Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.147

http://tlp.law.pitt.edu

Throwing New Flags: Should There Be Criminal Sanctions or a Better Chance of Civil Sanctions for Lawyers or Service Providers Who Breach Confidentiality?

Lea L. Lach

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.

This site is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

Throwing New Flags: Should There Be Criminal Sanctions or a Better Chance of Civil Sanctions for Lawyers or Service Providers Who Breach Confidentiality?

Lea L. Lach[*]

INTRODUCTION

Although it is fairly new and threatening to client confidentiality, "cloud computing" does not warrant extraordinary efforts to impose new sanctions for its adverse consequences. This change in the way that lawyers store and access client files is controllable even without an increase in criminal or civil penalties for breach of client confidentiality. The risks that cloud computing carries are not entirely new, and state bar associations' attitudes toward the practice reflects that understanding.

What seems more radical is the possibility of criminal penalties for lawyers who breach confidentiality. Criminal penalties can affect certain types of American lawyers and some foreign lawyers, but they are rare for American lawyers in general. Furthermore, the difficulty of proving criminal intent and the likelihood of lawyer resistance would probably undermine efforts to fine or imprison a wider range of lawyers for breach of confidentiality.

It would also be difficult to hold online service providers[†] ("OSPs") liable for negligence that enables a lawyer's breach of confidentiality. Making OSPs more susceptible to civil penalties might be easier to imagine than increasing the chances of criminal penalties for lawyers. Federal law and OSPs' own policies however, often provide a shield from civil penalties that lawyers and clients are in no position to change at this time.

The following Article explains why cloud computing poses the risks to client confidentiality that it does and why Americans should not regard a greater likelihood of criminal or civil penalties as a solution. Part I provides an overview of cloud computing and its relationship to legal ethics. The overview of cloud

[*] J.D. Candidate, University of Pittsburgh School of Law, May 2014; B.A., Political Science and History, University of Pittsburgh.

[†] Online service providers are referred to as OSPs, Internet service providers, and service providers interchangeably throughout the paper.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

computing first explains how the technology works and its advantages and disadvantages. The overview then describes the responses of several state bar associations to the ethical implications of cloud computing. Part II explains why lawyers should not face criminal sanctions for cloud-related breach of confidentiality. Part III explains why it is not feasible to increase the chances of provider liability. Part IV concludes by arguing that even though cloud computing introduces new concerns specific to client confidentiality, increased civil penalties and criminal sanctions are not required to manage those concerns.

I. OVERVIEWS: CLOUD COMPUTING AND ITS RELATIONSHIP TO LEGAL ETHICS

A. Cloud Computing 101

When someone engages in cloud computing, it is illusory for him to think that he and his inner circle have complete control of their data. People use websites like Google and Facebook[1] through an entire "network of computers and servers that are publicly accessible over the Internet . . . ."[2] Yet new stronger software and computer chips make it possible for devices anywhere in the world, to behave as just one computer would, even laptops and smartphones.[3] When people store or share data, which they can do to a considerable extent using cloud computing, it falls under the management of third-party servers.[4] Besides being under third-party control, these servers may be scattered geographically.[5] Any server within a particular third party's network can pick up the stored or shared data.[6] The "server farms" also allow third parties to enable later access to stored data on a number of

[1] Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 171–72 (2011) (noting that use of Google or Facebook counts as "cloud computing").

[2] Meghan C. Lewallen, Note, *Cloud Computing: A Lawyer's Ethical Duty to Act with Reasonable Care when Storing Client Confidences "In the Cloud,"* 60 CLEV. ST. L. REV. 1133, 1138 (2013).

[3] Comm. on Legal Ethics and Prof'l Responsibility, Pa. Bar Ass'n, *Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property: Formal Opinion 2011-200*, THE PA. LAWYER, May/June 2012, at 49, *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf [hereinafter Pa. Bar Ass'n]; Trope & Hughes, *supra* note 1, at 171.

[4] Lewallen, *supra* note 2.

[5] Pa. Bar Ass'n, *supra* note 3.

[6] Lewallen, *supra* note 2.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

different devices.[7] Of course, the third parties' role means that the data is accessible to them as well.

Cloud computing certainly has advantages as well as disadvantages. Perhaps the most important overall advantage is the ability to access cloud-based services from a wide range of devices. A person could find a new piece of information almost as soon as it reaches her inbox and immediately tell her client.[8] For businesses like law firms, cost reduction and storage space may be equally important.[9] It might be less expensive to let third parties manage data than to link it to a specific office-based desktop or server.[10] According to Meghan C. Lewallen, the lesser expense may have the particular advantage of, "giving smaller firms a more level playing field with competitive large firms."[11] Even if cloud computing indeed bears a lower price than its predecessors, it can still provide a great deal of storage space and easy access to stored data.[12] Lawyers could even "engage in online document collaboration with clients and colleagues," which allows for the receipt of feedback on a document while a lawyer is still in the process of completing that document.[13] Document collaboration may further reduce costs because lawyers may become less likely to waste paper and ink on drafts they believe to be "final" before learning that more revisions are needed. Cloud computing can greatly enhance a firm's work without automatically imposing a high financial price.

The disadvantages may however, seem worse than just a high financial price. The involvement of third parties is itself a disadvantage[14] because consumers cannot easily monitor those third parties for signs of abuses. Cloud service providers can be fairly secretive,[15] and consumers must often choose between

---

[7] Trope & Hughes, *supra* note 1, at 164.

[8] *See* Lewallen, *supra* note 2, at 1139 (stating that cloud computing enables "quick and efficient communication"); Pa. Bar Ass'n, *supra* note 3 (stating that advantages of cloud computing include "quick, efficient communication" and "immediate access to updates").

[9] Lewallen, *supra* note 2, at 1139.

[10] *Id.*

[11] *Id.*

[12] *Id.*; Pa. Bar Ass'n, *supra* note 3.

[13] Lewallen, *supra* note 2, at 1140.

[14] *See* Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 363 (2013); Pa. Bar Ass'n, *supra* note 3, at 49–50.

[15] *See* Trope & Hughes, *supra* note 1, at 174–75.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

accepting unfavorable terms and conditions or rejecting the service.[16] Yet the provider could alter a program or engage in "maintenance" duty in a way that limits access to the service for a while.[17] This scenario is not favorable for a lawyer who needs to communicate with his client right away, such as a criminal lawyer whose client faces execution. In some cases, data may even vanish completely rather than temporarily. Most importantly for the purposes of this Article, cloud computing can easily undermine client confidentiality.

B. Cloud Computing's Relationship to Legal Ethics

Cloud computing strongly challenges lawyers' ability to carry out their duty of confidentiality. According to Rule 1.6(a) of the American Bar Association's Model Rules of Professional Conduct, attorneys "shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized . . . or the disclosure is permitted by paragraph (b)."[18] Paragraph (b) of Rule 1.6 lays out several exceptions,[19] but confidentiality is the general rule. Nearly all American jurisdictions have adopted the Model Rules.[20]

Information that must stay confidential is vulnerable in the "cloud" because the very nature of cloud computing makes it hard to prevent unauthorized access. Lawyers essentially engage in "outsourcing" when they use cloud computing.[21] Lawyers allow a third-party service provider to manage information[22] in return for upholding the provider's terms and conditions.[23] If the service provider is a large, for-profit company like Google, it may not be inclined to respect ethical rules that do not govern its own business. Even if this is not true, authority figures within a company may be incapable of monitoring every employee at all times. An employee might peruse confidential information and use it for a malicious purpose despite a company policy or prohibiting such conduct.[24] This person is probably

---

[16] *See* Pa. Bar Ass'n, *supra* note 3, at 53.

[17] Trope & Hughes, *supra* note 1, at 178.

[18] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (1983).

[19] *Id.* at 1.6(b).

[20] *See Alphabetical List of States Adopting Model Rules*, A.B.A., http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules.html (last visited Jan. 24, 2014).

[21] Pa. Bar Ass'n, *supra* note 3, at 52.

[22] Lewallen, *supra* note 2.

[23] *See* Pa. Bar Ass'n, *supra* note 3, at 53.

[24] *See* Lewallen, *supra* note 2, at 1141.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

someone whom the lawyer does not know, because a low-level employee probably would not be involved in the service agreement's formation. In fact, there is a strong possibility that the employee is working in a distant country given that a company can set up servers throughout the world.[25] Even worse, what he or she did might not violate that country's laws.[26] In fact, the lawyer may never see or know every person or server involved in the management of client information, and agreements often do not allow for much advance negotiation.[27]

Even though many state bar associations permit the use of cloud services, lawyers may not use the unintentional release of confidential information as a defense. For example, a Pennsylvania ethics opinion states that storing confidential client data "in the cloud" is fine if a lawyer acts reasonably to preserve the data's confidentiality and uses "reasonable safeguards . . . to ensure that the data is protected from breaches . . . and other risks."[28] The opinion gives numerous suggestions for meeting these conditions, from firewall installation to negotiation of lawyer-friendly terms with service providers.[29] At the same time, it notes that carelessness may violate more than just Pennsylvania's version of Model Rule 1.6.[30]

Ensuring confidentiality is also necessary for a lawyer to be truly "competent" under Pennsylvania's Rules of Professional Conduct, specifically Rule 1.1.[31] Rule 1.15 of these Rules demands safeguarding of a client's property, which can include electronic files.[32] Given these suggestions and the conditions they reflect, a lawyer would clearly bear some responsibility for even a third party's improper use or exposure of data.

A similar attitude is present among the bar associations of states other than Pennsylvania. An informal Ohio ethics opinion allows for cloud computing but cites the same kinds of ethics rules as the Pennsylvania ethics opinion and calls on

[25] Lewallen, *supra* note 2; Pa. Bar Ass'n, *supra* note 3.

[26] Pa. Bar Ass'n, *supra* note 3, at 50.

[27] *See id.* at 53.

[28] *Id.*

[29] *Id.* at 52–53.

[30] *Id.* at 50 (noting that Pennsylvania has a version of ABA Model Rule 1.6).

[31] *Id.*

[32] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

lawyers to take steps to keep data confidential.[33] A New Jersey ethics opinion avoids the term "cloud" and speaks instead of "an electronic filing system" in which files "are scanned into a digitized format such as Portable Data Format ("PDF")."[34] A lawyer could retrieve these files almost anywhere he goes,[35] but the opinion states that digitizing them would be fine if he uses "reasonable affirmative steps to guard against the risk of inadvertent disclosure."[36] In nearby New York, the state bar association calls for "reasonable care" while permitting storage of client files in the cloud, and explains what lawyers can do to ensure that service providers respect their obligations.[37] A Massachusetts ethics opinion also stresses confidentiality and the role of service providers while taking the same overall position as the New York opinion.[38] In general, these opinions do not *mandate* particular methods of preventing breach of confidentiality but instead allow for cloud computing when there is some action to prevent breach.[39] Ultimately, however the exact nature of the preventative action is a matter of discretion for lawyers.

The fact that lawyers have discretion in determining the measure of protection against a breach raises questions about the appropriateness of the usual sanctions for breach of confidentiality. When lawyers allow third parties to handle large amounts of data, they are taking a serious risk. It is hard to oversee a third party's use or abuse of data, especially if the data exists on a server in a foreign country.[40] Regardless of the risks, lawyers have strong incentives to use cloud computing anyway because it is quick and fairly inexpensive. The combined seriousness of the risks and likelihood that lawyers will still use the cloud may indicate a need for more stringent deterrents to breach of confidentiality.

---

[33] Professionalism Comm., Ohio State Bar Ass'n, *OSBA Informal Advisory Opinion 2013-03*, OHIO STATE BAR ASS'N (July 25, 2013, 12:00 AM), https://www.ohiobar.org/ForPublic/LegalTools/Documents/OSBAInfAdvOp2013-03.pdf.

[34] Advisory Comm. on Prof'l Ethics, *Electronic Storage and Access of Client Files*, N.J. COURTS, http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf (last visited Feb. 5, 2014).

[35] *Id.*

[36] *Id.*

[37] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *Ethics Opinion 842*, NEW YORK STATE BAR ASSOCIATION (Sept. 10, 2010), http://www.nysba.org/CustomTemplates/Content.aspx?id=1499.

[38] *Ethics Opinions: Opinion 12-03*, MASS. BAR ASS'N (May 17, 2012, 12:00 AM), http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03.

[39] *See* Advisory Comm. on Prof'l Ethics, *supra* note 34; N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 37; Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

[40] Lewallen, *supra* note 2; Pa. Bar Ass'n, *supra* note 3.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

II. CRIMINAL SANCTIONS FOR LAWYERS WHO BREACH CONFIDENTIALITY THROUGH CLOUD COMPUTING

A. Current Available Sanctions in the United States and Abroad

Typical sanctions for lawyers who breach confidentiality threaten a lawyer's reputation and pocketbook but hardly threaten his freedom. In Massachusetts,[41] New Jersey,[42] New York,[43] Ohio,[44] and Pennsylvania,[45] the highest state court or appeals court, along with a special court or committee devoted to legal ethics, is responsible for disciplining lawyers. Examples of sanctions that one of these bodies may impose include disbarment, suspension from practice, censure, or reprimands.[46] Even though these types of sanctions are not criminal sanctions, or even really civil sanctions, sanctions such as disbarment or suspension deny lawyers the freedom to practice the profession of their choice. It is important to note however, that not all lawyers face either of these sanctions for ethics violations. Furthermore, if the sanction results in a mere reprimand, the lawyer may lose clients or respect but still technically be free to practice law.

While sanctions are also available outside of a state's ethical discipline system, they do not always accompany ethical discipline and do not involve imprisonment of a lawyer in any case. There is discussion about the victims of a confidentiality breach possibly filing lawsuits based on legal malpractice or breach of fiduciary duty,[47] or on the tort of breach of confidence.[48] This is a client's choice, however. It will not *necessarily* accompany ethical proceedings.[49] Furthermore, these lawsuits are all civil claims. A client could for example receive money damages from a lawyer, but the lawyer will not go to jail no matter how egregious the breach.

---

[41] Debra Moss Curtis, *Attorney Discipline Nationwide: A Comparative Analysis of Process and Statistics*, 35 J. LEGAL PROF. 209, 258–59 (2011).

[42] *Id.* at 280–82.

[43] *Id.* at 286–88.

[44] *Id.* at 293–94.

[45] *Id.* at 298–99.

[46] *Id.*

[47] Douglas R. Richmond, *Lawyers' Professional Responsibilities and Liabilities in Negotiations*, 22 GEO. J. LEGAL ETHICS 249, 262 (2009).

[48] Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 673–74 (2012).

[49] Richmond, *supra* note 47.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

There is at least one federal statute providing for criminal sanctions against lawyers who misuse private information. As Stacey A. Tovino notes, this development actually came later than the original statute.[50] In 1996, the Health Insurance Portability and Accountability Act ("HIPAA") left it to either a separate statute or the Department of Health and Human Services to enact privacy rules for health care information.[51] The Department issued a "Privacy Rule" in the early 2000s.[52] The rule first applied to health care plans and clearinghouses as well as certain health care providers, and it limited their use and disclosure of certain health care-related information on individuals.[53] Even though there was no direct impact on lawyers who had to access such information to effectively represent a doctor or hospital, as in a malpractice case,[54] the Rule required that covered entities clearly ensure that outside lawyers and other "business associates" kept the information confidential.[55]

In 2009, direct regulation finally arrived and opened lawyers to penalties already possible for plans and providers, including criminal sanctions.[56] The direct regulation was part of the Health Information Technology for Economic and Clinical Health Act ("HITECH").[57] Section 13404(a) of HITECH expressly forbids "a business associate of a covered entity" to "use and disclose . . . protected health information" under most circumstances.[58] HITECH goes on to say, in § 13404(c), that civil and criminal penalties can cover business associates.[59] Since the Privacy Rule's definition of "business associate" includes lawyers,[60] lawyers are among those who could face criminal penalties if they do not obey § 13404(a) and companion provision § 13404(b).[61] A lawyer faces these penalties if she engages in

---

[50] Stacey A. Tovino, *Gone Too Far: Federal Regulation of Health Care Attorneys*, 91 OR. L. REV. 813, 814–15 (2013).

[51] *Id.* at 816–17.

[52] *Id.* at 817.

[53] *Id.* at 819.

[54] *Id.* at 822–23, 825.

[55] *Id.* at 823–25.

[56] Tovino, *supra* note 50, at 823–25.

[57] *Id.* at 814–15, 826.

[58] 42 U.S.C. § 17934(a) (2012).

[59] *Id.*

[60] *See* 45 C.F.R. § 160.103(1)(ii) (2013).

[61] 42 U.S.C. § 17934(c) (2012).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

knowing and wrongful disclosure, obtainment or use of protected information.[62] Fines and imprisonment are possible, and a prison term could last one year, five years, or ten years depending on the circumstances of the crime.[63] The Act does not cover a wide range of lawyers, but it is significant just for subjecting lawyers to the risk of fines and imprisonment for misuse of private information.

Foreign law also provides a model for using the criminal law to punish lawyers' failure to uphold confidentiality standards. For example, France's criminal code provides for a fine and a year of imprisonment for "disclosure of secret information by a person entrusted with such a secret . . . because of his position or profession . . . ."[64] At least one legal commentator presents this provision as one that would apply to lawyers.[65] He also notes a provision of Germany's criminal code that can subject lawyers to fines or imprisonment if they do not safeguard confidential information.[66] A German lawyer who "unlawfully discloses a secret of another . . . which belongs to the sphere of personal privacy or a business or trade secret . . . confided to or otherwise made known to him in his capacity as . . . attorney" could pay a fine or spend up to a year behind bars.[67] The European laws do not use the words "confidentiality" or "confidential,"[68] but they still threaten lawyers with criminal penalties for certain disclosures of information they receive through their work.

Foreign law and HITECH demonstrate how states could punish lawyers for confidentiality breaches under criminal law, but it is important to remember that these laws do not cover a wide range of U.S. lawyers. Foreign law will not apply to Americans who work almost exclusively in the United States. Additionally, the German and French laws are part of codes that cover entire countries, while the U.S. generally leaves lawyer discipline to each of the individual states. HITECH is a federal law and applies to American lawyers, but the lawyers must work with

---

[62] 42 U.S.C. § 1320d-6(a) (2012).

[63] 42 U.S.C. § 1320d-6(b) (2012).

[64] CODE PÉNAL [C. PÉN.] art. 226-13 (Fr.), *available at* http://www.legislationline.org/documents/section/criminal-codes.

[65] David L. Nersessian, *How Legislative Bans on Foreign and International Law Obstruct the Practice and Regulation of American Lawyers*, 44 ARIZ. ST. L.J. 1647, 1673 n.127 (2012).

[66] *Id.*

[67] STRAFGESETZBUCH [StGB] [PENAL CODE], Nov. 13, 1998, BUNDESGESETZBLATT, Teil I [BGBL. I] 3322, as amended, § 203 (Ger), *available at* http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

[68] *Id.*; CODE PÉNAL [C. PÉN.] art. 226-13 (Fr.).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

health care-related information and represent certain health care-related entities.[69] Using statutes that cover few or no U.S. lawyers as bases for statutes that cover nearly all U.S. lawyers and confidentiality breaches may lead to enforcement difficulties. What might work well against foreign lawyers or small groups of lawyers and breaches will not necessarily work well against U.S. lawyers and breaches in general. Persons involved in state law enforcement would have to keep a closer watch on far more lawyers than HITECH covers, and it may be harder to catch every breach when the group of lawyers theoretically subject to a statute is broad.

Even if states could easily identify breaches when they occur, the range of lawyers who could experience criminal sanctions may be small in reality. As common criminal law and statutory criminal law in the U.S. tend to attach a *mens rea* element to crimes,[70] a defendant generally must have some idea that his conduct is unlawful.[71] There are "strict liability" statutes that do not call for a *mens rea*, but the number is fairly small and the statutes tend to focus on "potentially harmful or injurious items" like grenades.[72] However, proving that a lawyer breached confidentiality with a particular *mens rea*, such as "purposely" or "knowingly,"[73] may be difficult if he committed the breach through cloud computing. The lawyer may understand the general risks but still fail to realize that a particular action can or will result in breach. Furthermore, some serious breaches could result from omissions, such as failure to install a strong firewall, rather than actions. A criminal statute would have to name specific actions or omissions in cloud computing that can or will result in breach, which may take a great deal of the state legislature's time and still not cover all serious risks.

The statute could call for a "recklessly" or "negligently" *mens rea* if many actions and omissions seem more like civil negligence than criminal acts. If the state has adopted the Model Penal Code's definitions of recklessness or negligence, though, many lawyers and breaches may still fall short of the standards for criminally reckless or negligent conduct. Recklessness under the Code "involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor's situation."[74] Negligence "involves a gross deviation from the

[69] Tovino, *supra* note 50, at 843–44.

[70] Staples v. United States, 511 U.S. 600, 605–06 (1994).

[71] *Id.* at 606–07.

[72] *Id.* at 606–08.

[73] MODEL PENAL CODE § 2.02 (1962).

[74] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

standard of care that a reasonable person would observe in the actor's situation."[75] A breach of confidentiality that warrants civil liability may not be sufficiently "gross" to warrant criminal sanctions.

Regardless of the required *mens rea*, lawyers may express strong resistance to criminal sanctions for what were traditionally legal ethics violations. Lawyers are not accustomed to *any* criminal sanctions as a response to breach of client confidentiality. Disciplinary action under legal ethics rules is also not the only punishment that a lawyer may receive. Civil sanctions like monetary damages are also available. Many lawyers may legitimately perceive criminal sanctions as excessive and unnecessary, which could greatly undermine their potential to deter breaches of confidentiality.

There are also legitimate reasons to trust state bar associations to deter breaches that may occur through cloud computing. The mere fact that bar associations are letting members use the cloud suggests that they find breaches of confidentiality preventable. They are also describing many strategies for preventing breach in their ethics opinions. For example, the Pennsylvania Bar Association's Formal Opinion spreads breach prevention strategies across two pages,[76] and the Ohio State Bar Association's Informal Advisory Opinion ("OSBA") spreads strategies across four pages.[77]

Additionally, not every risk and concern that cloud computing implicates is unique to cloud computing. As the New Jersey opinion on "Electronic Storage And Access of Client Files" says, many lawyers "use messengers, delivery services, document warehouses, or other outside vendors" not involved in the cloud.[78] When a lawyer chooses these traditional vendors, "physical custody of client sensitive documents is entrusted to them. . ."[79] The Pennsylvania Bar Association likens cloud computing to "an *online* form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney."[80] The Pennsylvania Bar Association, too, acknowledges that lawyers had ways to leave client data with outsiders in earlier times. At the same time, it explicitly indicates that the same ethics rules can cover cloud computing and the older means of outside storage alike. The Ohio State Bar Association is even more forthright in

[75] *Id.*

[76] Pa. Bar Ass'n, *supra* note 3, at 52–53.

[77] Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

[78] Advisory Comm. on Prof'l Ethics, *supra* note 34.

[79] *Id.*

[80] Pa. Bar Ass'n, *supra* note 3, at 52 (emphasis added).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

acknowledging that the cloud presents problems that are not so new by claiming that "issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite. . ."[81] If there are some similarities between cloud computing and earlier means of storing files, state bar associations are probably well-prepared for breach-of-confidentiality claims involving the cloud.

In that case, new criminal penalties hardly seem necessary to deter breaches and ensure that lawyers face some kind of discipline for breaches. Bar associations are aware of the risks of cloud computing, and persons in charge of disciplining their lawyer peers do not intend to be more lenient than they would be if the breach resulted from offsite paper storage. The threats of earlier data storage methods to confidentiality also did not make lawyers more vulnerable to criminal penalties. There was no change in the criminal law to make lawyers more vulnerable to its reach, at least outside the narrow context of health care. Yet threats of civil or professional penalties undoubtedly motivated some lawyers to be more careful about avoiding breach of confidentiality. If cloud computing and earlier storage methods are somewhat analogous, there is reason to hope that deterrence through current civil and professional penalties will remain effective.

III. BETTER CHANCE OF CIVIL PENALTIES FOR ONLINE SERVICE PROVIDERS THAT ENABLE BREACH

One alternative to more stringent penalties for lawyers is a greater likelihood of civil liability for companies providing cloud-computing services, such as Google, Facebook, and YouTube.[82] There are already some contexts where one person's tort can lead to liability for another person or for a larger entity.[83] For example, even when an employee directly commits a tort, the employer may still face liability for that tort.[84] Such indirect liability can be appropriate when a breach takes place. The actual breach may be the lawyer's work, but perhaps it would be much harder or impossible to commit the breach without a certain action or omission of the service provider. Perhaps the risk of this breach was clear to the company, but the company failed to take any steps to reduce the risk even though certain steps were feasible. Lawyers still merit punishment for breach of their

[81] Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

[82] Trope & Hughes, *supra* note 1, at 171–72.

[83] Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222–23, 228 (2006).

[84] *Id.* at 228.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

clients' confidentiality, but the responsibility may not always fall on lawyers alone. Efforts to deter breach in the cloud may not be complete unless service providers face a greater likelihood of penalties for negligence that enables a breach.

There are however, two important factors, which make it very difficult for lawyers and clients to hold the companies liable at this time.

A. Federal Law

Federal law grants service providers some protection against liability for torts like negligence. Under one statute, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[85] This provision shields Internet service providers from liability when potentially tortious content comes from a third party.[86] In fact, "[c]ourts have flatly refused to strip . . . immunity even when the ISP has an active role in creating or distributing the content."[87] If a lawyer uses the provider's services to post confidential client data and the client sues both lawyer and provider, it may be dispositive that the lawyer posted the information. Given courts' broad reading of the federal law, the provider could escape liability even if it negligently designed its service or neglected to block or punish conduct that violates its terms of use.

Some courts have denied complete immunity to service providers in the past few years, but this is not true of all federal circuits and does not affect most passive providers.[88] Elizabeth M. Jaffe, an Associate Professor at John Marshall Law School in Atlanta, explores the denial of complete immunity in a Hastings Communications & Entertainment Law Journal article published in 2012.[89] One opinion that she cites in her article is a federal district court opinion that indicates that complete immunity may not apply when providers "are encouraging and soliciting wrongful content from third parties or creating such content."[90] Jaffe then notes that several federal appellate courts may similarly deny that a provider has complete immunity in some cases.[91] As support for this assertion, Jaffe names just

---

[85] 47 U.S.C. § 230(c)(2)(B) (2012).

[86] Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 368 (2005).

[87] *Id.* at 370.

[88] Elizabeth M. Jaffe, *Imposing a Duty in an Online World: Holding the Web Host Liable for Cyberbullying*, 35 HASTINGS COMM. & ENT. L.J. 277, 286, 289 (2013).

[89] *See id.*

[90] *Id.* at 286.

[91] *Id.* at 289.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

four appellate courts and notes that two others may still find complete immunity.[92] Whether victims of a breach of confidentiality have any chance to hold a provider liable seems to depend at least in part on where they live. Additionally, the appellate court opinions that Jaffe cites to support her point involved providers that did more than just publish controversial content.[93] These opinions would not aid victims of a breach who merely claim that the provider was negligent in designing a site or enforcing its terms and conditions. Omissions alone likely remain insufficient to enable liability for providers. The development reported is encouraging but does not mean that change in the law is unnecessary to increase a provider's chance of liability.

Chances are that the will to change the law does not exist in Congress right now. This is evidenced by the fact that the Communications Decency Act's immunity provision has survived for nearly twenty years, ever since the law's passage in 1996.[94] It is unlikely that many members of Congress would be inclined to try amending a long-standing statute when Congress cannot even pass a lot of new legislation.[95] Even in a more active Congress, members may be reluctant to disturb service providers' fairly solid reliance on federal immunity from negligence liability. Reliance is an important consideration because the current law is clear about what providers may do or allow without fear of liability. Altering the law may make it harder for companies to figure out when and whether they would be liable for third-party conduct, especially if active participation in the conduct is not necessary. Of course, service providers could probably count on Congress to respect their reliance because of their wealth, lobbying ability, and importance in American life. Under these circumstances, clients cannot count on Congress to limit Communications Decency Act immunity within the next few years.

B. Online Service Providers' Terms and Conditions

Service providers themselves may also restrict a lawyer's ability to hold them liable for negligence, as well as the lawyer's freedom to reject the restriction. In addition to the technology that enables lawyers to breach client confidentiality, cloud service providers like Google and Dropbox present lawyers with "Terms of

---

[92] *Id.*

[93] *Id.* at 290–92.

[94] *Id.* at 339 (noting that the law providing immunity from liability for third-party postings is the Communications Decency Act of 1996).

[95] *'Do-Nothing' Congress on Track for One of the Least Productive Years Ever*, NBC NEWS (Feb. 3, 2013, 7:37 PM), http://www.nbcnews.com/politics/politics-news/do-nothing-congress-track-one-least-productive-years-ever-v21578861.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

Service."[96] These "Terms of Service" explain what the user and the service provider may and may not do in relation to the service provided.[97] One likely condition is limitation of the provider's liability.[98]

Acceptance of the limitation frees providers from most, if not all, responsibility that they might otherwise bear for losses such as data or profit losses.[99] Persons and entities closely connected to the company may also enjoy protection, including suppliers,[100] distributors,[101] and employees.[102] It may be irrelevant whether a person would be claiming punitive damages, consequential damages, or exemplary damages.[103] The same may be true of the overall "legal theory" that the person, if allowed to do so, may wish to use in court.[104] Google's terms and conditions even include a provision on "Business uses of our Services"[105] that is especially relevant to private law firms. This provision imposes a promise on businesses to "hold harmless and indemnify Google . . . from any claim, suit or action arising from or related to the use of the Services. . ."[106] There are states that prohibit these kinds of limitations from being effective in practice,[107] but certainly not all states. A person or business that refuses to accept the limitation will likely be unable to use the service, because the terms and conditions of these agreements tend to be adhesive.[108] Lawyers who directly defy the terms could be charged with unauthorized access to the services under federal law.[109] If lawyers find that the terms do not go far enough to ensure protection of confidential data,

---

[96] *See, e.g.*, *Policies & Principles: Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/ (last modified Nov. 11, 2013); *Dropbox Terms of Service*, DROPBOX, https://www.dropbox.com/terms (last updated Mar. 26, 2012).

[97] GOOGLE, *supra* note 96; DROPBOX, *supra* note 96.

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] GOOGLE, *supra* note 96; DROPBOX, *supra* note 96.

[104] *Id.*

[105] GOOGLE, *supra* note 96.

[106] *Id.*

[107] DROPBOX, *supra* note 96.

[108] Kesan et al., *supra* note 14, at 424; Pa. Bar Ass'n, *supra* note 3, at 53.

[109] Kesan et al., *supra* note 14, at 422.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

then they must forgo the service in the first place. Of course, their options for data storage may be very limited if most storage systems involve cloud computing.

The Pennsylvania Bar Association suggests that lawyers may soon gain more freedom to negotiate better terms, but bar associations do not regard this freedom as a current reality. The Pennsylvania Bar Association notes, "new competition in the cloud computing field is now causing vendors to consider altering terms."[110] It then suggests that this development may make it easier for lawyers to negotiate terms that better protect confidentiality.[111] However, the use of "consider" to describe service providers' attitude towards changing their terms suggests that most providers are only weighing the possibility of change right now. The Pennsylvania Bar Association offers no example of an actual change in terms that improves their compatibility with lawyers' duties. The New York State Bar Association says that lawyers can protect confidentiality by making sure that service providers accept an obligation to do the same and that there is a way to enforce it.[112] Lawyers would not necessarily have to convince a provider to change its written terms and conditions, because the New York State Bar Association's statement may simply mean that lawyers must be sure *existing* terms and conditions establish the obligation and a means of enforcement. Similarly, while the Ohio State Bar Association urges lawyers to "make reasonable efforts to ensure that the vendor's conduct is compatible with . . . professional obligations,"[113] it does not say that they should negotiate more lawyer-friendly terms. It simply adds that "the lawyer must exercise due diligence in ascertaining whether the vendor will be capable of conduct consistent with the lawyer's own obligations."[114] The way this phrase is written, a lawyer could satisfy the obligation by examining a provider's terms and refusing to use the provider's services if the terms make him uneasy. The text does not imply that a lawyer can only satisfy the obligation by asking the provider for a change in terms that better suits the lawyer's duties. Bar associations likely avoid mentioning this possibility because their members are aware that it is not really a current option. There is some hope that it will be a real option, but providers are just starting to move in that direction now.

The opinions also make it clear that lawyers can exercise some control over the effects that a cloud service provider may have on confidentiality. The advice

[110] Pa. Bar Ass'n, *supra* note 3, at 53.

[111] *Id.*

[112] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 37.

[113] Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

[114] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

from the New York and Ohio bar associations mentioned above can help lawyers prevent a breach from happening in the first place.[115] If they screen a provider's terms for compatibility with their duties and choose only services with the most compatible terms,[116] they are still making decisions that reduce the chances of a breach. The Pennsylvania Bar Association lists many examples of cloud service features and terms and conditions that lawyers should look for.[117] Some of these include a way for providers to keep data from persons with no need to see it; a way for lawyers to retrieve data if they give up the service; and terms and conditions allowing law firms to audit security features.[118] If a service and related terms have many features like these, persons working for the service provider probably intend to be vigilant about confidentiality. The features and terms reflect a conscious awareness of how easily cloud service can undermine confidentiality. The chances of negligent service design are probably lower in that case. It should also be easier to trust the provider to avoid negligent acts or omissions in a situation that could lead to breach, such as emergence of a virus.[119] If a lawyer follows bar association suggestions when choosing a provider, then he should end up with a provider that does not negligently disregard the lawyer's obligations. The difficulty of imposing civil penalties on providers may not matter because responsibility for breach is less likely to lie with the provider.

IV. CONCLUSION

Cloud computing is a new danger to client confidentiality, but not a reason to expand the sanctions available to lawyers and online service providers who breach confidentiality. It is certainly disturbing to imagine a lawyer or provider granting an unseen third party access to a Pittsburgh client's files in another state or country. The client would likely assume that even her friends and family in Pittsburgh will never see the files, yet careless cloud computing may allow total strangers to see them. Even worse, in this scenario, the lawyer at least implicitly promised to keep the files confidential because his state ethics code requires it.

This scenario could easily arouse calls for criminal sanctions against lawyers or a better chance of civil sanctions for service providers, but neither option is

[115] *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 37; Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

[116] *See* Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

[117] Pa. Bar Ass'n, *supra* note 3, at 52–53.

[118] *Id.*

[119] Trope & Hughes, *supra* note 1, at 183.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu

practical right now. With the exception of the HITECH Act that covers only some lawyers,[120] American law does not provide for criminal sanctions when lawyers breach client confidentiality. Even if it did, proving criminal intent may be challenging when many breaches would likely resemble civil negligence more than criminal acts. Meanwhile, raising the risk of civil sanctions for cloud service providers is nearly impossible because federal law[121] and their own terms and conditions[122] would likely shield them from liability. For the time being, clients must trust state bar associations to help lawyers prevent breach of confidentiality in the cloud and to impose sanctions for it. Fortunately, bar associations seem well prepared to do so in light of their experience with earlier storage methods that posed a threat to confidentiality.[123]

Trust remains important in the lawyer-client relationship no matter how much technology might change. Even though it may be harder to trust lawyers to protect confidential information today, it is reasonable to believe that their bar associations can meet that challenge without new sanctions for breach of confidentiality.

[120] Tovino, *supra* note 50, at 830–31.

[121] 47 U.S.C. § 230 (2012).

[122] GOOGLE, *supra* note 96; DROPBOX, *supra* note 96.

[123] *E.g.*, Professionalism Comm., Ohio State Bar Ass'n, *supra* note 33.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.147 ● http://tlp.law.pitt.edu