not assume any risk of leakage and thus the third party doctrine does not apply.

Under agency theory, the only purpose of the agency relationship is for the agent to carry out the will of the principal. At a minimum, the principal must have the right to set the goal of the relationship.[35] Unlike the depositors' relationship with the banks in *Miller*, Mint acts as an agent to its users. Banks are parties to commercial transactions with their depositors but are not their agents, since each party's goals differ. The banks have a substantial stake in the negotiable instruments' continued availability and acceptability, while the depositors have a stake that is limited to their account balance. Mint, by contrast, clearly defines its role as an agent in its User Agreement.[36] Mint acts to serve its users and has the same scope of authority as its users. In other words, Mint acts as an extension of its users and therefore not as a party to the commercial transactions. Consequently,

33. *Id.* at 443.
34. *Id.*
35. RESTATEMENT (THIRD) OF AGENCY § 1.01 (2006).
36. Mint—Terms of Use, *supra* note 5, § 10.

the third party doctrine does not apply.

1. Assessment of Users' Expectation of Privacy Under Third Party Doctrine

Agency theory allows Mint to circumvent the third party doctrine. An agency relationship is formed when two parties consent that one party is an agent and the other is a principal.[37] Unlike the banks in *Miller*, Mint defines its role as an agent to users and the users accept that by agreeing to Mint's User Agreement.

There are two caveats to the agency theory. First, if the court perceives Mint's goals as substantially different from users' goals, the agency theory may lose its footing. For instance, the court might construe Mint's selling of its users' anonymized or aggregated financial data as substantially different from users' goals, or to be in conflict, because users value their privacy. If so, Mint would be more like a party rather than an agent and the third party doctrine will apply.

Second, an agent may still consent or be compelled to disclose users' data. To pass Fourth Amendment muster, the agent must act within the scope of the agency relationship if an agent chooses to convey user information to the government. Similarly, if the government compels an agent to disclose user information, the government must proceed with a warrant or show that neither the agent nor the users have a reasonable expectation of privacy and that the agent acted within the scope of the agency. Both parties have strong arguments to win their case. Even though the court has favored the third party doctrine in the past,[38] the court may favor users under the agency theory.

B. BUSINESS RECORDS

Miller held that checks, deposit slips, account records, loan documents, and other financial records of depositors held by banks were not confidential communications, but rather negotiable instruments to be used in commercial transactions and exposed to the banks' employees in the ordinary course of business.[39] Consequently, the records were considered business records of the banks and the depositors had no reasonable expectation of privacy in the records.[40]

The government may argue that users do not have a reasonable expectation of privacy in the information they store with Mint because it is exposed to Mint's employees in the ordinary course of business. Mint's business consists of providing consolidated financial pictures to users as well as selling users' data to other businesses. In the User Agreement, Mint specifies that employees and third party vendors will require access to

37. RESTATEMENT (THIRD) OF AGENCY § 1.01.

38. United States v. Miller, 425 U.S. 435, 443 (1976); *see also* Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971).

39. *Miller*, 425 U.S. at 440.

40. *Id.*

users' data in order to provide consolidated financial pictures to users.[41] Additionally, Mint has the right to sell anonymized and aggregated users' information to buyers under the User Agreement.[42] Consequently, as in *Miller*, users' data are business records and not confidential because the data is exposed to employees, third party vendors, and data buyers, all in the ordinary course of Mint's business.

Users may argue that they have a reasonable expectation of privacy because users' information is not a negotiable instrument, is not exposed to Mint's employees in the ordinary course of business, as well as because users have passwords on their Mint accounts.

1. Negotiable Instruments and the Ordinary Course of Business

Users' information is not exposed to Mint's employees in the ordinary course of business because the information is exposed only to those employees and third party vendors necessary to provide proper service to users. Users' information is guarded zealously and exposed only to few select employees and third party vendors unlike with the banks in *Miller*.[43] Employees or third party vendors must pass a difficult selection process and follow strict procedures in accessing the users' data within the limited scope of serving the users.[44] Users' information is guarded zealously by ensuring only the authorized persons can access the building where the data is stored. Mint uses hand scanning, guards, locked servers, constant monitoring, and encryption as security measures for these buildings.[45] Mint password-protects servers with user data and further ensures security by requiring the use of an "encryption key that is broken up into five separate smart cards carried only by senior Mint.com executives."[46]

Furthermore, user information in Mint is not a negotiable instrument, unlike the checks at issue in *Miller*. Mint has no stake in the continued availability and acceptance of user information.

Finally, Mint's sale of anonymized or aggregated user information does not expose user information to Mint's employees in the ordinary course of business because users have lost any identifying association to the data. The data is, in substance, disconnected from users.

i. Assessment of Users' Expectation of Privacy Following Exposure in the Ordinary Course of Business, and Negotiable Instruments

The Supreme Court has historically treated business and corporate

41. Mint—Privacy and Security Policy, *supra* note 9, § 2.

42. *Id.*

43. *Id.*; *Miller*, 425 U.S. 435.

44. Mint—Privacy and Security Policy, *supra* note 9, §§ 1–2, 12 ("They may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.").

45. Jennifer Saranow Schultz, *Should You Trust Mint.Com?*, N.Y. TIMES BLOG (July 6, 2010), http://bucks.blogs.nytimes.com/2010/07/06/should-you-trust-mint-com.

46. *Id.*

records as non-confidential information.[47] Private records become business records when exposed to employees in the ordinary course of business.[48] In examining whether Mint has sufficiently exposed the information, we need to measure the extent of employee and third party access to user information. However, even if employees can access user information in the ordinary course of business, users retain a reasonable expectation of privacy if the access is via software and not human review.

In *Warshak I*, the court explained that if employees' review, monitor, or screen user data using software without any human intervention, then the users' reasonable expectation of privacy remains intact.[49] This is analogous to the post office screening of packages for evidence of drugs or explosives. The post office scans the content of packages without much human intervention such that the screening does not defeat privacy expectations in the content of the mail or packages.[50] On the other hand, if the screening requires extensive human intervention, then the user information held by Mint would be exposed to employees in the ordinary course of business and thus, users would have no reasonable expectation of privacy.

Therefore, the government needs to show not only that user information is exposed to Mint's employees in the ordinary course of business, but also that the exposure requires extensive human intervention.

2. Password Protection

Users retain reasonable expectations of privacy because they set passwords on their Mint accounts. In *United States v. Barth*, Defendant Barth took his computer to a technician for repair.[51] Unbeknownst to the defendant, the technician was a government informant.[52] The informant found the defendant's child pornography files in the computer and gave them to the government.[53] The court held that data in closed computer files and hard drives has Fourth Amendment protection because the files were analogous to the content of a person's closed containers and closed personal effects, which had received protection in the past.[54]

Placing passwords on online accounts is analogous to having a closed container for physical items, a hard drive for data storage, or having a private computer file.[55] Physical space and distance disappear on the Internet. Internet users utilize passwords for online services to create personal spaces or virtual closed containers accessible only to the owner of

47. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 149 (2008).

48. *Miller*, 425 U.S. at 440–43.

49. Warshak v. United States, 490 F.3d 455, 474 (6th Cir. 2007).

50. *Id.*

51. United States v. Barth, 26 F. Supp. 2d 929, 932-33 (W.D. Tex. 1998).

52. *Id.*

53. *Id.*

54. *Id.* at 936–37.

55. Harvard Law National Security Research Group, *supra* note 1, at 17.

the services and a few authorized third parties. Mint users use passwords to create a virtual closed container for their information. Following the logic of *Barth*, users have a reasonable expectation of privacy for the information that they store in the virtual closed container.[56]

i. Assessment of Users' Expectation of Privacy Under Theory of Password Protection

The Supreme Court has repeatedly ruled that owners have a reasonable expectation of privacy for the contents in a closed container. In *United States v. Ross*, the Court held that the owner of a closed container enjoys Fourth Amendment protection so long as the content in the container is concealed from plain view.[57] Again, in *United States v. Jacobsen*, the Court repeated that an owner's reasonable expectation of privacy remained intact if the container was closed and the content was protected from public view.[58]

Under this rule, the court will likely hold that users have a reasonable expectation of privacy in users' information in password-protected Mint accounts because passwords on Mint accounts can be thought to create a virtual closed container that conceal users' information from plain view.

To summarize, in the business record discussion, users can counter the government's position that users' information is exposed to Mint's employees in the ordinary course of business with two arguments: that the limited exposure and password protection of their information establishes reasonable expectation of privacy. Analogizing passwords to a virtual closed container may gain traction in courts considering the repeated holding of Fourth Amendment protection for closed containers users. Any further examination of the ordinary course of business exposure will require information about the extent and the nature of access that employees and third parties have to user information stored by Mint.

3. Records Ownership

Because the depositors' financial records belonged to the banks and were not "private papers," *Miller* held that the depositors did not have a reasonable expectation of privacy in the records.[59] The banks owned the checks, deposits slips, loan documents, and other financial records because they were addressed to and from the banks. Additionally, the banks had a substantial stake in the records' continued availability and acceptance, which tends to give the banks more sense of ownership of the records.

The government may argue that Mint claims the ownership of user information by asserting its rights to sell user information in aggregation or anonymity to third parties at any time, similar to the banks which own financial records in *Miller*. Neither aggregation nor anonymity diminishes

56. *Id.*
57. United States v. Ross, 456 U.S. 798, 822–23 (1982).
58. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984).
59. United States v. Miller, 425 U.S. 435, 437 (1976).

the fact that the information sold is user information. In contract law, a sale of goods occurs when title has been transferred for a price.[60] A seller must own the title of the goods before the seller can transfer the goods. Mint's claim of ownership of user information is more pervasive and clear in comparison to the bank's ownership of financial documents in *Miller* because the banks did not claim they could sell the depositors' financial documents.

Mint also has a stronger claim of ownership of user data because it has a substantial stake in the business. Mint's business model relies on selling aggregated and anonymized user data to third parties. Consequently, users have no reasonable expectation of privacy in their data.

Users may argue that they retain a reasonable expectation of privacy because Mint does not own their information. Unlike the banks in *Miller*, Mint's relationship to its users is like a bank's relationship to its depositor of one of its safe deposit box. The bank merely provides a service to store depositors' belongings. Safe deposit box customers can choose how to organize their items or what information to store in the safe. Users still own the items and information in the safe deposit box, not the banks. Banks cannot consent or be compelled to turn over items in safe deposit boxes. Thus, depositors have a reasonable expectation of privacy in their items and information stored in the safe deposit boxes.[61]

Like safe depositors, Mint users own the data they store in Mint because Mint only uses user-identified information to improve its service to users and it needs the user's permission before providing the information to a third party.[62] Mint, similar to the banks with safe deposit boxes, merely provides a service to store and organize information. Users use Mint to organize their financial records by authorizing the collection of information from various financial institutions. Similar to the banks with safe deposit boxes where depositors give certain bank employees access to their safe deposit boxes, users give Mint's employees access to their data stored by Mint. Consequently, like the safe depositors, users have a reasonable expectation of privacy for their data stored by Mint.

Finally, even if Mint's selling of aggregated and anonymized user information indicates Mint's ownership of the information that would defeat the reasonable expectation of privacy in such information, users should be able to retain privacy in non-aggregated or non-anonymized user information. This is because Mint's access is limited to aggregated and anonymized users' data. The government cannot bootstrap Mint's limited ownership in the aggregated and anonymized users' data to allow the government to access non-aggregated or non-anonymized user data.[63]

60. U.C.C. § 2-106 (as amended through 2002).

61. United States v. Thomas, 878 F.2d 383 (6th Cir. 1989).

62. Mint—Privacy and Security Policy, *supra* note 9, §§ 1–2, 5.

63. *See* Warshak v. United States, 490 F.3d 455, 471 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

i. Assessment of Users' Expectation of Privacy Under the Records Ownership Theory

The safe deposit box analogy may have some merit, but the government can easily counter this analogy by distinguishing the frequency of access in the respective cases. The banks do not reveal the content of the safe deposit boxes and do not regularly access the safe deposit boxes. Mint, in contrast, regularly accesses user information via employees and third party vendors. Moreover, the banks do not require depositors to give their employees or third party vendors access to the depositors' safe deposit boxes. Most importantly, the banks do not sell any information or content in the safe deposit boxes.

The government's strongest argument is that Mint has established ownership by selling aggregated or anonymized user data to third party vendors because selling requires ownership.[64] The court may find for the government because its argument is more convincing than the users' argument that Mint is like a bank with a safe deposit boxes.

C. NORMATIVE INQUIRY

In addition to the positive inquiry where the Supreme Court evaluated the subjective and objective reasonable expectations, *Katz* employed a normative approach.[65] *Katz* held that "[T]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication"[66] and the caller "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[67] In other words, the phone has a vital role in society. Consequently, whatever people actually thought or knew about the privacy of their telephone calls, they were *entitled to believe* in the privacy of those calls, because any other result would be destructive of society's ability to communicate.[68] *Katz* expanded the scope of privacy to include at least some new technologies that enable private communication.

Echoing *Katz*'s normative approach, *Warshak* held that "[email] plays an indispensable part in the Information Age" and that "email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."[69]

Nonetheless, the government may still argue that users do not have any reasonable expectation of privacy in their Mint data. The courts in *Katz* and *Warshak* decided that telephone and email users have a reasonable

64. *See* U.C.C. § 2-106 (as amended through 2002).
65. Freiwald, *supra* note 14, ¶¶ 27–28.
66. Katz v. United States, 389 U.S. 347, 352 (1967).
67. *Id.*
68. Freiwald, *supra* note 14, ¶ 29.
69. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

expectation of privacy because the telephone and email were vital to society. But unlike phone calls and emails, Mint's act of consolidating user data on Mint's website is not a communication by definition.[70] Mint's process of gathering users' financial information from various financial institutions, subsequently organizing and consolidating the data, and finally presenting the data on their website is not a process of exchanging information between individuals or an act of transmitting data to users. Mint merely moves user data from one storage place to another.

Furthermore, the telephone and email have a vital role in societal communication. People are entitled to believe in the privacy of those calls or emails because any other result would be destructive of society's ability to communicate. Unlike the telephone or email, placing people's consolidated financial data on Mint's website does not have a vital role in the ability of society to communicate; it is merely a convenience. Mint's service is a far cry from those at issue in *Katz* and *Warshak*. The inability to track spending habits does not paralyze society's ability to communicate. Therefore, users have no reasonable expectation of privacy in their information in Mint.

Users may argue that they have a reasonable expectation of privacy under the normative approach. Communication is also "an act or instance of transmitting" information.[71] Mint does not meet the definition of communication because Mint obtains user information from various financial institutions, subsequently organizes and consolidates the information, and lastly transmits the information to individual users, whose access is password protected.

Moreover, sending consolidated data to users via Mint's website (where only users can view the information), is analogous to delivering letters to a P.O. box or email inbox. P.O. box users visit their individually locked boxes in the post office to access their letters, while email users access the email collected in their inbox on the email provider's website. Under *Warshak*, which established users' reasonable expectation of privacy in email, and *Ex Parte Jackson*, which did the same for postal mail,[72] users should have a reasonable expectation of privacy in their information on Mint's website.

Furthermore, *Katz* and *Warshak* should be interpreted broadly. The Supreme Court and the Sixth Circuit have laid a foundation of Fourth Amendment jurisprudence that includes a broad view regarding the vital role of communication in society.[73] After all, privacy protection is not only about communication, but also about the protection of information, the

70. Webster's dictionary defines "communication" as "a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior" or as "an act or instance of transmitting." *Communication Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/communication (last visited Nov. 2012) [hereinafter *Communication Definition*].

71. *Id.*

72. Ex parte Jackson, 96 U.S. 727, 733 (1877).

73. *See generally* Freiwald, *supra* note 14, ¶ 3.

individual, and physical territory.[74] More importantly, the court should not only reflect and mirror society's expectations, but also form and project the practices we *should* have.[75] In *Kyllo v. United States*, the court noted that technological progress must not erode the privacy guaranteed by the Fourth Amendment.[76]

Technology for convenience may become a necessity as its popularity increases. Email, letters, and the telephone were once mere conveniences. The cloud computing platform used by Mint has evolved over the years and experts predict that it will someday become a necessity because of its low cost and convenience, just like how the telephone, letters, and email have evolved.[77] In an era where people have multiple credit cards and bank accounts, where debts and bankruptcy are becoming more common, and where the time to care for personal and family matters is limited to a few hours a week, it can be argued that Mint's service is becoming a necessity.

1. Assessment of Users' Expectation of Privacy Under a Normative Inquiry

The easiest way for users to establish a reasonable expectation of privacy under the normative approach is to use *Warshak*'s email analogy and *Ex Parte Jackson*'s letters analogy.[78] If the court will not accept the analogies, users will have a tougher argument to make: that without Mint's services, society's ability to communicate or to function would be destroyed. Users will need to show that posting their consolidated information on Mint's website plays a vital role in society.

The court tends to avoid determining the vital role of a piece of technology.[79] Determining whether an ever-evolving current or future technology has a vital role in society without clear explanation from precedents is a daunting task. Susan Freiwald has recommended that instead of using the mushy "vital role" analysis in *Katz*, the court should structure a vital role analysis into several determining factors.[80] The court should also consider distinctive perspectives in its vital role analysis. From a narrow perspective, the online consolidating financial information service provided by Mint may not be vital to society. But, from a broader perspective, the intermediated content stored online by a third party like

74. ELEC. PRIVACY INFO. CTR., PRIVACY AND HUMAN RIGHTS 2006: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (1st ed. 2007).

75. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

76. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

77. *See* Harvard Law National Security Research Group, *supra* note 1, at 3; *see generally* Oza, *supra* note 18, at 1045–46 (comparing the means used to access the internet in 1985 to those in common use in 2008); Summary, THE FUTURE OF VIRTUALIZATION, CLOUD COMPUTING & GREEN IT: GLOBAL TECHNOLOGIES & MARKETS OUTLOOK - 2011-2016, RESEARCHANDMARKETS.COM, http://www.researchandmarkets.com/reports/1402312/the_future_of_virtualization_cloud_computing_and (last visited Nov. 2012) (summarizing the results related to cloud computing found in MKT. INTEL GRP., *supra* note 3).

78. Ex Parte Jackson, 96 U.S. 727 (1877).

79. See Freiwald, *supra* note 14, ¶¶ 3, 33–34.

80. *Id.* at ¶¶ 49–50.

Mint may soon attain a vital role in society as cloud computing is becoming a necessary part of our daily life.

IV. EXAMINING USER CONSENT TO MINT'S DATA ACCESS, AND THE IMPLICATIONS FOR THE FOURTH AMENDMENT

In 2010, the Sixth Circuit, confirming the federal appellate reasoning in *Warshak I*,[81] held that mere access by an intermediary or a third party was insufficient to eliminate an expectation of privacy in stored email.[82] However, when a user agreement provides ISPs access for regular auditing, inspection, or monitoring of users' files, or provides ISPs with blanket access, users lack a reasonable expectation of privacy.[83]

If the user agreement "clearly provide[s] for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of emails,"[84] users retain a reasonable expectation of privacy. Such limited ISP access reserved only for extraordinary circumstances is insufficient to undermine users' expectation of privacy. In dicta, the *Warshak I* court exemplified Yahoo!'s user agreement as ISP access in extraordinary circumstances.[85] Yahoo! may access users' emails if the access is:

> reasonably necessary to: (a) comply with legal process; (b) enforce the [Terms of Service]; (c) respond to claims that any Content violates the rights of third parties; (d) respond to your requests for customer service; or (e) protect the rights, property or personal safety of Yahoo!, its users and the public.[86]

Similarly, the 2010 *Warshak* court held that a subscriber agreement stating that the ISP "*may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service," does not diminish the users' reasonable expectation of privacy.[87]

The government may argue that Mint lacks a reasonable expectation of privacy for the following reasons. First, users have consented to limited protection of their information stored by Mint. Additionally, Intuit's, as well as Mint's, employees and third party vendors have blanket access to user information because they may access the information in the ordinary course of business. Mint can also sell anonymized or aggregated user information to the highest bidder.

First, the government may argue that users have agreed to limited protection of their information stored by Mint. Mint's privacy policy does not expressly specify protection for users' financial information. Mint

81. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

82. United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2008).

83. *Id.* at 286–87; *see also* Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

84. *Warshak*, 490 F.3d at 474.

85. *Id.* at 474 n.7.

86. *Id.*

87. *Warshak*, 631 F.3d 266, 287 (6th Cir. 2008) (emphasis added).

merely protects "personal information,"[88] defined as the users' name, address, phone number, fax number, and email address.[89] This personal information is distinguished from users' financial information derived from financial institutions. One may reasonably interpret Mint's Privacy and Security Policy not to provide any privacy protection to users' financial information. Consequently, users have consented to the absence of protection of their financial information and thus, have no reasonable expectation of privacy in that information.

Second, even if "personal information" can be interpreted to include users' spending or financial information, the users' consent to Mint's access, either expressly or impliedly, to their information exceeds the *Warshak* standard. *Warshak* held that users' privacy remains intact only if ISP share access in limited or extraordinary circumstances[90] such as is necessary for the operation and the protection of ISP services.[91]

The government is also likely to argue that Mint and Intuit have blanket access to users' personal information because employees and third party vendors may access the information within the normal course of business. In addition, third party contractors who provide services to Intuit or Mint may also access users' personal information within their normal course of business. Intuit's employees, as well as Mint's, may access users' personal information to operate and develop Mint's service, to analyze site usage and improve service, to do market research, plan projects, deliver administrative notices, and to provide money alerts and communications relevant to Mint's service.[92] Mint's claim that its employees are selected carefully does not diminish the blanket access argument.

Finally, the government may argue that users consented to the Privacy and Security Policy that permits Mint to sell anonymized or aggregated users' personal information to third party buyers. Such blatant exposure of users' information to third parties clearly exceeds the *Warshak* standard, which has set limited or extraordinary circumstances as the narrow boundaries of ISP access to email. Regardless of the anonymity or aggregation of user data, user's consent to access information for sale at any time constitutes blanket access beyond the *Warshak* standard. Mint's access also surpasses the Yahoo! user agreement described in *Warshak I*[93] and Warshak's ISP user agreement described in the 2010 *Warshak* decision.[94]

On the other hand, users may argue that their consent is insufficient to eliminate their reasonable expectation of privacy. First, the User

88. *See* Mint—Privacy and Security Policy, *supra* note 9.

89. *Id.*

90. Warshak v. United States, 490 F.3d 455, 474 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

91. *Warshak*, 631 F.3d at 287.

92. Mint—Privacy and Security Policy, *supra* note 9, § 1.

93. *Warshak*, 490 F.3d at 474 n.7.

94. *Id.* at 474.

Agreement protects users' financial and spending information and expressly defined personal information. Second, the users' consent to disclosure of aggregated or anonymized users' information does not waive their privacy interest in non-aggregated data. Even in the unlikely case that users have waived their privacy expectation, the waiver applies only to aggregated or anonymized user information. Lastly, the users' consent does not provide blanket access because Mint lacks any authority to review the financial information derived from third party institutions. Mint's access is limited to situations necessary to protect and develop its service. All access is, therefore, within the *Warshak* standard.

As mentioned, Mint expressly defines user's personal information as identifying information such as the users' name, address, phone number, fax number, and email address.[95] It is reasonable to interpret "personal information" to include "financial information" and "spending information" because the interpretation is consistent with the reading of the Privacy and Security Policy as a whole, and Mint's intention is to sell user data.

Section 2 of the Privacy and Security Policy states that aggregated or anonymized personal information may be disclosed to organizations that conduct research into consumer spending.[96] Purchasers would not be interested in aggregated or anonymized names, addresses, phone numbers, fax numbers, or email addresses alone. Thus, it is reasonable to infer that Mint may sell aggregated or anonymized financial or spending information of its users. Additionally, Mint's founder, Aaron Patzer recently[97] talked about the rich value of Mint's user spending data and how the aggregated data would attract hedge funds.[98] In response to users closing their Mint accounts, Patzer emphasized that Mint sold only aggregated or anonymized user data.[99] Therefore, the definition of personal information, reasonably and perhaps even necessarily, includes financial and spending information. Any protection specified in the User Agreement surely extends to user financial or spending information.

The second reason that privacy interest is not waived is that the users' consent to the disclosure of aggregated or anonymized data does not destroy their privacy interest in non-aggregated data. This is because privacy is the right to be free from unauthorized intrusions.[100] Intrusion transpires when the information identifies individuals. Similarly, disclosing

95. Mint—Privacy and Security Policy, *supra* note 9.

96. *Id.*

97. Aaron Patzer, Founder, Intuit, Remarks at SXSW panel: Data is Money: How Geeks are Changing Finance (Mar. 13, 2010).

98. Felix Salmon, *Personal Finance Online*, REUTERS.COM (Mar. 14, 2010), http://blogs.reuters.com/felix-salmon/2010/03/14/personal-finance-online.

99. Josh Smith, *Mint.com CEO Patzer Says It Doesn't Sell Individual Data*, DAILYFINANCE (Mar. 18, 2010), http://www.dailyfinance.com/2010/03/18/mint-com-ceo-patzer-says-it-doesnt-sell-individual-data.

100. *Communication Definition*, *supra* note 70.

anonymized or aggregated data is analogous to publishing polling results or empirical results in academic journals or other publications. Users retain a reasonable expectation of privacy even if their unattributed private views about abortion or insurance-financed contraception are published for public eyes. Otherwise, people will stop answering questions for public polling and research, crippling efforts to find solutions to societal problems or even worse, halting the democratic process.

Similar to users' bootstrap argument above,[101] even if government defeats users, government can only access aggregated or anonymized data because Mint's access is limited to aggregated or anonymized users' data.[102]

Finally, users retain a reasonable expectation of privacy because Mint's access is not a blanket access. Mint has no review authority over users' information from third party financial institutions.[103] Without "reviewing authority," Mint cannot inspect, monitor, or audit user data as demanded in *Warshak*.[104] Mint has security inspection authority like the ISP in *Warshak*, but the court in *Warshak* considered it to be a limited access and not a blanket access.[105]

User consent to Mint's access to their information does not constitute blanket access because the access is limited to situations enumerated in the Privacy and Security Policy. The enumerated situations only allow access, *inter alia*, to operate and develop Mint's service, to analyze site usage and improve service, to do market research, plan projects, deliver administrative notices, and to provide money alerts and communications relevant to Mint's service.[106] Such explicitly limited situations do not constitute blanket access. The access is necessary to protect and operate the service for users and consequently and is consistent with *Warshak* decision.[107] Therefore, users have not consented to a scope of access that defeats their reasonable expectation of privacy.

A. ASSESSMENT OF USERS' EXPECTATION OF PRIVACY UNDER MINT'S ACCESS TO USERS' DATA

Both sides have strong arguments about whether the Privacy and Security Policy defeats users' reasonable expectation of privacy. Mint's five millions users seem to have no qualms about giving up their aggregated or anonymized data privacy in a commercial setting despite the real possibility that aggregated data, depending on its granularity, and anonymized data can be re-traced to specific users.[108]

101. *See supra* Part III.B.3.
102. *See* Warshak v. United States, 490 F.3d 455, 471 (6th Cir. 2007).
103. Mint—Terms of Use, *supra* note 5, § 4.
104. United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010).
105. *Id.*
106. Mint—Privacy and Security Policy, *supra* note 9, § 1.
107. *Warshak*, 631 F.3d at 287.
108. Frederic Lardinois, *Report: Mint Considers Selling Anonymized Data from Its*

Susan Freiwald, an expert in information privacy law, argues that users granting Mint access to their data should not defeat their reasonable expectations of privacy because their interest in making use of the service necessitates the involvement of an intermediary.[109] Permitting access to an intermediary who needs such access to provide a service should have no bearing on one's reasonable expectations of privacy in relation to the government.[110]

From a public policy perspective, the reasonable expectation of privacy should not be determined by a click through online agreement that no average user would even read.

Users would waste $781 billion,[111] or 76 workdays per person per year, reading applicable privacy policies, thereby burdening society with inefficiency.[112]

Furthermore, no meaningful negotiation can take place even if a user were to read the terms of the agreement. Users generally have a weak bargaining position relative to the service providers, and the Internet would grind to a halt if users and website operators negotiated the terms of every visit.

Deciding a constitutional matter such as the Fourth Amendment based on websites' user agreements, which companies can change on a whim, and where individual users have no right to negotiate and have no bargaining power is against public interest and our foundation as a free society.

V. CONCLUSION

Here, *Katz* and *Miller* are the seminal precedents in discussing users' reasonable expectation of privacy in the context of financial information. They define the landscape of the reasonable expectation of privacy conversation. *Katz* created the two-prong test for reasonable expectation of privacy, while *Miller* applies the test in a financial context using the third party doctrine, business records, record ownership arguments, and the normative approach.

Part III concluded that first, after applying the precedents, users and the government are equally persuasive in their respective positions under the agency theory and the third party doctrine. Under the business records argument, the court will likely decide in favor of the users if the court finds

Users, READWRITE.COM (May 18, 2009), http://www.readwriteweb.com/archives/report_mint_considers_selling_anonymized_data_from.php.

109. Bellia & Friewald, *supra* note 47, at 165.

110. *Id.*

111. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

112. Keith Wagstaff, *You'd Need 76 Work Days to Read All Your Privacy Policies Each Year*, TIME.COM (Mar. 6, 2012), http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/#ixzz1xJZRJM2a.

the use of passwords to be analogous to a closed container that hides its content from public view.

Under the records ownership argument, the government has convincing arguments that the aggregated or anonymized data is user data, and that Mint's selling of such data implies ownership. Users may argue that Mint is unlike the banks in *Miller*, but more like the banks with safe deposit boxes. The court will likely find for the government because Mint has access to user data and Mint sells user data, while the banks with safe deposit boxes do not have any access to and do not sell the contents of the safe deposit boxes.

Under the normative argument approach in *Katz*, the court may hold for the government if they find that online financial consolidators like Mint are not vital to society. Otherwise, the court may find for the users if it uses Mint's case to tackle the privacy issues related to cloud computing. Cloud services have become pervasive in society such that Mint's *operational model* of retrieving user information from one place and transporting it to another place necessitates privacy protection. In this sense, it does not matter whether Mint is dealing with financial documents, attorney-client communications, or trade secret communications. There should be privacy protection for information transported through such an operational model.

In Part IV, both the government and the users have persuasive arguments on whether the users' consent to Mint's access defeats a reasonable expectation of privacy in user information. The court will likely decide for the government because users' consent to the User Agreement permits Mint to expose users' identifying information to public view. However, experts may disagree with this proposition, and finally, regardless of Mint's access specified in the User Agreement, the agreement should not be dispositive. Online user agreements are wrought with legal issues such as the lack of equal bargaining power and negotiation and inefficiency in time and costs. Most importantly, deciding constitutional issues based on online user agreements is clearly unsound and against the fabric of our society.

Advances in technology are mind-boggling and the law must keep pace with the technology. For now and for the sake of the future, I argue that the right course of action is to unambiguously extend cognizable privacy rights to user data stored in Mint, even if the data is used by Mint. The very reason of the pervasiveness of cloud computing is the convenience and low cost of having another party store or manage the users' computing power. It would bring the most promising and convenient social revolution in technology to a halt if users could not rely on data privacy stored online. Protecting privacy during transfers ensures that businesses are incentivized to develop ways that allow users to maximize the usefulness of information that is rightfully theirs. Finally, whatever user information Mint uses is anonymized and aggregated. Thus, if there is any forfeiture of privacy rights, it would be in the aggregated statistics and not the individually identifiable data.