The John Marshall Law Review

Volume 46 | Issue 1 Article 8

2012

Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege, 46 J. Marshall L. Rev. 383 (2012)

Timothy Peterson

CLOUDY WITH A CHANCE OF WAIVER: HOW CLOUD COMPUTING COMPLICATES THE ATTORNEY-CLIENT PRIVILEGE

TIMOTHY PETERSON*

I. INTRODUCTION

A. Cloudy Days Ahead

You have a choice. You can build a data control center, purchase a bunch of servers, purchase some industrial air conditioning units, and hire a team of Information Technology personnel to maintain the servers; or, you can pay $795.00 a year to get 350 gigabytes of cloud storage through Dropbox which can be expanded at $200.00 per 100 gigabytes.[1] The choice seems easy from a cost point of view, but, before a law firm moves to the cloud, the laws and rules surrounding the attorney-client privilege need to be more definite. People, including lawyers, are turning to cloud computing because of reduced costs, ease of use, and convenience. However, the law has not kept up with the adoption of cloud services.[2]

B. Heading to the Clouds

Part II explains the concept of cloud computing and what constitutes cloud computing. It examines the characteristics that distinguish cloud computing from older computing models, explores the benefits of cloud computing to lawyers, and considers a few examples of how a lawyer might use the cloud. Part II gives a brief history of the attorney-client privilege, the elements of the privilege, and waiver of the privilege. Part III examines the

* JD, The John Marshall Law School, 2013. I would like to thank Brent Ohlman, whose discussions inspired me to research cloud computing and the attorney-client privilege. I would also like to thank the editors and Editorial Board of *The John Marshall Law Review* for their tireless work on this Comment.

1. *Dropbox for Teams*, DROPBOX, http://www.dropbox.com/teams (last visited Oct. 15, 2012).

2. *See* Ilana R. Kattan, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 648-49 (2011) (arguing that courts' interpretations of the Stored Communications Act exclude communications stored in the cloud).

complications for the attorney-client privilege created by cloud computing, the deficiencies of the law in regard to the privilege and cloud computing, and proposals that might fix those deficiencies. Part IV proposes two possible solutions: amending the ABA model rules to allow the use of cloud computing or enacting statutes which will protect both lawyers and clients from inadvertent disclosure.

II. BACKGROUND

A. A New Concept and an Old Concept

This Part discusses what cloud computing is, why people want to use the cloud, and possible concerns raised by it. It then examines the history of the attorney-client privilege, how the privilege can be waived, and different approaches to implied waiver. Finally, this Part sets the stage for examining how the privilege complicates what would otherwise be clear advantages to utilizing cloud computing.

B. A Definition: What Is Cloud Computing?

The phrase "cloud computing" has made its way into the vernacular more and more as companies that offer cloud services seek to grow their customer base. However, there is a lot of uncertainty for the average person as to what constitutes cloud computing. This uncertainty is not surprising given the current state of cloud services and the ways in which cloud computing differs from older computing models. Many people use cloud services already, and may just not realize it (e.g., Gmail, Dropbox, iCloud, etc.).

Essentially, cloud computing allows users to store data and applications on remote servers owned by others.[3] The data and applications can then be accessed from anywhere the user has internet access, including on home computers, work computers, tablets, and smart phones.[4] While these are common

3. Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283, 287-92 (2010).

4. *Id.* at 283, 287-92. A great analogy for the basics of cloud computing is money. We can keep our money with us, at home (on our personal computer's hard drive) or we can deposit our money into a bank (cloud service) and have access to it whenever and wherever we need it (ATM machine, debit card, checks, and online transfers which are akin to a home computer, work computer, smart phone, and friend's computer). Robin Hastings, *Cloud Computing*, LIBR. TECH. REP., May 2009, at 10.

Cloud computing is also broken up into three areas, Software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), and infrastructure-as-a-service ("IaaS"). Martin, *supra* note 3, at 287.

SaaS provides applications through the internet, removing the need for

characteristics of cloud computing, there is no single definition with which everyone agrees.[5]

A definition is lacking for several reasons.[6] One reason is that cloud computing has involved contributions from people with various computing backgrounds who bring different perspectives to the cloud.[7] Another reason is that the technologies that make cloud computing possible continue to evolve.[8] A final reason is that

---

CD-ROMs or downloading software onto your computer. This is the most traditional form of cloud computing. *Id.* It is just an old, familiar idea (applications/software) in a new context. *Id.* Westlaw is one type of SaaS, which is comparable to an old Windows program called Encarta Encyclopedia. *Id.* Instead of the entries being stored on a CD or your hard drive like with Encarta, they are stored on servers owned by someone else (West, in this case) and accessed through the internet. *Id.*

PaaS provides servers connected to the cloud upon which a developer can create an application and make it available to users on the internet. *Id.* at 291. For the person who uses the application, there is no indication that a PaaS, such as salesforce.com, is hosting it on its servers. *Id.* So, a PaaS is often used to deliver a SaaS to a user. *Id.*

IaaS allows developers to have more control and flexibility over applications they create by providing only the servers and networks, and publishing to the internet while allowing the developers to designate the operating system and servers their application requires. *Id.* at 292-94.

5. *See* Diane J. Skiba, *Are You Computing in the Clouds? Understanding Cloud Computing*, 32 NURSING EDUC. PERSP. 266, 266 (2011) (reviewing several sources for definitions of cloud computing).

The definitions vary. One such definition is, "the delivery of scalable IT resources over the internet as opposed to hosting and operating those resources locally, such as on a college or university network." *Id.* Another is, "a networking solution in which everything from computing power to computing infrastructure, applications, business processes to personal collaboration—can be delivered to you as a service wherever and whenever you need." *Id.* Yet another defines cloud computing as "the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a services." *Id.* One last definition is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." *Id.*

See also Lizhe Wang et al., *Cloud Computing: A Perspective Study*, 28 NEW GENERATION COMPUTING 137, 139 (2010) (defining cloud computing as "a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and persuasive way").

For a more simplistic definition see Mark H. Wittow & Daniel J. Buller, *Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime*, 14 J. INTERNET L. 1, 4-5 (2010) (defining cloud computing as a metaphor for the internet and "when an Internet connection delivers hardware power and software functionality to users regardless of where they are or which computer they are using.").

6. Wang et al., *supra* note 5, at 138.

7. *Id.*

8. *Id.*

cloud computing is just now being used on a large scale.[9]

C. Why Would Anyone Use Cloud Computing?

Cloud computing offers many benefits for everyone. Using a cloud service reduces costs, as many provide free or inexpensive applications to users.[10] Cloud computing allows greater access to data and applications, increasing productivity.[11] Cloud computing also helps to preserve data in case of hardware failure.[12] By keeping everything in the cloud, a crashed hard drive, a dead computer, or the destruction of computing equipment does not strike the bone-chilling fear into a person that it once did.[13]

More specifically, lawyers and law firms can use services like Dropbox to back up data to the cloud and access it anywhere.[14]

---

9. *Id.* For example, Google recently released a new operating system "Chrome OS" that works almost entirely on the cloud. *Chromebook*, GOOGLE, http://www.google.com/chromebook/ (last visited Oct. 15, 2011).

10. Shellie Stephens, *Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20*, 2011 U. ILL. J.L. TECH. & POL'Y 237, 239. One of the best things for any business looking to use the cloud is scalability (economies of scale), which allows users to pay only for what they require, and quickly and easily increase the available resources if the need arises. Martin, *supra* note 3, at 294.

11. Stephens, *supra* note 10, at 239-40. Because applications and data in the cloud are accessed through the internet, they are compatible with multiple operating systems. *Id.* There are data backup applications that can sync folders on a MacBook, which are then available on Windows and other Apple computers through the internet, Android phones and tablets through the internet or an application, and an iPhone or iPad through the internet or an application. *Your Files, Anywhere*, DROPBOX, https://www.dropbox .com/features (last visited Oct. 15, 2012).

Having access to data and applications anywhere there is an internet connection can greatly increase productivity. Martin, *supra* note 3, at 294. A delayed or missed flight can turn into a few hours of work on an iPad or laptop. *Id.* There is also less time spent fixing or tinkering with the hardware or software because that is handled by the cloud service provider. *Id.*

The greater access and increased productivity has brought several companies, and several cities, to use the cloud every day. Stephens, *supra* note 10, at 240. Los Angeles and Seattle have adopted Google's cloud services, and the federal government began moving to the cloud in 2009. *Id.* at 240-41.

12. Stephens, *supra* note 10, at 239; Martin, *supra* note 3, at 294.

13. Martin, *supra* note 3, at 294. Because the data and applications are not dependent on the computer from which the user is working, any computer can be switched out with any other computer with no effect. *Id.* Accessing data from a crashed computer that was synced to the cloud is as easy as accessing the internet on any other computer. *Id.*

This does not mean there are no similar risks when using cloud services. *Id.* at 291. Because cloud service providers will use their own applications and operating systems in which data can be stored or applications built, a user may become locked in to that service despite any shortcomings. *Id.* There is also the risk that the cloud service provider will go out of business, leaving your data or applications inaccessible. *Id.*

14. *Your Files, Anywhere*, DROPBOX, https://www.dropbox.com/features

Client information, research, notes, and pictures can be organized and synced with the cloud through Evernote.[15] Similarly, using Westlaw Next, firms can organize cases, statutes, court rules, and other research into folders, all while highlighting and making notations.[16] This information is then accessible anywhere one can access Westlaw Next.[17] However, because this technology is new, it is uncertain how courts will apply the law to the cloud.

D. Statutes that Do Not Quite Fit the Cloud

The most pertinent statute governing electronic communications is the Stored Communications Act ("SCA"), a part of the Electronic Communications Privacy Act of 1986 ("ECPA").[18] With this act, Congress sought to ensure Fourth Amendment privacy rights to electronic communications.[19] The SCA covers two types of services: Electronic Communication Services ("ECS") and Remote Computing Services ("RCS"), both of which are usually

---

(last visited Oct. 15, 2012). Dropbox allows users to designate certain files or folders on their computer that will be automatically backed up to Dropbox's servers. *Id.* These files can then be accessed at any time, from any computer, smart phone, or tablet. *Id.* Dropbox also saves previous versions of documents in case you make a change that you no longer want. *Id.*

15. *Take Note of Anything*, EVERNOTE, http://www.evernote.com/about/learn_more/ (last visited Oct. 15, 2012). Evernote allows the user to clip articles, pictures, full webpages, and anything else that can be found on the internet or in your email inbox and save it to the Evernote servers. *Id.* Then, the user can organize these items into folders, with specific tags. *Id.* Notations, highlighting, editing, and drawings can all be made on the items that are clipped. *Id.* This allows a lawyer to take notes on an email sent by a client and link case law to that email. *Id.* Just like with Dropbox, things stored in Evernote can be accessed on any computer, smart phone, or tablet at any time. *Id.*

16. *Getting Started with Online Research Using Westlaw Next*, WESTLAW, http://west.thomson.com/promotions/e-mag/getting-started-WLN/index.html#/4/ (last visited Oct. 15, 2012).

17. *Id.*

18. Kattan, *supra* note 2, at 628. The Electronic Communications Privacy Act ("ECPA") deals more with hackers and government criminal investigations. Martin, *supra* note 3, at 305. The other major legislation in this area is the Computer Fraud and Abuse Act ("CFAA"). *Id.* at 308. The CFAA is directed at computer crime, including hacking and the sale of passwords to protected computers with the intent to defraud. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2008).

19. Kattan, *supra* note 2, at 628. The Act was also amended in 1994 and 1996. Martin, *supra* note 3, at 305. These amendments raised the standard for law enforcement officers to access data and heightened electronic privacy protections more broadly. *Id.*

Specifically, the SCA requires a warrant for police to search stored messages that have been in storage for 180 days or less. 18 U.S.C. § 2703(b). However, older messages may be searched with the mere production of an administrative subpoena, a grand jury subpoena, or a court order. *Id.*

provided by cloud service providers.[20]

Electronic Communication Services are "any service which provides to users thereof the ability to send or receive wire or electronic communications."[21] The problem comes from the definitions of electronic storage. The Department of Justice's definition only covers email stored on a server before being opened, but not after it is opened.[22] The other definition comes from the Ninth Circuit, finding that email on a server is in electronic storage, whether it is open or not. However, the court hinted, in dicta, that this did not apply to cloud email services because data "stored in the cloud [was] not stored for 'backup purposes.'"[23]

Remote Computing Services means offering "to the public [] computer storage or processing services by means of an electronic communications system."[24] To qualify as an RCS, a service provider must maintain the service on the user's behalf and must not have access to the user's information, other than to provide storage or computer processing.[25] This means that any service provider that accesses the user's information for advertising, as Google does, cannot be an RCS.[26]

E. Proposals for Fixing the Law

In 2010, Microsoft introduced the Cloud Computing Advancement Act, part of which seeks privacy modifications to the ECPA.[27] This includes abandoning the distinction between ECS and RCS, because they no longer fit the technology.[28] Microsoft

20. Kattan, *supra* note 2, at 632.

21. 18 U.S.C. § 2510(15) (2012). The statute covers more than just computer messages. Any message that is at least partly transmitted through "a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ." but does not cover electronic bank transfers or tone-only pagers. § 2510(12).

22. Kattan, *supra* note 2, at 633.

23. *Id.* at 633-35.

24. 18 U.S.C. § 2711(2) (2012).

25. 18 U.S.C. § 2703(b)(2)(B) (2012).

26. Kattan, *supra* note 2, at 639. It seems unlikely a company like Google would stop accessing user data. Google gives away free cloud storage because it makes a lot of money from advertisements.

27. Martin, *supra* note 3, at 309.

28. *Id.* In addition to its legislative offerings, Microsoft has also proposed industry standards that make the infrastructure and security cloud service providers offer more accessible and easier to understand information for end users so they can make a more informed decision. *Id.* IBM has introduced another industry proposal it calls the "Open Cloud Manifesto." *Id.* at 310. IBM also calls on greater transparency and consistency among cloud providers so that consumers can make an informed choice. *Id.* However, IBM seeks solutions that will not inhibit innovation. *Id.* Despite some of the commonalities, Microsoft has refused to join the Open Cloud Manifesto because it is seen as too vague and unrepresentative of Microsoft's interests. *Id.* Another major cloud service provider, Amazon, has also refused to join. *Id.* There are also legislative barriers to amending the SCA. *See* William Jeremy

also proposed a federal law that allows users to control what data could be collected about them, online and offline.[29] This would allow a law firm to opt out of having its data collected by a cloud service provider, or to at least prevent the collection of privileged data.[30]

F. Why Lawyers Should Not Use the Cloud: The Risks

While there are many benefits to cloud computing, it has also created new problems. There are multiple concerns involving the legal field, as well as more general privacy concerns. In traditional computing models, the users have had more control over their data.[31] One of the key characteristics of cloud computing is that the user's data is stored on servers and networks they do not own, taking management and protection of the hardware out of the hands of the user and placing it in the hands of the cloud service provider.[32] The user must trust what the cloud service provider says about how it protects the user's privacy.[33]

Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO L.J. 1195, 1234-35 (2010) (arguing that the SCA's privacy protections are already close to what Congress would intend, even though the definitions no longer fit, and that Congress has taken steps toward reducing privacy since September 11, 2001).

29. Martin, *supra* note 3, at 309.

30. Solutions have come in non-legislative form as well. One company, SpiderOak, has employed a new model for terms of service. It provides a similar service to cloud backup and storage of files, but its employees do not and cannot have access to a user's data. *Welcome to SpiderOak Help*, SPIDEROAK, *https://spideroak.com/faq/* (last visited Oct. 22, 2012) [hereinafter SpiderOak FAQ]. The only information available to SpiderOak is how many bites of encrypted data a user is using and this information is only used for billing purposes. *Id.* Instead of a user agreement, users agree to a "Password Policy" stating that users are solely responsible for remembering their passwords, and SpiderOak provides no password recovery because it does not store passwords. *Id.* The benefit of this "zero-knowledge" model is that there are limited concerns about implied waiver because the data stored with SpiderOak is not accessible by the service provider or any other third party. The downside is that people can be forgetful and forgetting passwords makes the data inaccessible. SpiderOak does allow users to create a hint that might remind them of what their password is if they do happen to forget it. *Id.*

31. Wittow & Buller, *supra* note 5, at 6.

32. *Id.*; Martin, *supra* note 3, at 289.

33. Wittow & Buller, *supra* note 5, at 6. Trusting a cloud service provider can be dangerous. In 2009, the Electronic Privacy Information Center filed a complaint with the Federal Trade Commission alleging that Google, one of the largest cloud service providers, did not provide adequate safeguards for confidential information it collected through services like Gmail. *Id.*

However, in July 2010, Google received Federal Information Security Management Act (FISMA) compliance for establishing security standards to protect the information it gathers. David J. Goldstone & Daniel B. Reagan, *Social Networking, Mobile Devices, and the Cloud: The Newest Frontiers of Privacy Law*, 55 BOS. BAR J. 17, 18 (2011). Google was the first cloud service

In addition to the lack of control over hardware, there is also the risk of hackers, data leaks, and the interception of data being transferred to the cloud.[34] However, these risks are inherent in any computing model involving the internet.[35] There is no real solution that will work in every situation.[36]

Regarding legal issues, cloud computing may also open up personal jurisdiction to more courts than a person or company anticipated.[37] Because of the way cloud services work, a user's data could be almost anywhere in the world, and possibly in multiple places, subject to the laws of multiple jurisdictions.[38] Using a cloud service provider can also lead to questions of who is liable when a mistake happens.[39] There are also concerns about which nation's laws govern data in the cloud.[40] Additionally, cloud

---

provider to achieve FISMA compliance. *Id.*

34. Martin, *supra* note 3, at 298.

35. *Id.* Many people also voluntarily put private information into the cloud, such as on Facebook profiles. Because people are not always careful, information that a user would like to keep secret can make its way into someone else's hands. For example, the federal government has instructed investigators to collect information from social networking sites that might reveal location, motives, relationships, or the existence of a crime. Goldstone & Reagan, *supra* note 33, at 18.

36. Martin, *supra* note 3, 298.

37. Fernando M. Pinguelo & Bradford W. Muller, *Avoid the Rainy Day: Survey of U.S. Cloud Computing Caselaw*, 2011 B.C. INTELL. PROP. & TECH. F. 1, 2. The case of *Forward Foods LLC v. Next Proteins, Inc.* involved a company which used a cloud service to create a "virtual data room" that allowed other companies to download documents with the appropriate password. Forward Foods LLC v. Next Proteins, Inc., No. 603892-2007, 2008 WL 4602345, at *1 (N.Y. Sup. Ct. Oct. 15, 2008). Because one of the litigants had accessed this data room at its New York Office with a password given to it by Next Proteins, the New York court held that there were sufficient minimum contacts with the state for the court to exercise personal jurisdiction over the defendant. *Id.* at *3.

However, companies and individuals would probably still be able to rely on the doctrine of forum non conveniens to protect against lawsuits in "far-off jurisdictions." Pinguelo & Muller, *supra*, at 4.

38. Matthew A. Verga, *Cloudburst: What Does Cloud Computing Mean to Lawyers?*, 5 J. LEGAL TECH. RISK MGMT. 41, 46 (2010). For example, data stored in the United States might be subject to laws such as the Health Insurance Portability and Accountability Act of 1996. *Id.* If stored in the European Union, the data may be subject to the EU's more stringent privacy regulations. *Id.* Finally, any data stored outside of the United States may be subject to a U.S. prohibition on exporting certain types of data. *Id.*

39. Andrew C. DeVore, *Cloud Computing Privacy Storm on the Horizon?*, 20 ALB. L.J. SCI. & TECH. 365, 369 (2010). Someone who uses a cloud service provider to build an application does not control the servers or network used to make that application available. *Id.* If the hardware were to fail and allow some cause of action to arise, it is unclear to what extent a cloud service provider might be held responsible. *Id.* The person using the cloud service provider is at its mercy if a mistake is made. *Id.*

40. *See* Verga, *supra* note 38, at 46 (describing the question of "[i]n what geographic location is the data?" to be one of the most difficult questions to

service providers may allow access by certain employees, or may potentially share some of the information with third-party organizations for various purposes, including advertising.[41]

There is also uncertainty about which U.S. laws apply to data in the cloud. The statute which governs cloud computing is the Stored Communications Act ("SCA") which is part of the Electronic Communications Privacy Act ("ECPA")–but, this statute is more than twenty years old.[42] It is also uncertain whether this law applies to data in the cloud given that courts have had to redefine "communication" with subsequent advances in technology.[43]

While cloud computing raises these potential issues, concerns over new technology, especially in the legal field, have always been around.[44] In 1997, there was still concern about the use of email by law firms and the risks inherent in doing so.[45] Seemingly, lawyers

---

answer in regards to cloud computing).

41. *Id.* at 47. Cloud computing is not the first technology where third party access to electronic communications has been an issue. *See* Sherry L. Talton, *Mapping the Information Superhighway: Electronic Mail and the Inadvertent Disclosure of Confidential Information*, 20 REV. LITIG. 271, 281-85 (2000) (finding that the concerns of unauthorized access to email is greatly limited by encryption).

42. Robinson, *supra* note *28*, at 1196.

43. Martin, *supra* note 3, at 305-06.

44. *See generally* Joe Dysart, *The Trouble with Terabytes: As Bulging Client Data Heads for the Cloud, Law Firms Ready for a Storm*, A.B.A. J., Apr. 2011, at 32 (finding that neither businesses nor lawyers are prepared for a coming wave of e-discovery requests and litigation involving cloud services). This becomes even more complicated when cell phones are added to the mix. Luckily, there are programs that will capture a "forensic image of a mobile phone" such as EnCase Neutrino developed by Guidance Software. *Id.* at 35. There are also applications, such as the open source Prey Project and Lookout, which can remotely wipe phones, display the phone's location, and lock the phone to prevent further use unless a password is provided. PREY, http://www.preyproject.com (last visited October 15, 2012).

However, cloud computing, especially cloud backup services, can make discovery easier. J. Mark Jones & John D. Martin, *Electronic Discovery—Developing Solutions to New and Complex Challenges*, S.C. LAW. May 2004, at 15, 18. Traditional computer backup systems were designed for disaster recovery, not for retrieving certain specific documents. *Id.* If somehow a company's computers were destroyed or the hard drive crashed, the company would simply want to restore all of the data. *Id.* This is the scenario for which traditional computer backup systems were made. *Id.*

Cloud services make it much easier to retrieve single specific documents. Google documents, for example, uses Google's powerful search engine to search your documents.

45. Jonathan Rose, *E-Mail Security Risks: Taking Hacks at the Attorney-Client Privilege*, 23 RUTGERS COMPUTER & TECH. L.J. 179, 225 (1997) (suggesting that law firms "err on the side of caution" when communicating with clients via email). As cloud computing becomes more secure and better understood, it seems likely that it will become as commonplace in law firms as email is today. When Rose's article was written, the law firms he surveyed were very cautious with emails. *Id.* at 222-25. These firms used private

will always be somewhat slow adopters of new technologies, at least until they are better understood, and the courts, legislatures, and rule makers have given some guidance on their proper use.[46] This is because lawyers have a higher duty of confidentiality than the general public in the form of the attorney-client privilege.

G. The Attorney-Client Privilege

The attorney-client privilege is a foundational principle of the legal profession. The privilege protects communications between an attorney and his client, or potential client, so long as the communications do not further a crime and are kept confidential by both parties.[47] This protection is often viewed as an impediment to the search for truth, bringing some courts to construe the privilege narrowly and find implied waiver for a broad spectrum of conduct.[48]

H. History and the Present Trends

The roots of the attorney-client privilege date back to Roman law.[49] Originally, the privilege belonged to the attorney, but, by

---

networks, email encryption, required clients to use the same service provider as the firm, or forbade confidential information from being transmitted between attorneys and clients via email. *Id.*

46. Talton, *supra* note 41, at 297. The advantages of email were seen as so great for the legal community that the law and old legal concepts needed to be reshaped to accommodate email use by law firms. *Id.*

The advantages of cloud computing can be even greater than those of email because it allows a small firm or solo practitioner to access the same state of the art technology as a large firm. Stephens, *supra* note 10, at 239-40. One of the biggest burdens to the widespread adoption of cloud computing in the legal field is the uncertainty about the laws governing the cloud. Kattan, *supra* note 2, at 632-37. This uncertainty and its role in complicating the attorney-client privilege will be discussed in Part II.

The law governing cloud computing is the Stored Communications Act, which is part of the Electronic Communications Privacy Act. Robinson, *supra* note 28, at 1196. This law was passed over twenty years ago. *Id.* With technology changing as quickly as it does, a twenty year old law seems completely deficient for governing the technology of today.

For another perspective on regulation of cloud service providers see Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1811, 1818 (2011) (arguing that the federal government and the FCC should begin to view cloud service providers more as public utilities and use regulations based on public utility regulations to protect the end-user's privacy).

47. Ken M. Zeidner, *Inadvertent Disclosure and the Attorney-Client Privilege: Looking to the Work-Product Doctrine for Guidance*, 22 CARDOZO L. REV. 1315, 1315 (2001). The privilege is a rule of evidence. *Id.* It prevents discovery and admission at trial of communications between the attorney and his client. *Id.* This is meant to promote open communication with the attorney so the best legal advice can be given. *Id.*

48. *Id.* at 1315-16.

49. *Id.* at 1320.

the eighteenth century, ownership transferred to the client.[50] In England, the privilege originally belonged, not only to lawyers, but to all members of the English ruling class.[51] The scope was also much narrower, applying only to a lawyer testifying during litigation and not to legal advice or drafting documents.[52] As English laws changed to make parties competent witnesses, the privilege expanded to cover their testimony as well.[53] The privilege was once again expanded when company documents and records were allowed admission as an exception to the hearsay exclusion.[54] The privilege continues to expand to this day.[55]

Presently, the attorney-client privilege remains the property of the client.[56] The privilege is considered substantive, rather than procedural law.[57] This means that a federal court sitting in diversity will determine the attorney-client privilege according to the law of the state where it sits.[58]

Generally, there are four elements required to establish the privilege.[59] The party claiming the privilege must show that there was: "(1) a communication; (2) made between privileged persons; (3) in confidence; and (4) for the purpose of obtaining or providing legal assistance to the client.[60] Once the privilege has been

---

50. *Id.* at 1320-21. In England, the theory behind the privilege belonging to the attorney was to "protect[] the honor of the legal advisor as a gentleman." *Id.* Ownership was subsequently given to the client based on a new rationale for continuing the privilege. *Id.* The client needed "freedom of action when dealing with his attorney." *Id.*

51. 24 CHARLES ALAN WRIGHT ET AL., FED. PRACTICE & PROCEDURE § 5472 (1st ed. 2012).

52. *Id.*

53. *Id.*

54. *Id.* Corporations wanted to help protect documents that were adverse to their positions from being used against them, so they began to frame them as communications with legal counsel. *Id.*

55. *See id.* (citing Upjohn Co. v. U.S., 449 U.S. 383, 395 (1981), which found the privilege to apply to employees who are not part of the corporation's control group).

For a more complete history of see WRIGHT ET AL., *supra* note 51 (discussing the various historical perspectives on the attorney-client privilege).

56. Zeidner, *supra* note 47, at 1321.

57. *Id.* This has implications for conflicts of law problems. However, this discussion is beyond the scope of this Comment. For a discussion of the attorney-client privilege in international law see Helena M. Tavares, *The United States Perspective on Travelling with the Attorney-Client Privilege: Checked or Carry-on Baggage*, 7 INT'L L. PRACTICUM 9 (1994) (finding that U.S. courts have tended to favor applying the U.S. version of the attorney-client privilege when there are sufficient contacts to justify applying U.S. law, but readily admit evidence covered only by a foreign version of the privilege).

58. Zeidner, *supra* note 47, at 1321.

59. *Id.* at 1323.

60. *Id.* These elements generally do not cover third parties who are present when the communication is made. Tavares, *supra* note 57, at 11. The presence of a third party can constitute grounds for waiver of the privilege. *Id.*

established, it can only be broken through waiver."[61]

I. Waiving the Attorney-Client Privilege

There are two ways that the attorney-client privilege can be waived: explicitly or implicitly.[62] Explicit waiver merely requires intent to no longer have the communications be privileged.[63] Implicit waiver can be more difficult to prove. Generally, waiver is implied when the party's conduct is inconsistent with the elements of the attorney-client privilege.[64] For purposes of this Comment, the most important way the privilege can be implicitly waived is through disclosure of the information to a non-essential party.[65]

J. Approaches to Implied Waiver

The courts have taken three different approaches to finding implied waiver.[66] The first approach is the strict liability approach, where any inadvertent disclosure constitutes waiver.[67] Any mistake, no matter how innocent, will waive the privilege.[68]

The second approach is the subjective intent approach, which requires intent to waive before waiver can be found.[69] This means that an inadvertent disclosure can never result in waiver.[70] This approach follows the constitutional approach to waiver.[71]

However, third parties will be protected if they are essential to the advice being given, that is, they "ha[ve] a common interest with the client in the matter." *Id.*

61. Zeidner, *supra* note 47, at 1331.

62. *Id.* at 1331-32.

63. *Id.* at 1331.

64. *Id.* at 1331-32. For example, the privilege has been found implicitly waived when a party places select material into evidence (waiver regarding "any withheld communications relating to the same subject matter[]"), or when a party places privileged communications at issue in litigation (plenary guardian seeking to void trust amendments). *Id.* at 1332.

65. *Id.* at 1333.

66. *Id.* at 1336.

67. *Id.* at 1336-37.

68. *Id.* at 1340. Courts that use this method justify it as encouraging attorneys to be more diligent in document production by the threat of a malpractice suit. *Id.*. Not all commentators are convinced that this approach actually achieves the stated goal. *See id.* at 1340-42. (arguing that the threat of a malpractice suit is quite low and the discovery process has an inherent threat of inadvertent disclosure).

69. *Id.* at 1343.

70. *Id.* Just like the strict-liability approach, the subjective-intent approach is simple and easy to apply. *Id.* at 1344. However, it ignores characteristics about the law and the attorney-client relationship. *Id.* If a lawyer makes a mistake, the client will suffer the consequences. *Id.* There does not seem to be a justification for treating inadvertent disclosure of privileged materials differently. *Id.* at 1345.

71. *Id.* Zeidner points out that the seminal case for the subjective-intent approach, Mendenhall v. Barber-Greene Co., 531 F. Supp. 951 (N.D. Ill. 1982)

The third approach is the circumstances approach, where the court examines five factors to determine if there has been waiver.[72] The factors the court looks at are "the reasonableness of the precautions to prevent inadvertent disclosure, the time taken to rectify the error, the scope of the discovery, and the extent of the disclosure," as well as overall fairness.[73] Of all the approaches, the first and third implicate the cloud most strongly.

K. New Technology and Implied Waiver

Cloud computing is such a new concept that there is currently no case law discussing its involvement with the attorney-client privilege. There are, however, cases involving other newer technologies and a person's interest in privacy which can be used to inform a discussion on cloud computing and the attorney-client privilege.[74] As technology has advanced, it has mainly been left to the courts to apply existing statutes to the new technology—often

---

misinterpreted the case it relied upon, Johnson v. Zerbst, 304 U.S. 458 (1938). *Johnson* is only applicable when dealing with constitutional rights. Zeidner, *supra* note 47, at 1345. However, the attorney-client privilege is not a constitutional right, but instead flows from statutes or common law. *Id.* at 1321.

72. *Id.* at 1348-49.

73. *Id.* at 1349. This approach also has drawbacks as the factors do not give much guidance to parties beforehand to know what is reasonable. Lawyers will not know what they need and need not do. This creates a system of ad hoc determinations of when the privilege has been waived. The lack of direction and clear standards encourages litigation of all disputes involving potential inadvertent disclosure. *Id.* at 1351-54.

Zeidner offers a new approach based on the attorney work-product doctrine. Essentially, when an inadvertent disclosure has been made, there would be a presumption that the attorney-client privilege has not been waived, but the opposing party would be able to rebut that presumption by showing a "substantial need" of the disclosed materials. *Id.* at 1356. Then the party will have to show that a "substantial equivalent" cannot be obtained without undue hardship. *Id.*

Another approach is suggested by Roberta M. Harding. She suggests that whether the disclosure was intentional or inadvertent should not play a role in deciding waiver. Roberta M. Harding, *"Show and Tell": An Analysis of the Scope of the Attorney-Client Waiver Standards*, 14 REV. LITIG. 367, 410 (1995). Instead, the court should decide whether, due to the disclosure, "the disclosing party is placed in a significantly better situation than its opponent." *Id.* The court would examine all documents disclosed and other privileged materials on the same subject matter, narrowly defined, to determine if unfairness has resulted. *Id.* If it has, the court should find that the privilege has been waived for all documents relating to the same subject matter. *Id.*

74. *See, e.g.*, U.S. v. Warshak, 631 F.3d 266, 282-89 (6th Cir. 2010) (discussing email and the Stored Communications Act); Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other grounds*, 130 S. Ct. 2619 (2010) (finding a reasonable expectation of privacy in text messages).

causing circuit splits.[75] This is even more difficult when the governing law is not amended to reflect the technology.[76] With the state of the law governing the cloud unclear and lacking, lawyers must watch for potential implied waiver concerns when using the cloud.

III. ANALYSIS

A. Complicating the Matter

This Part describes how using the cloud complicates the attorney-client privilege and how cases have already addressed similar issues with other technologies. These cases will then be used to examine how a court might rule on an implied waiver claim. Ultimately, it concludes that, while a strong argument could be made for each side, features of certain, usually free and popular, cloud services will prevent courts from finding a reasonable expectation of privacy in cloud services.

B. How Cloud Computing Complicates the Attorney-Client Privilege

Use of cloud services poses a great risk of disclosure of privileged material to non-essential third parties due to the terms of service to which a user must agree.[77] Because cloud computing is a new technology, the law has not yet adapted to the special needs of cloud computing.[78] To remedy this, cloud service providers have used contractual terms of service to govern the service provider's and the end user's responsibilities.[79]

Cloud service providers collect information in various ways. Google, one of the largest cloud service providers, is primarily an advertising company that uses cloud services to deploy advertisements in a targeted way.[80] Starting in 2004, Google introduced automated scanning into Gmail, searching for key words to detect viruses and spam, and to provide more targeted advertisements to the user.[81] Although it says that it collects data, Dropbox does not collect data itself—it actually opens your data to

75. Martin, *supra* note 3, at 305-06 (discussing a split in authority regarding whether copying email constitutes interception of a communication).

76. *Id.* at 305 (noting the amendments to the ECPA have been aimed at raising the standard on law enforcement access to electronic data).

77. Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593, 593 (2010).

78. *Id.*

79. *Id.*

80. *Id.* at 600.

81. *Id.*

others.[82] Dropbox uses third parties to help improve and maintain various parts of its service, and these companies can be given access to your data.[83] Dropbox also reserves the right to disclose your information "to protect Dropbox's property rights."[84] All of these data access policies are agreed to by the end user during initial signup as a requirement for use of the service.[85] The majority of the data that these services collect are voluntarily given to them by the user.[86]

Despite the amount of information they collect, cloud service providers have been responsive to their users' privacy concerns. Cloud service providers have slowly introduced better privacy and security measures as a way to draw more customers, especially those who have felt uneasy about the reliability and privacy the cloud can offer.[87] However, they have not been so quick to adopt larger changes, such as encryption of stored data.[88] Substantial progress has been made regarding openness to the end user about how the service provider can access or use the data.[89]

This advancement acts as a double-edged sword for attorneys. While it is now easier to know the services that access your data

---

82. *Dropbox Privacy Policy*, DROPBOX, https://www.dropbox.com/privacy (last visited Oct. 15, 2012).

83. *Id.*

84. *Id.*

85. Stylianou, *supra* note 77, at 604.

86. *Id.*

87. *Id.* at 608-09. A larger concern for the individual user is security measures taken against hackers or the government accessing private information. *Id.* at 606. These areas have been the focus of much of scholarly legal writing about cloud computing. *See, e.g.,* David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2232-38 (2009) (arguing that courts should extend Fourth Amendment privacy rights to cloud services and find cloud service providers to be more like landlords in reference to the storage space); Wittow & Buller, *supra* note 5, at 9 (expecting new claims to arise in the coming years due to cloud computing such as "insider theft" and hackers). Cloud service providers are a bountiful target for hackers because data for numerous users is stored in one place. DeVore, *supra* note 39, at 369. However, hackers are of little concern for this Comment because data accessed by a hacker would not constitute a disclosure, it being more akin to theft.

There are also possible liability issues if a cloud service provider makes a mistake. A Microsoft subsidiary had a server crash that caused everyone with a T-Mobile Sidekick phone to lose their information. *Id.* Google made an error that allowed users to access other user's documents without authorization. *Id.* A study from 2008 found that 88% of data breaches were due to "insider negligence," which shows that the threat is very real, and litigation in this area is likely to increase as more people put their data into the cloud. *Id.* at 368. These risks may be the reason the U.S. government decided not to keep classified or sensitive data in the cloud. *Id.*

88. Stylianou, *supra* note 77, at 609.

89. *Id.*

and for what purpose they do so, lawyers are now on notice that data can be accessed by non-essential third parties.[90] A lack of attention to a cloud service provider's terms of service could easily result in an implied waiver of the attorney-client privilege.[91]

C. Cases that Inform a Cloud Computing Analysis: Employer Policies and Expectations of Privacy

It should come as no surprise, given the novelty of the cloud, that there are no cases involving the cloud and the attorney-client privilege. However, there are cases involving circumstances similar to those created by cloud computing that will form the basis of this analysis.

In *Stengart v. Loving Care Agency, Inc.*,[92] an employee communicated with her attorney through her personal email account, but used an employer-issued computer to do so.[93] The employee sued her former employer for "constructive discharge" due to a "hostile work environment [and] harassment due to her gender, religion, and national origin."[94] Her employer had provided the employee with a computer to use for work-related purposes.[95] The computer was equipped with internet access.[96] The laptop was also, unbeknownst to the employee, equipped with a program that captured a picture of every website she visited, including her password protected personal email account.[97] It was through this email account that she contacted her lawyer about her situation at work.[98] When she left her employment, she returned the laptop to the company, because it was their property.[99] The employer was later able to retrieve several of these emails stored on the computer.[100] It was the employer's policy that it could access any records, email, voicemail, or internet communications, because they were considered the business records of the company.[101]

---

90. *Id.*

91. It is important to keep in mind the test of the state in which the attorney is practicing. For instance, in Illinois, the courts apply the subjective-intent test. People v. Murry, 711 N.E.2d 1230, 1235 (Ill. App. 1999). There can be no waiver in Illinois without intent to waive the privilege. *Id.* Therefore, implied waiver does not exist in Illinois and lawyers in states with similar methodologies should be more open to use of cloud services.

92. Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

93. *Id.* at 655.

94. *Id.* at 656.

95. *Id.* at 655.

96. *Id.*

97. *Id.* at 655-56.

98. *Id.* at 656.

99. *Id.*

100. *Id.*

101. *Id.* at 657.

To determine whether the privilege had been waived as to the emails the company retrieved, the court had to decide whether the employee had a "reasonable expectation of privacy" in using her personal email on her work computer.[102] To make this determination, the court looked at the company's policy about computer use; monitoring computer use; the right of access to the computer and emails by third parties; and notification to the employee about those policies.[103] The court also found it pertinent that the employee took steps to secure the privacy of her emails by using a password protected account, instead of her company email, and by not storing her password on the company's computer.[104] The court found that the privilege had not been waived because the employee sought to maintain privacy and the company's policy was too vague to adequately warn of what would or would not be monitored.[105]

This case can be used to analyze a hypothetical case involving cloud computing. In *Stengart*, the employee used a service that stored her information on a hard drive which belonged to someone else and to which the owner of the hard drive had access. One of the key components of cloud computing is that the user's data is stored remotely, on servers owned by someone else.[106] As discussed above, many cloud service providers have access to the information stored on their servers through contractual terms of service to which the user must agree.[107] A court could then consider whether the employee has a reasonable expectation of privacy in the cloud service. That determination could be based on the terms of service,

---

102. *Id.* at 660.

103. *Id.* at 662 (quoting In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)) (internal citations omitted).

104. *Id.* at 665.

105. *Id.* The pertinent text of the company's policy on its computers and email use was as follows:

> The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice.
>
> ****
>
> E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.
>
> The principal purpose of electronic mail (e-mail) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

Id. at 657 (ellipses in original).

106. Martin, *supra* note 3, at 283, 287-92.

107. Stylianou, *supra* note 77, at 609.

the monitoring by the service provider, the right of third parties to access the information, the notification to the user, and the attempts the user made to keep the information private, such as encryption.[108]

One strike against finding a reasonable expectation of privacy would be the increased openness and clarity with which service providers are making their privacy terms available to the user.[109] If a service provider is very clear about their ability or a third party's ability to access the information, privacy expectations should clearly be diminished.

While the *Stengart* court did not go into much detail, it did note that the reasonable expectation of privacy is derived from Fourth Amendment search and seizure jurisprudence.[110] Criminal law requires that the target of a search has manifested a subjective expectation that the object sought would remain private, as well as a societal recognition that the target's belief was reasonable.[111] It seems less reasonable that, faced with the

---

108. These would be analogous to the employer's policy regarding company computers and email; the employer's right to access the information on those computers; notification to the employee about the employer's policy and access rights; and steps taken to keep emails private, such as password protection and not storing the password on the computer. *Stengart*, 990 A.2d at 662. It is important to note that no court has made these claims, but these seem like the factors a court would take into consideration—should a cloud computing case arise.

109. Stylianou, *supra* note 77, at 609.

110. *Stengart*, 990 A.2d at 660. The most famous case applying the Fourth Amendment in technology is *Katz v. United States*. Katz v. U.S., 389 U.S. 347 (1967). In this case, the FBI placed a listening device on a telephone booth and recorded statements made by the defendant, which were later used at trial over Katz's objection. *Id.* at 348. The Supreme Court held that the FBI had violated the Fourth Amendment and reversed Katz's conviction. *Id.* at 359.

In addition to the Court's holding, Justice Harlan, in concurrence, found that Katz had a reasonable expectation of privacy when using the phone booth. *Id.* at 360-61 (Harlan, J., concurring).

111. *Warshak*, 631 F.3d at 284. This case involved the owner of the company which produced and sold a "male-enhancement" drug called Enzyte. *Id.* at 276. To boost sales, the company offered a free sample, but automatically enrolled the customer in a monthly shipping program without informing them. *Id.* at 277-78. After numerous complaints, the company enacted a mandatory disclosure, which "was not always read, and it was designed not to work." *Id.* at 278.

As the company grew and outsourced its call center, customers were actually informed of the program and declined enrollment 80% of the time. *Id.* at 278-79. Warshak then ordered all customers, even those who declined enrollment, to be added to the auto-ship program. *Id.*

Customers began disputing the auto-ship charges at such a high rate that it threatened the company's bank accounts and ability to accept credit cards as payment. *Id.* at 279-80. To avoid this, Warshak ordered transactions be split into two, and later three so there would be a lower percentage of disputed charges. *Id.* at 280.

In 2006, Warshak and several others were indicted for conspiracy to

clear terms of service of some service providers, an attorney would have a reasonable expectation of privacy when placing data in the cloud.[112]

That is not to say a court could not find a reasonable expectation of privacy in a cloud service. In another case involving new technology, one court found a reasonable expectation of privacy in text messages.[113] In *Quon v. Arch Wireless Operating Co.*,[114] the Ninth Circuit found that, while the wireless phone carrier may have been able to view the contents of text messages "for its own purposes," this was irrelevant to whether the owner of the phone had a reasonable expectation of privacy in those text messages.[115] The court analogized text messages to email and letters, finding that nobody would have a reasonable expectation of privacy in the identity of the person the communication was sent, but would have a reasonable expectation of privacy regarding the

---

commit mail, wire, and bank fraud, mail fraud, making false statements to banks, bank fraud, money laundering, and obstruction of a Federal Trade Commission proceeding, amongst other charges. *Id.* at 281.

As part of the investigation and prosecution, the U.S. government obtained "thousands of emails" from Warshak's internet service provider, which Warshak unsuccessfully attempted to suppress. *Id.*

The defendants were convicted on most of the charges and Warshak appealed the use of the emails at trial. *Id.* at 281-82. The Sixth Circuit found that the government did violate Warshak's Fourth Amendment rights in obtaining the emails, but declined to reverse because the government had relied on the Stored Communications Act in good faith. *Id.* at 282.

However, not all email has been treated equally. An Illinois appellate court found that accessing cloud-based email through the internet was sufficiently different than accessing traditional email and does not enjoy the same privacy protections as traditional email. Kattan, *supra* note 2, at 635.

112. *See* U.S. v. Miller, 425 U.S. 435, 442-43 (1976) (holding there was no reasonable expectation of privacy to the contents of information voluntarily given to a bank to conduct bank business). However, it should be noted that this has not gone unchallenged. In *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit found that as a matter of law, there was a reasonable expectation of privacy in the contents of text messages. *Quon*, 529 F.3d at 905.

It is also worth noting that the court, in this case, looked to other technologies, such as telephones, letters, and emails. *Id.* at 905-06. When cloud computing cases come before the courts, they will be required to make similar analogies to older technology, which will now include text messages.

There has also been a split as to whether users of Google's Gmail service have a reasonable expectation of privacy to their emails. *See* In re U.S., 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) (holding no reasonable expectation of privacy because of Google's clear terms of service allowing it to access user's emails for advertising purposes); *but see* U.S. v. Cioffi, 668 F. Supp. 2d 385 (E.D.N.Y. 2009) (noting that the government did not dispute that the defendant had a reasonable expectation of privacy in his personal Gmail account).

113. *Quon*, 529 F.3d at 907, *rev'd on other grounds*, 130 U.S. 2619 (2010).

114. *Quon*, 529 F.3d 892.

115. *Id.* at 905.

contents of the message.[116]

This case can also be used to examine a case involving cloud computing. While many of these services have access to the information stored on their servers, that access is generally limited to maintenance and billing.[117] This type of access, like the access in *Quon*, is merely for the service provider's "own purposes" (maintenance, billing, etc.) and it is reasonable to think they would not disseminate the information.[118]

However, the *Quon* court also found it significant that the wireless company was not actively monitoring or auditing the contents of the text messages.[119] This is problematic for any of the free cloud service providers, like Google, who actively access the contents of communications for advertising and other purposes.[120] As long as advertising is how these services make their money, they will have an incentive to tailor the advertisements their customers view to those customer's interests based on the content of their data.[121]

IV. PROPOSAL

While caution is usually the best policy for lawyers when it comes to new technology, the benefits of cloud computing makes cloud services tempting for any business.[122] That is why a multi-faceted solution is the best way to bring the benefits of cloud computing to the legal field.[123]

---

116. *Id.*

117. *Dropbox Privacy Policy*, DROPBOX, https://www.dropbox.com/privacy (last visited Oct. 15, 2012).

118. *Quon*, 529 F.3d at 905.

119. *Id.* at 906.

120. Kattan, *supra* note 2 (explaining that Google makes most of its money through advertisements); *see also* Stylianou, *supra* note 77, at 593, 600 (discussing why Google scans the text of communications).

121. See Stylianou, *supra* note 77, at 593, 600 (noting that Google not only scans messages for advertising purposes, but also to detect spam and viruses).

122. As the internet generations begin to fill the ranks of the legal profession, this tendency toward caution might become more difficult. The generations who have grown up their whole lives with the use of the internet will be much more apt to learn new technologies and seek to use them in the practice of law. Either the legal profession will need to address new technologies more quickly in the future, or the internet generations will have to curb their enthusiasm and ability to adapt to new technologies. The latter seems more likely, as the legal profession has thus far maintained a high level of caution.

Technologies that allow lawyers to be more efficient and reduce costs, like cloud computing, will be even more tempting to adopt before the law has adapted to them.

123. This does not necessarily mean that lawyers should avoid cloud computing entirely, although the ultra cautious lawyer may follow this route. For example, cases an attorney cites to often can be stored in the cloud to be referenced wherever the attorney may be working, allowing the cloud to be

Legislation of some sort would be the best way of protecting information in the cloud. Microsoft has already proposed possible legislation that is much broader than a lawyer's professional concerns. However, because of the expansive reach of some of the terms of the proposed legislation, there are better options. Another possible solution would be to amend the American Bar Association's Model Rules. Finally, in some circumstances, it would be more desirable to lobby legislatures for more cloud- or lawyer-specific protections.

Because the legislative and rule-making process can be long and cumbersome, lawyers should not wait for these significant changes to take place before taking advantage of cloud services. However, for purposes of clarity, stability, and uniformity of the law, there must be legislation, and rules of professional responsibility must be adopted regarding cloud computing and the attorney-client privilege.

A. Microsoft's Legislative Proposal

The legislation least likely to pass is Microsoft's proposal to allow individuals to decide what information is made available to cloud service providers, as well as to other organizations.[124] This proposal is likely to face large opposition from cloud service providers because it will limit the information they can gather for advertising, which allows them to provide certain services for free.[125] A better solution would take the current realities of cloud services into account.[126]

B. A Lawyer-Only Solution: The ABA Model Rules

A better option is to amend the American Bar Association's (ABA) Model Rules of Professional Conduct to clearly allow attorneys to use cloud services, even with providers that

---

utilized without involving client communications or jeopardizing the attorney-client privilege.

124. Brad Smith, *Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing*, MICROSOFT (Jan. 2010), http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/microsoft_corporation_2nd_document_en.pdf. This proposal goes beyond the internet and would allow people to control what information is collected about themselves offline as well. *Id.*

125. *See supra* note 77, at 593, 600 (explaining how Google scans emails and other documents in its cloud services to find keywords to direct advertisements toward the interests of the user).

Whether people should or should not have the right to not have data about themselves collected is beyond the scope of this Comment.

126. For the time being, it seems a better course of action would be to open the cloud to lawyers and discuss concerns over data collection as cloud services become more prominent. *See supra* sources cited note 46 (describing how the benefits of email were so great that old legal concepts were changed).

potentially have access to data or scan data for advertising purposes.[127] The ABA has expressed willingness to extend the basic text of its rules regarding the attorney-client privilege to new technology in the past.[128] When it approved the use of unencrypted email communications with clients, the ABA noted that all forms of communication have the risk of interception or disclosure.[129]

The attorney-client privilege is found in several places in the Model Rules.[130] There is no specific rule that governs electronic communications, but the rule makers did comment that, when using technology, a lawyer must "take reasonable precautions" against disclosure.[131] However, "reasonable" is not defined, leaving it up to the courts to decide.

In the interest of uniformity, the ABA should adopt a new model rule specifically governing the use of electronic communications and disclosure of client information. The model rule should read as follows:

> A lawyer shall be free to use electronic and internet-based means for communicating with clients or for storage of client information, unless directed not to by the client.[132]

---

127. The American Bar Association Model Rules of Professional Responsibility are a good choice because almost every state, and the District of Colombia, has adopted them. *Alphabetical List of States Adopting Model Rules*, AMERICAN BAR ASSOCIATION http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules.html (last visited Oct. 15, 2012).

128. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 413 (1999) [hereinafter ABA Formal Op. 99-413](finding that lawyers may use unencrypted email to communicate with clients without violating the attorney-client privilege).

129. *Id.* However, the ABA did caution lawyers against using unencrypted email for transmitting "highly sensitive matters" and suggested avoiding email use in those situations might be the best course. *Id.*

130. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 (2007) (requiring competent representation); MODEL RULES OF PROF'L CONDUCT R. 1.3 (2007) (requiring "reasonable diligence"); MODEL RULES OF PROF'L CONDUCT R. 1.6 (2007) (requiring a lawyer to keep information regarding representation of the client confidential); MODEL RULES OF PROF'L CONDUCT R. 5.1 (2007) (requiring lawyers to make sure co-counsel maintains client confidentiality); MODEL RULES OF PROF'L CONDUCT R. 5.3 (2007) (requiring lawyers to make sure non-lawyer employees maintain client confidentiality).

131. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2007).

132. One could argue that a rule such as this will completely relieve lawyers of responsibility, which might encourage negligent representation. However, clients will greatly benefit from their lawyer's use of the cloud. Use of the cloud makes people more efficient, allowing them to get their work done faster, something many clients would appreciate. *See supra* notes 11-18 and accompanying text (describing increases in productivity, lower costs, and preventing data loss as clear benefits of using the cloud).

This rule would be broad enough to encompass all forms of email and cloud services. It would also maintain the ABA's current practice of allowing clients to determine how communications are made.[133]

There should also be a comment explicitly dealing with a service provider's ability to access data or scan data for advertising purposes. That comment should read:

> The mere fact that a service provider can access information or does access information for advertising or maintenance purposes does not make use of that service by an attorney unreasonable.

The ABA has recognized this with regard to internet-based email services, finding internet-based email services no less reasonable to use than the telephone.[134] Access or potential access by a service provider should not be a reason to deprive lawyers of the advantages of cloud computing.[135] The ABA has said that absolute privacy is not demanded of a lawyer, just reasonable privacy.[136] Finally, a lawyer must remember to use best judgment and refrain from certain forms of communication, even if the client does not request more stringent security.[137]

---

133. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2007) (requiring a lawyer to fulfill any requests made by the client to implement special security precautions when dealing with communications); *see also* ABA Formal Op. 99-413 (applying this kind of limitation to other forms of communication).

134. ABA Formal Op. 99-413. The ABA has found that, in all likelihood, a service provider would have a difficult time accessing a lot of emails because of the high volume of data that would process through its system each day, and the speed with which this data is traveling. *Id.* at Part C.

Also pertinent to the ABA, emails are generally broken apart into smaller pieces of data and then recompiled when they reach their destination, making the likelihood that a service provider would actually access an entire email or document at all, let alone in context, relatively small. *Id.*

135. *See supra* notes 10-17 and accompanying text (describing the advantages of cloud computing such as lower costs, higher productivity, and the prevention of data loss due to a disaster).

136. ABA Formal Op. 99-413, Part A.

137. *Id.* Lawyers always have an obligation to consider how the mode of communication they select could affect the information it contains. *Id.*

For example, if a lawyer knows the client's email address is her work email address and the client has an employment discrimination claim against the employer, it would be the responsibility of the lawyer not to contact the client by email regarding the case, or to provide the client information on how to access documents stored in the cloud about the case through that email address.

There will always be times when certain forms of communication, including fax machines, telephones, and even face-to-face conversation, should be avoided. *Id.* Lawyers must recognize this and be able and willing to adapt. Lawyers also have a responsibility to explain to their clients when certain forms of communication would not be appropriate. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 459 (2011). Thus far, the ABA has only commented on use of work email and use of a computer owned by the

The benefit of using a model rule to effect this change, at least in some states, is removing the slow legislative process of passing a bill.[138] However, this might not be possible in all states, and some state courts might not be willing to adopt the change. For this reason, it will also be necessary for legislatures to take up this cause and consider legislation that will help protect information in the cloud.

C. A Cloud-Specific Legislative Solution

While most of this Comment focused on the attorney's end of the attorney-client privilege, the most comprehensive and best solution to this problem is based upon a rule that has already been implemented in New York. There, the statute governing the attorney-client privilege has an addendum that states:

> [N]o communication under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.[139]

This means that whether a communication was made electronically is usually not a factor in determining waiver.[140] However, New York's rule seems most appropriate when dealing with email, because it focuses on communication.[141]

New York's rule would be better if it was amended to protect the storage of communications in the cloud, as well. The amended statute should read:

> No communication under this article shall lose its privileged character for the sole reason that it is communicated by electronic means, stored electronically, or because persons necessary for the delivery or facilitation of such electronic communication or storage may have access to the content of the communication.[142]

---

employer. *Id.* Lawyers should assume that the ABA's mandate also applies to conversations about the risks of cloud services and the need for confidentiality, especially until courts and legislatures have determined the rules regarding cloud computing.

138. *See* People v. Jackson, 69 Ill. 2d 252, 256 (Ill. 1977) (recognizing that, in Illinois, the supreme court has the exclusive power to regulate all of the courts).

139. N.Y. <PRIVILEGED COMMUNICATIONS; ELECTRONIC COMMUNICATION THEREOF> Law § 4548 (McKinney 2012).

140. *See* Scott v. Beth Israel Medical Center, Inc., 17 Misc. 3d 934, 938, 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007).

141. *See id.* (noting that the purpose of the rule was to protect the use of email as a growing means of communication, especially in the corporate context).

142. It is important to remember that one of the main problems with cloud services is that service providers allow third parties to have access to the information for advertising and maintenance purposes. *See* Stylianou, *supra*

Because this legislation is broader in protecting not only attorneys, but also clients, it would be the most desirable route.

This Comment focused on the attorney side of the privilege because of the great benefits the cloud provides to businesses. However, individuals also have access to the cloud, and this legislation strikes a balance between the necessary protections and reasonableness on the part of the client. Interpretation of New York's statute makes it clear that employer email policies will remain significant.[143]

V. CONCLUSION

New technology will always create new challenges for the law as a whole. The legal profession has been rightfully cautious in adopting new technologies, given the risks of a breach of duty to the client. A finding of implied waiver can be devastating to a client's case. However, lawyers should not just accept that a new technology is out of their reach. Courts and the ABA have been slow to take on new technologies, so the push must begin sooner rather than later. It is also important to develop safe cloud services that can be used now, so lawyers can benefit from the lower costs and increased productivity that comes with cloud computing. Caution is the best initial policy, but legislation and development must be at the forefront.

---

note 77, at 600; *Dropbox Privacy Policy*, *supra* note 82 (discussing how and why Google and Dropbox access a user's data). The delivery and facilitation language in the proposed legislation seems broad enough to include things like advertising, because advertisements are how certain service providers provide their service for free. However, it would probably be prudent for lawyers to opt for any paid, non-advertisement-based services these companies provide.

143. *See Scott*, 17 Misc. 3d at 939 (finding that the New York law did not trump an employer's email policy forbidding personal use).