2014

Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege When Lawyers Store Clients' Files in the Cloud--and What, if Anything, Can Lawyers and Law Firms Realistically Do in Response?

Sarah Jane Hughes
Indiana University Maurer School of Law, sjhughes@indiana.edu

DID THE NATIONAL SECURITY AGENCY DESTROY THE PROSPECTS FOR CONFIDENTIALITY AND PRIVILEGE WHEN LAWYERS STORE CLIENTS' FILES IN THE CLOUD – AND WHAT, IF ANYTHING, CAN LAWYERS AND LAW FIRMS REALISTICALLY DO IN RESPONSE?

Sarah Jane Hughes[*]

I. INTRODUCTION

In the months since Edward Snowden's revelations about the National Security Agency's ("NSA") comprehensive gathering of metadata from telephone calls, emails and uses of the Internet here and abroad, many commentators have focused on whether and to what extent the data collection programs have exceeded the NSA's authority.[1] Additionally, commentators have asked how the data may have enabled the NSA's recognition of many relationships previously considered confidential by the parties to the underlying communications.

---

[*] Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law, Maurer School of Law, Indiana University, Bloomington, Indiana. Hughes is the co-author of RESPONDING TO NATIONAL SECURITY LETTERS: A PRACTITIONER'S GUIDE (ABA, 2009) (with Professor David P. Fidler), the curator and primary editor of RFIDS, NEAR-FIELD COMMUNICATIONS AND MOBILE PAYMENTS: A GUIDE FOR LAWYERS (ABA, 2013), and co-author with Roland T. Trope of the article entitled *Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing,* 38 *WM. MITCHELL L. REV.* 111 (2011), hard copies of which are available from the author. She also has published articles on privacy and data security, electronic and mobile payments, banking law, virtual currencies, and policies and regulations related to the deterrence of money laundering. She is a graduate of Mount Holyoke College and of the University of Washington's School of Law. She can be reached at sjhughes@indiana.edu.

Professor Hughes wishes to thank Professor Jon Garon for his kind invitation to participate in this Law + Informatics Symposium on Cyber Defense Strategies and Responsibilities for Business and Industry. She also acknowledges the valuable research for this paper provided to her by Janelle R. Duyck, Maurer School Class of 2015, particularly the compilation of formal and informal opinions issued by state bar associations or states' highest courts on cloud-computing and professional ethics since August 4, 2011 that appears as Appendix I to this paper.

This paper would not be possible without the path-breaking presentations in 2009 and 2010 by Roland L. Trope and Claudia Ray, members of the New York Bar, relating to professional ethics and use of social media and cloud computing entitled *The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms and Judges,* Essay for CLE Program, ABA Annual Meeting, San Francisco, August 2010, and *Head in the Cloud – Feet on the Ground: Understanding the Ethical Challenges of Web 2.0 for Lawyers, Law Firms and Judges,* ABA Annual Meeting, Chicago, August 2009. Copies of the essays Mr. Trope and Ms. Ray prepared are on file with the author.

1. Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

Less attention had been paid to other collateral consequences of the NSA's data-gathering work and the threats it poses to the confidential and privileged information that communications between lawyers and clients often contain. Focus shifted to certain collateral consequences with two relatively recent revelations in particular: the revelations that (1) the NSA may have introduced some tools to allow it to decrypt encrypted data,[2] and (2) that it apparently enjoyed the fruits of signals intelligence by its Australian counterpart, the Australian Signals Directorate, relating to the representation by a U.S. law firm and its client the government of Indonesia pertaining to a then-pending trade dispute between the U.S. and Indonesia, and shared those fruits with client agencies in the federal government.[3] Both reports raise fresh concerns over privileged communications and clients' confidential data moving through electronic communications into storage, including cloud computing storage.

In our 2011 article entitled *Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing* [hereinafter "Red Skies"],[4] Roland L. Trope and I observed, among other things, that lawyers and law firms using the cloud for storage of clients' files and documents would enable easier access to files and documents by governments.[5] We asserted that lawyers, law firms, and clients would not know about the access or manner of access until the access had been obtained.[6] (Like most Americans, at that time, we were unaware of the scope of the NSA's surveillance programs relating to domestic telecom communications and Internet storage.) Our prediction was based on the then-known authority for the government to gain access,[7] the ongoing disputes about the protections that the Electronic Privacy Communications Act of 1986 ("ECPA") gave to telecom records,[8] and the fact that both the Foreign Intelligence Supervision Act ("FISA")[9] and other "national security letters" authority prohibited the disclosure

2. *See generally* Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages,* THE GUARDIAN (July 11, 2013), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

3. See Jason Risen and Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm,* N.Y. TIMES, Feb. 15, 2014, at A1 [hereinafter Risen & Poitras].

4. 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, 230-235 (2011).

5. *Id.* at 230-233.

6. *Id.*

7. *E.g.,* Electronic Communications Privacy Act of 1986, Title II (Stored Communications Act), 18 U.S.C. §§2701 -2722, Pub. L. 99-508, 100 Stat. 1848; Foreign Intelligence Surveillance Act of 1978, 50 U.S. C. ch. 36, Pub. L. 95-511, 92 Stat. 1783. For a comprehensive discussion of national security letter laws, see David P. Fidler & Sarah Jane Hughes, RESPONDING TO NATIONAL SECURITY LETTERS: A PRACTITIONER'S GUIDE (2009).

8. *See* Somini Segupta, *Updating an Email Law From the Last Century,* N.Y. TIMES, Apr. 25, 2013, at B1, *available at* http://www.nytimes.com/2013/04/25/technology/updating-an-e-mail-law-from-the-last-century.html?pagewanted=all.

9. Foreign Intelligence Surveillance Act of 1978, 50 U.S. C. ch. 36, Pub. L. 95-511, 92 Stat. 1783.

of their receipt by the person or firm holding the information sought.[10] Only in recent months has the Department of Justice made it clear that they obtained information used in criminal proceedings via one of the "national security" avenues of access they have.[11]

Our 2011 article also anticipated the enhanced risks that governments and others could gain access to cloud-stored files when the cloud provider stores documents in undisclosed offshore locations,[12] and we cited the ABA's Formal Op. 08-451, which noted that new issues could arise with the non-U.S. laws on seizures in judicial or administrative proceedings notwithstanding claims of client confidentiality.[13]

This paper updates that 2011 article in modest ways related to its forecast of more and easier government surveillance of work product and client documents in cloud storage. From the base of the 2011 article, it also looks at the more recent past with its revelations of NSA surveillance and towards a future in which lawyers and law firms may have to employ less technologically hip techniques for communicating with clients while maintaining traditional lawyer-client privileges and storing clients' trade secrets and other confidential records.

Part II of this article explains the most current rules on lawyers' obligations to protect the confidential and privileged information they obtain from clients using as its benchmarks the August 2012 amendment to Rules 1.1, [14] 1.4,[15] 1.6,[16] (including its new subsection (c)), and 1.15,[17] and new comments to those sections of the America Bar Association's (ABA) Model Rules of Professional Conduct ("MRPC") based on the ABA's Commission on Ethics 20/20.[18] It also compares the 2012 amendments to the Model Rules of Professional Conduct that relate to the NSA data-collection programs to the prior MRPC versions of these

---

10. 18 U.S.C. § 2709 (2011); 18 U.S.C. § 3123(d)(2) (2011); s*ee also* Matt Apuzzo & Nicole Perlroth, *U.S. Relaxes Some Data Disclosure Rules,* N.Y. TIMES, Jan. 28, 2014, at B1-2 (providing that earlier in 2014, the Obama administration agreed to allow Internet companies such as Google, Microsoft, Yahoo, and Facebook to disclose how often the government asks for their customers' information, but will not permit the companies to reveal what the government collects or how much data it collects. Apuzzo and Perlroth also cite Forrester Research predictions that concerns over data accessed by national security letters and FISA court orders "could cost the so-called cloud computing industry as much as $180 billion – a quarter of its revenues – by 2016").

11. *See NSA Surveillance: A New Door to Court Challenges?* NEWSMAX WORLD (Feb. 27, 2014), http://www.newsmaxworld.com/GlobalTalk/US-NSA-surveillance/2014/02/27/id/555118/ (last visited on April 14, 2014).

12. *Red Skies*, *supra* note 4, at 148-49, citing ABA Comm'n. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008) [hereinafter ABA Formal Op. 08-451] (discussing the scope of MODEL RULES OF PROF'L CONDUCT RULE 1.1).

13. *See id.*

14. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2012).

15. MODEL RULES OF PROF'L CONDUCT R. 1.4 (2012).

16. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).

17. MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012).

18. A AM. BAR ASS'N COMM'N ON ETHICS 20/20, *Report to the House of Delegates*, www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited Jan. 25, 2014).

Rules.[19] To provide additional perspective on access to files and documents stored in the cloud by federal and state law enforcement agencies in the United States *other than the intelligence agencies*, this article briefly discusses the ABA's 2012 Criminal Justice Standards on Law Enforcement Access to Third Party Records.[20]

Part III looks at the differences between "privileged" and "confidential" information and the risks to each category of information that the NSA surveillance raises. Part IV discusses enhanced risks to data and storage flowing from the formerly secret "back doors" and encryption-breaking practices that NSA has introduced into commonly used electronics such as tablets and smart phones that allows more surveillance by the NSA and FBI,[21] and hacking by many potential sources including possibly by clients' counter-parties.[22] This part expresses doubts that President Obama's January 17, 2014 Signals Intelligence Directive, [23] which outlines the scope of continuing collection and review of telephonic and other electronic communications, will correct the risks to clients' confidential and privileged records in the cloud.

In Part V, this article briefly discusses lawyers' and law firms' duties arising under data security breach notification laws enacted by the States and in the European Union that arise when their electronic records are hacked, whether in their own offices or in the cloud. Among the sources of data security prevention and public responsibility for breaches and notification, it also cites the Federal Trade Commission Act.[24]

---

19. *See* Trope & Hughes, *supra* note 4, for a fulsome discussion of the pre-2012 version of the Model Rules of Professional Conduct.

20. AM. BAR ASS'N, *Criminal Justice Standards on Law Enforcement Access to Third Party Records,* http://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access.html (last visited April 14, 2014).

21. *See Close the N.S.A.'s Back Doors,* N.Y. TIMES, Sept. 22, 2013, at SR10, *available at* http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html?_r=0, (mentioning coverage by itself, The Guardian, and ProPublica that the NSA "now has access to the codes that protect commerce and banking systems, trade secrets and medical records, and everyone's e-mail and Internet chat messages, including virtual private networks, and encryption protecting data on iPhone, Android and BlackBerry phones").

22. *See, e.g.,* E. Michael Maloof, *NSA Has Total Access via Microsoft Windows*, http://www.wnd.com/2013/06/nsa-has-total-access-via-microsoft-windows/ (last visited Apr. 14, 2014) (citing Joseph Farah, *G2 Bulletin*, http://g2.wnd.com (Jun. 23, 2013)) (reporting that the NSA has "backdoor access to all Windows software since the release of Windows 95" and tying the backdoors to "insistence by the agency and federal law enforcement for backdoor "keys" to any encryption; providing further that Windows "software driver used for security and encryption functions contains unusual features that give the NSA the backdoor access" and "[s]uch access to the encryption system of Windows can allow NSA to compromise a person's entire operating system").

23. Presidential Policy Directive/PPD-28, *Signals Intelligence Activities,* WHITE HOUSE (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

24. 15 U.S.C. § 45 (2010).

Part VI first surveys recent, publicly available advice, primarily concerning technology tools that address cloud computing risks and solutions. It also reports on increasing client demands that law firms undergo cybersecurity audits themselves, and states some conclusions about lawyers' obligations when using cloud computing and storage, including new risks connected to the NSA's telecommunications data-gathering programs and its back-doors and encryption-busting propensities that threaten lawyers' ability to use the cloud for storage of confidential or privileged communications with and information belonging to clients as to require prompt reexamination of such use and renewed efforts to inform clients of the potential risks.[25]

In Part VII, this articles poses some questions about the future of protecting clients' trade secrets and other highly proprietary information from government surveillance and via back doors from competitors' or other hackers' intrusions. Risks to confidential and privileged data point to the need for some restraint, if technologically feasible, on collection by the NSA, FBI and other agencies, of communications involving lawyers and law firms with clouds. Alternatively, risks point to a need for post-collection minimization policies that federal agencies ought to implement or be forced to implement by the Obama Administration or Congress. This part recommends that lawyers and law firms may have no alternative but to revert to relatively old-fashioned approaches to protecting clients' data that is confidential or privileged despite the efficiency and economy of the cloud. These methods include in-person conversations, physical storage of tangible records with proper physical and administrative safeguards in place to protect them – as well as a really good map of where the records are stored, and such old-fashioned ideas as using manual typewriters for the most sensitive communications, such as clients' patent applications and merger and acquisition plans.

II. THE 2012 AMENDMENTS TO THE MODEL RULES OF PROFESSIONAL CONDUCT

Our 2011 *Red Skies* article included extensive analysis of core duties included in the 2007 version of the MRPC,[26] particularly, the duties to:

- provide competent representation and, accordingly, to stay abreast of new technologies and uses of technologies;[27]

- obtain clients' informed consent to the use of cloud storage for communications with and documents belonging to clients, including attorney work-product on client matters;[28]

25. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2007).
26. Trope & Hughes, *supra* note 4 at 137-63.
27. *Infra* at text accompanying notes 57 to 96.

- protect confidential information and privileged communications from "inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client" by use of reasonable efforts.[29] And,

- communicate with clients on various aspects of the representation.[30]

Amendments to the main text or to the comments accompanying the MRPC incorporated in the 2012 amendments to the MRPC[31] adjust some of the duties.

A. Rule 1.1 Competence

In *Red Skies,* Mr. Trope and I argued that Rule 1.1's mandate for "competent representation" included a duty to stay abreast of new technologies and of risks related to the use of technologies.[32] New Comment [6] to MRPC 1.1 now mentions those duties explicitly:

> [6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology,</u> engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[33]

B. Rule 1.4 Communication

Rule 1.4 was not amended by the American Bar Association in 2012. It still reads:

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

---

28. *I Infra* at text accompanying notes 97 to 138.

29. AM. BAR ASS'N COMM'N ON ETHICS 20/20, *Initial Draft Proposals on Lawyers' Use of Technology and Client Development* 5 (2011), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20110629ethics202technologyclientdevelopmentinitialresolutionsandreport.authcheckdam.pdf.

30. MODEL RULES OF PROF'L CONDUCT R. 1.4 (2012).

31. AM. BAR ASS'N COMM'N ON ETHICS 20/20, *Report to the House of Delegates*, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf (last visited Apr. 4, 2014).

32. Trope & Hughes, *supra* note 4 at 154.

33. MODEL RULES OF PROF'L CONDUCT R. 1.1, cmt. 6 (2012) (underlining in original demonstrates changes from the 2007 text).

(2) consult with the client about the means by which the client's objectives are to be accomplished;

(3) reasonably keep the clientinformed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.[34]

Comment [4] to MRPC 1.4 also was amended in 2012,[35] but not, in my view, in a manner that alters the recommendations that Mr. Trope and I made in *Red Skies*.[36]

Comment 16 to MRPC 1.6 requires lawyers to recognize the risks that technology poses, particularly where a third party might have access to the information.[37] Our 2011 article concluded that "… in addition to recognizing risks, to competently safeguard information, the lawyer must similarly assume and provide for the fact that third-party communications providers are not likely to protect client information as zealously as the client's advocate should."[38]

Rule 1.6 Confidentiality of Information now reads:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

---

34. MODEL RULES OF PROF'L CONDUCT R. 1.4 (2012).

35. MODEL RULES OF PROF'L CONDUCT R. 1.4, cmt. 4 (2012) ("Client telephone calls should be promptly returned or acknowledged," was replaced by "[A] lawyer should promptly respond to or acknowledge client communications.").

36. Trope & Hughes, *supra* note 4 at 137-51.

37. MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. 16 (2007). *See also* ABA Formal Op. 08-451, *supra* note 12 (concluding that a lawyer may outsource support services, but recognizing that the lawyer ultimately remains responsible for rendering competent legal services to the client).

38. Trope & Hughes, *supra* note 4 at 154, citing New York Op. 842, NEW YORK STATE BAR ASS'N COMM. ON PROF'L ETHICS, Formal Op. 842, ¶ 5 (2010) [hereinafter New York Op. 842], *available at* http://www.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions825present/EO_842.pdf, for the proposition that the exercise of "reasonable care" does not require that the lawyer "guarantees that the information is secure from *any* unauthorized access."

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(6) to comply with other law or a court order.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. [39]

I would make two observations in particular about MRPC 1.6. First, Rule 1.6(a) does not contain a qualifying subjective mental element, which its 2007 predecessor also lacked.[40] The continued absence of a "knowing" requirement in Rule 1.6(a) means that, absent informed consent, the lawyer shall not reveal information relating to the representation.[41]

Second, new MRPC Rule 1.6 (c) creates a duty that requires lawyers to recognize the issues related to drafts stored in the cloud. These issues include, at the minimum, prospects that (1) copies of all documents are made each time that a document is moved to the cloud, and (2) standard cloud storage protocols use

39. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).
40. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).
41. Trope & Hughes, *supra* note 4, at 152.

back-up storage of multiple copies of documents.[42] Regrettably, lawyers may have no knowledge, at any given time, how many copies of a file exist and where those copies may be stored. Copies effectively are all individual documents for purposes of e-discovery, whether or not the lawyer or firm knows of their existence. Copies also potentially "reside" in different jurisdictions or nations (where privacy and security laws may demand different protections, including no protection at all for data originating outside their borders). Copies also may become unavailable via outages to the cloud servers at critical moments with no indemnification or reimbursement for associated injuries likely forthcoming from the cloud providers.[43] These facts complicate the lawyer's ability to recognize and control risks to clients' confidential and privileged documents and communications.

The Rule also appears to require awareness and, to the extent feasible, prevention of newer-age risks in choosing to store data in the cloud including both the risk of surveillance by government agencies in the U.S. and abroad[44] and risks of non-government penetration via the "back doors" introduced into certain electronic devices by U.S. agencies.[45] Given what we now know of the NSA's practices both alone and in collaboration with friendly intelligence services,[46] prevention could require abandonment of many technologically enabled efficiencies – such as conference calls or Skype calls in lieu of travel or of cloud-shared work products – in favor of old-fashioned communications and storage methods mentioned in Part VII of this article.

Accompanying new Rule 1.6(c) are amendments of comments [18] and [19].[47] Comment [18] to Rule 1.6(c) now provides:

C. Acting Competently to Preserve Confidentiality

> [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against <u>unauthorized access by third parties and against</u> inadvertent or unauthorized disclosure by the lawyer or other persons who are

42. Trope & Hughes, *supra* note 4, at 224-230.

43. *Id.* at 175-199 (discussion including provisions of cloud contracts on liability to their clients).

44. *See Spy Agency Tracked Passengers for Days through Free Wi-Fi at Major Canadian Airport: Report,* NAT'L POST, http://news.nationalpost.com/2014/01/31/spy-agency-kept-tabs-on-passengers-through-wi-fi-at-a-major-canadian-airport-cbc-report/ (last visited Apr. 20, 2014).

45. David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway into Computers,* N.Y. TIMES, Jan. 15, 2014, at A1, *available at* http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0 (reporting that, since "at least 2008," the NSA has implanted radio-frequency software on 100,000 computers worldwide with capacity to conduct surveillance and launch cyber-attacks, but that there is "no evidence" of its use inside the United States).

46. *See* Risen & Poitras, *supra* note 2.

47. MODEL RULES OF PROF'L CONDUCT R. 1.6(c), cmt. 18-19 (2012).

> participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take addition steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements on loss of, or unauthorized access to, electronic information is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own law firm, see Rule 5.3, Comments [3]-[4].[48]

New comment [19] to Rule 1.6(c) adds the last sentence to what had been in the 2007 comment:

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to

48. MODEL RULES OF PROF'L CONDUCT R. 1.6(c), cmt. 18 (2012) (underlining original in published text of amended comment 19).

> comply with other law, such as state or federal laws that govern data privacy, is beyond the scope of these Rules.[49]

The 2012 amendments also remind lawyers and law firms of their duties to protect documents and data covered by confidentiality or privilege rules that belong to former clients:

> **Former Client**
>
> [20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.[50]

Accordingly, lawyers' and law firms' duties to files, documents, data and communications extend beyond the representation and concerns over cloud storage apply to information archived in the cloud, to the same extent as they apply to active files and clients.

Based on the information that the NSA's surveillance of electronic communications has been ongoing for many years, it appears that files that lawyers and law firms archived in the past could be imperiled as well as more recently stored files.

D. Rule 1.15 Safekeeping Property

Finally, lawyers' duties to protect clients' property are based on Rule 1.15.[51] Subsection 1.15(a), among other things, provides that "… Other property shall be identified as such and appropriately safeguarded."[52] The duty to safeguard property "appropriately" is the key aspect of this Rule's relationship to cloud computing and other technology uses by lawyers and law firms for the purpose of this article.

In *Red Skies,* Mr. Trope and I pointed out that outages in the cloud can render stored files unavailable for periods of time while the cloud provider recovers data, etc.[53] We also explained that lawyers and law firms can lose access to cloud-stored data by breaching their contracts with cloud providers.[54] Thus, the risk of losing access to documents temporarily or perhaps permanently in the event of a more massive cloud outage or dispute between the lawyer or firm and the provider should be considered when lawyers decide whether to store clients' most valuable documents in the cloud and in their choice of cloud providers.

---

49. MODEL RULES OF PROF'L CONDUCT R. 1.6(c), cmt. 18 (2012) (underlining original in published text of new comment 18).
50. MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. 20 (2012).
51. MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012).
52. *Id.*
53. Trope & Hughes, *supra* note 4, at 175-199.
54. *Id.* at 196-198.

This consideration is more important if the only or most recent copies are stored in the cloud, as a recent episode in North Carolina revealed. According to media reports, a Charlotte law firm suffered the loss of access to "its entire cache of legal documents to the malware program called 'Cryptolocker Trojan'" despite attempts by the principals to pay the $300 ransom the hackers demanded in a bid to have the documents unscrambled.[55] At least, according to the report, the malware only destroyed the ability to read the contents of the stored files, it apparently did not steal them.[56] However, this may be of less comfort to the firm because, assuming that the firm was entirely "paperless" as many strive to be, the firm lost documents of value to its clients and to its relationship with clients.

III. DID NSA DATA CAPTURE DESTROY ATTORNEY-CLIENT PRIVILEGE OR WAIVE CONFIDENTIALITY STATUS FOR CLIENTS' FILES AND DATA THAT LAWYERS AND LAW FIRMS STORED IN THE CLOUD?

In this part of the article, we come to the heart of concerns that explicitly relate to surveillance of communications, including telephonic and transmissions to cloud storage of files that lawyers hold or work on with clients. Privilege and confidentiality are separate concepts and will be discussed in turn below.

A. Attorney-Client Privilege and NSA Surveillance

According to a leading commentator on the attorney-client privilege, Professor Geoffrey C. Hazard, Jr.:

> The attorney-client privilege may well be the pivotal element of the modern American lawyer's professional functions. It is considered indispensable to the lawyer's function as advocate on the theory that the advocate can adequately prepare a case only if the client is free to disclose everything, bad as well as good. The privilege is also considered necessary to the function as confidential counselor in law on the similar theory that the legal counselor can properly advise the client what to do only if the client is free to make full disclosure.[57]

But Professor Hazard also observed that attorney-client privilege "is invoked to conceal legally dubious or dirty business. And when dubious or dirty business has been done, most likely someone has suffered as a result. In the nature of things, then the attorney-client privilege has its victims."[58] Moreover, he suggested:

---

55. *See* John E. Dunn, *Cryptolocker Scrambles US Law Firm's Entire Cache of Legal Files,* COMPUTERWORLD (Feb. 14, 2014), http://www.computerworlduk.com/news/security/3501150/cryptolocker-scambles-us-law-firms-entire-cache-of-legal-files/.

56. *See id.*

57. Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege,* 66 CAL. L. REV. 1061 (1978) *available* at http://scholarship.law.berkeley.edu/californialawreview/vol66/iss5/5.

58. *Id. a*t 1062.

> In the present-day law [circa 1978], the issue concerning the attorney-client privilege is not whether it should exist, but precisely what its terms should be. There is no responsible opinion suggesting that the privilege be completely abolished. Total abolition would mean that an accused in a criminal case could not explain his version of the matter to his lawyer without its being transmitted to the prosecution. Defense counsel would become a medium of confession, a result that would substantially impair both the accused's right to counsel and the privilege against self-incrimination. Hence, it is common ground that the privilege ought to apply at least to communications by an accused criminal to his counsel, in contemplation of defense of a pending or imminently threatened prosecution, concerning a completed crime. Beyond this there is controversy as to the proper scope of the privilege, although superficially the authorities are in substantial agreement. [59]

Against this backdrop, we have evidence of one of the most bizarre examples of surveillance of lawyer-client communications that has come to light recently. I speak of reports published in early 2014 that via its Australian counterpart, the Australian Signals Directorate, the Directorate received and shared with the NSA the fact of communications between the DC office of a major U.S.-based law firm and its client, the government of Indonesia, related to a trade dispute between the two governments.[60] Apparently, not only did the Signals Directorate pass the communications – so far unspecified in their form – to the NSA, the NSA reputed shared the communications with "a client," whose identity one can infer was the White House, Department of Commerce, or the Office of the U.S. Trade Representative, the counter-party in the trade dispute.[61]

There is a bit of good news that follows the revelations about capture of the communications between Mayer Brown, the firm reportedly involved, and its client. Following publication of the story, I discussed it with several faculty colleagues to obtain their sense of the damage to a client's actual privileged communications with its lawyer. Here is how one senior colleague responded:

> A privilege is personal property. It belongs to the person/corporation that made the communication. The person must have intended it to be confidential forever, and it must have been confidential in fact. Only the behavior of the holder of the privilege or their agents can waive it, expressly or implicitly or sometimes negligently. Therefore, in most jurisdictions, intercepted

59. *Id.* at 1062-1063. As background for the balance of his argument, Professor Hazard also cited Uniform Rules of Evidence Rule 26, the ALI Model Code of Evidence rule 212 (1942), and Proposed Federal Rules of Evidence rule 502, 51 F.R.D. 315 (1971). Uniform Rules of Evidence rule 26, at that time, provided that the lawyer-client privilege applies to "communications … between lawyer and his client in the course of that relationship and in professional confidence … unless the legal service was sought or obtained to commit or plan to commit a crime or tort …." Hazard, *supra* note 56, at 1063, citing UNIFORM RULES OF EVIDENCE rule 26.

60. Risen & Poitras, *supra* note 3.

61. *Id.*

> communications, even under warrant, are still privileged. But that only means that they cannot be used in court proceedings.
>
> If the information is communicated voluntarily or knowingly to a third party with whom the speaker does not have an independent privileged relationship, it is no longer privileged, although it may still be confidential for various regulatory purposes. [62]

A second colleague added the following useful perspective, among others:

> . . . When the NSA surrepticiously intercepts communications, this is not the kind of context in which a party purposefully or intentionally waives the confidentiality of their communication. Therefore, as a doctrinal matter, the notion of "waiver" should not be extended to apply to communications surrepticiously intercepted by the government. As well, from a practical and a policy perspective, the opposite rule would allow the government to intercept confidential communications – even in cases between plaintiffs and the government – and then argue that confidential attorney-client communications are not protected by attorney-client privilege. This seems problematic for a number of reasons.[63]

I asked a third colleague and he responded:

> . . . I think the federal approach is that where the law does not prohibit intrusion into a FISA A-C communication, the government nevertheless must take reasonable steps to protect any information collected, shared, etc. If there are Attorney General procedures on this topic it would be valuable to have the professional community review, comment, and advise on them.[64]

Thus, it would appear that communications between lawyer and client intercepted by the NSA or received by the NSA and other U.S. agencies should be entitled to lawyer-privilege if the issue arises in a court proceeding.[65] But a different rule might apply – though also might not be applied – not if the issue arises in another forum, like negotiations over a trade dispute. And, certainly, in negotiations the privilege may be less important than the loss of confidentiality for the information intercepted as to data or strategy.

---

62. Email from Law Professor, Indiana University Maurer School of Law, to author (February 24, 2014) (on file with the author).

63. Email from a second Law Professor, Indiana University Maurer School of Law, to author (February 24, 2014) (on file with the author).

64. Email from a third Law Professor, Indiana University Maurer School of Law, to author (February 25, 2014) (on file with the author).

65. *See supra* note 62; *see also supra* note 63; *see also supra* note 64.

B. Confidentiality and Documents Stored in Clouds and, Presumably, Subjected to NSA Surveillance

The North Carolina law firm described above at least did not have their files stolen, just rendered unusable by everyone, including their clients. Although unusable, the confidentiality of the files was (apparently) not breached.

But let's think about the other law firm whose communications and shared work products likely contained information about the trade dispute that the client government considered confidential. What happens now? Did the law firm violate the duty to keep clients' confidential data confidential?

As explained above, the 2012 Model Rules of Professional Conduct impose on lawyers' duties to keep clients' confidential information confidential. This duty is explained, once again, in the following terms by new comment [19] to Rule 1.6(c):

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state or federal laws that govern data privacy, is beyond the scope of these Rules.[66]

Presumably, before the 2013 Snowden releases about the scope of NSA's interceptions, lawyers and law firms might not have imagined that their telephonic communications would be intercepted and digested – or that no court would authorize such interceptions in the context of a trade dispute.

But how about in this post-Snowden environment? There are two options, apparently. First, the client may require the lawyer to employ special security measures. Second, the client may give informed consent to the use of communications means that do not comply with the requirements of Rule 1.6. Either way, the lawyer and his or her clients must have conversations about the new risks to confidentiality that NSA interceptions now pose – and come to an

66. MODEL RULES OF PROF'L CONDUCT R. 1.6(c), comm. (2012) (underlining original in published text of new comment).

agreement about how the client wishes communications to be handled and protected. As described above, the client must make an informed consent – and this means that the lawyer knows enough about various technologies and the risks they may present to enable a frank and thorough conversation about the risks before the client makes its decision. It means that many more lawyers will have to learn a lot more about certain technologies and follow the literature and jurisprudence about NSA and other government interceptions than ever before.

IV. SHOULD REVELATIONS ABOUT THE NSA'S ACTIONS AFFECT LAWYERS' USE OF CLOUD COMPUTING? WHAT LIMITS SHOULD BE PLACED ON FEDERAL AND STATE LAW ENFORCEMENT AGENCIES' ACCESS TO CLIENTS' DATA HELD BY LAWYERS AND LAW FIRMS IN CLOUDS?

Subpart A of this part briefly discusses enhanced risks to lawyers' use of telecom and cloud computing and storage flowing from the secret "back doors" that the NSA secretly introduced into commonly used electronics such as tablets and smart phones.[67] Subpart B introduces the 2012 American Bar Association Standards on Law Enforcement Access to Third Party Records.[68]

A. NSA Data Mining

Commentators have assumed that the "back doors" that the NSA introduced into electronics were intended to allow more surveillance by the NSA and FBI.[69] They also express concerns that the back doors enable hacking by many potential sources including possibly by clients' counter-parties.[70] The topic of demonstrate how data held by one government agency could be misused by hackers came up at a recent House Financial Services Committee hearing. During questioning about his agency's collection of consumer credit transaction records, Director Richard Cordray of the Consumer Financial Protection Bureau responded that he could not guarantee their safety to 100%.[71]

---

67. *See, e.g.,* Maloof, *supra* note 22 (reporting that the NSA has "backdoor access to all Windows software since the release of Windows 95" and tying the backdoors to "insistence by the agency and federal law enforcement for backdoor 'keys' to any encryption.").

68. Am. Bar Ass'n, *supra* note 20.

69. *See* Maloof, *supra* note 22.

70. *Id*. (report that the Windows "software driver used for security and encryption functions contains unusual features that give the NSA the backdoor access" and that "[s]uch access to the encryption system of Windows can allow NSA to compromise a person's entire operating system").

71. Richard Pollack, *Federal consumer bureau data-mining hundreds of millions of consumer credit card accounts, mortgages*, WASH. EXAM'R (Jan. 28, 2014, 6:13 PM), http://washingtonexaminer.com/consumer-bureau-data-mining-hundreds-of-millions-of-consumer-credit-card-accounts-mortgages/article/2543039 (explaining that hackers could "reverse engineer" data to find consumers to which records pertain).

B. ABA Standards for Law Enforcement Access to Third Party Records

One area of risk to the confidentiality and privilege of clients' documents and data that has been largely ignored since Edward Snowden's revelations about the NSA data-collection practices relates to other, *non-national security* law enforcement agencies. These agencies might be interested in clients' records and communications in connection with the prevention and investigation of crimes, including money laundering and tax evasion, completeness of responses to agencies' investigations into compliance with federal securities or commodities or consumer credit or privacy protection laws, or for other investigatory purposes.

Agency interest in data stored with various institutional parties, including law firms, implicates the "third party records" doctrine that the United States Supreme Court articulated from the 1960's to 1980's. This doctrine has come under criticism since the advent of email, global positioning devices, social media, and cloud computing. The two primary Supreme Court decisions related to the "third-party-records" doctrine are *United States v. Miller*,[72] and *Smith v. Maryland*.[73]

In response in part to growing concerns about telecommunications and other access to third-party records by all levels of government, the American Bar Association in 2012 updated its Standards for Law Enforcement Access to Third Party Records.[74] Of particular relevance to the topic of this paper are Standards 25-4.1 (Categories of Information), 25-4.2 (Categories of Protection), and 25-5.3 (Requirements for Access to Records). These rules provide:

1. Standard 25-4.1 Categories of information

> Types of information maintained by institutional third parties should be classified as highly private, moderately private, minimally private, or not private. In making that determination, a legislature, court, or administrative agency should consider present and developing technology and the extent to which:
>
> (a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;

---

72. 425 U.S. 435 (1976) (holding that no person should have a reasonable expectation of privacy in information they voluntarily conveyed to a third party).

73. 442 U.S. 735 (1979) (holding installation at telephone company offices and use of a pen register was not a "search" and required no warrant because the individual target of the pen register had no reasonable expectation of privacy in records at the telephone company offices).

74. AMERICAN BAR ASSOCIATION, *Law Enforcement Access to Third Party Records*, *in* ABA STANDARDS FOR CRIMINAL JUSTICE (3d ed. 2013), *available at* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf. These Standards are not applicable to access related to a national security investigation. *Id.* at 5.

(b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;

(c) such information is accessible to and accessed by non-government persons outside the institutional third party; and

(d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.

2. Standard 25-4.2 Categories of protection

(a) The type of authorization required for obtaining a record should depend upon the privacy of the type of information in that record, such that: records containing highly private information should be highly protected, records containing moderately private information should be moderately protected, records containing minimally private information should be minimally protected, and records containing information that is not private should be unprotected. If a record contains different types of information, it should be afforded the level of protection appropriate for the most private type it contains.

(b) If the limitation imposed by subdivision (a) would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost, a legislature may consider reducing, to the limited extent necessary to correct his imbalance, the level of protection for that type of information, so long as doing so does not violate the federal or applicable state constitution.

3. Standard 25-5.3 Requirements for access to records

(a) Absent more demanding constitutional protection, consent pursuant to Standard 25-5.1, and emergency aid and exigent circumstances pursuant to Standard 25-5.4; and consistent with the privilege requirements of Standard 5.3(c); law enforcement should be permitted to access a record maintained by an institutional third party pursuant to the following authorization:

(i) a court order under 5.2(a)(i) if the record contains highly protected information;

(ii) a court order under 5.2(a)(ii) [5.2(a)(iii) or 5.2(a)(iv)] if the record contains moderately protected information; or

(iii) a subpoena under 5.2(b) if the record contains minimally protected information.

(b) If the record contains highly protected information, a legislature, a court acting in its supervisory capacity, or an administrative agency could consider more demanding restraints for access to the record, such as additional administrative approval, additional disclosure, greater

> investigative need, or procedures for avoiding access to irrelevant information.
>
> (c) The protections afforded to privileged information contained in records maintained by institutional third parties and the responsibilities of privilege holders to assert those privileges are those provided by the law applicable in the jurisdiction in which privilege is asserted. The jurisdiction in which law enforcement obtains documents may impose obligations on both institutional third parties to protect what might be privileged information and on law enforcement with respect to the access to, and storage and disclosure of, such information.

To the extent that the NSA obtains this information in the course of its data-collection efforts, a further question arises about the extent to which the NSA should be entitled to access the full content and to share it with other law enforcement agencies without observing otherwise applicable legal process protections.[75] Standard 25-4.2 specifically mentions privilege among the factors that law enforcement should take into account in accessing data, but it is unclear that such niceties are being observed.

V. WHAT DATA SECURITY BREACH LAWS APPLY TO LAWYERS AND LAW FIRMS?

This part of this paper summarizes sources of data breach security law that generally applies to business enterprises, a classification that includes law firms in some cases.

---

75. *See* Risen & Poitras, *supra* note 3, at A 18. The reporters also stated:

> The [NSA] is barred from sharing with prosecutors intercepted attorney-client communications involving someone under indictment in the United States, according to previously disclosed N.S.A. rules. But the agency may still use or share the information for intelligence purposes.
>
> . . .
>
> . . . disclosures in recent months from the documents leaked by Mr. Snowden show the agency routinely spies on trade negotiations, communications of economic officials of other countries, and even foreign corporations.

Id. Risen and Poitras also cited the fact that the NSA, following interception of communications of Americans as the DC lawyers may be, is "required to follow so-called minimization rules to protect their privacy, such as deleting the identity of Americans or information that is not deemed necessary to understand or access the foreign intelligence before sharing it with other agencies." *Id.*

A. State Data Security Breach Laws

Lawyers and law firms are subject to a multitude of non-uniform state data security breach laws,[76] as well as, depending on the nature of the data, federal laws including HIPPA,[77] and other guidance from the federal government, such as the FFEIC Guidance.[78]

Legislation requiring private entities, or government entities subject to their jurisdiction, to notify individuals of data security breaches that involve breaches of information that includes personally identifiable information, has been enacted by 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.[79] States with no security breach laws include Alabama, Kentucky, New Mexico, and South Dakota.[80]

Security breach laws typically have provisions regarding who must comply with the law (*e.g.*, businesses, data/ information brokers, government entities, etc.); definitions of "personal information" (*e.g.*, name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (*e.g.*, unauthorized acquisition of data); requirements for notice (*e.g.*, timing and method of notice, who must be notified); and exemptions (*e.g.*, for encrypted information).[81]

Lawyers' and law firms' ability to rely on the "safe harbors" for encrypted data that appear in state data security breach laws[82] appears to be diminishing proportionately to the new risks that arise as the NSA pursues encryption-breaking capacities.[83]

---

76. *See* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 382 (2006) (outlining the numerous differences in state data security laws).

77. *See generally* The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified variously in 42 U.S.C.).

78. *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *Data Security,* IT EXAMINATION HANDBOOK INFOBASE, http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/data-security.aspx (last visited May. 8, 2014).

79. NAT'L CONFERENCE OF STATE LEGISLATURES, *State Security Breach Notification Laws,* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (updated as of Jan. 21, 2014) (last visited Mar. 29, 2014). A listing of the citations to these state laws is in Appendix 2 to this paper.

80. *Id.*

81. *Id.* However, not all States define the term "encryption" and, when defined, the standards are not uniform. *See* Eric Hibbard, *Data Breaches and the Encryption Safe Harbor*, at 25, 2012 power point presentation, STORAGE NETWORKING INDUSTRY ASSOCIATION, *available at* https://www.snia.org/sites/default/education/tutorials/2012/fall/security/EricHibbard_Data-Breach-Encryption-Safe-Harbor_Final.pdf (citing Data Breach Laws: Will They Save or Sink You in a Massive Attack?, RSA Conference 2012, Session: LAW-203 (February 2012)).

82. *See* BAKER & HOSTETLER LLP, *Data Breach Charts* (2013), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (listing states with data breach notification requirements).

83. Steven Rich & Barton Gellman, *NSA Seeks to Build Quantum Computer that Could Crack Most Types of Encryption,* WASH. POST (Jan. 2, 2014), http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-

B. Federal Trade Commission Section 5 Jurisdiction

In addition, lawyers and law firms are subject to the jurisdiction of the Federal Trade Commission (FTC) and its "unfair and deceptive acts or practices in commerce" jurisdiction under section 5 of the Federal Trade Commission Act.[84] The FTC has not yet used this jurisdiction against lawyers or law firms that experienced a data security breach. The FTC has used Section 5 against corporations in its jurisdiction that have suffered data security breaches, including its June, 2012 complaint against the collection of affiliates that own and operate Wyndham hotels.[85] Paragraph 2 of the Complaint summarizes the basis for the FTC's action:

> Defendants' failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels franchised and managed by Defendants on three separate occasions in less than two years. Defendants' security failures led to fraudulent charges on consumers' accounts, more than $10.6 million in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia. In all three security breaches, hackers accessed sensitive consumer data by compromising Defendants' Phoenix, Arizona data center.[86]

As a result, lawyers and law firms who fail to maintain reasonable security and whose failure "allows" unauthorized persons to gain access to their networks, documents stored in clouds, or long-term archives cause injury to their clients, could be vulnerable to suit by the FTC as well as by their clients.

C. Other Sources of Data Breach Liability for Lawyers and Law Firms

1. The 1995 EU Data Protection Directive

Law firms that operate in the European Union as well as the United States – or who have clients who reside in the European Union's states – should already be familiar with the 1995 EU Data Protection Directive.[87] The Directive prohibits transfer of data pertaining to residents unless comparable data protection is afforded by the nation in which the transferee is located.[88] Disputes

---

encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html (expressing skepticism that the NSA has achieved its goal as of now).

84. 15 U.S.C. § 45(a) (2011).

85. *See* Complaint for Injunctive and Other Equitable Relief, F.T.C. v. Wyndham Worldwide Corporation, 2:12-cv-01365-SPL (D. Ariz. filed June 26, 2012).

86. *Id.* ¶ 2.

87. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

88. *Id.*

prior to the NSA data-gathering disclosures prompted the EU and United States to enter into an agreement providing procedures for enterprises in the United States to comply with the EU's requirements when they house or import data from the EU.[89]

Of fresh, post-Snowden interest to lawyers and law firms operating under the Safe Harbor or with intentions to do business in the EU or represent clients in the EU is the EU justice commissioner's recent call for bigger fines for breaches of European data security laws.[90]

And, lawyers should become aware of, to the extent that they are not already preparing to act on, proposals by Chancellor Angela Merkel of Germany to "create European data networks that would keep emails and other communications on the European side of the Atlantic, farther from prying American eyes…"[91]

2. Should Lawyers Consider Taking "Commercially Reasonable" Steps to Protect Data from Breaches and What Would Such Steps Entail?

In connection with their responsibilities and responsive strategies they may decide to employ, lawyers and law firms vulnerable to data security breach actions should ask themselves "what is commercially reasonable security?" As explained by one commentator,

> As most data breach class actions have been dismissed for lack of damages, courts generally have not examined what might constitute reasonable data security when [private] plaintiffs allege negligence. Although several states have data security laws that require businesses

89. For comprehensive information about the "safe harbor" requirements, see *Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018365.asp (last visited Apr. 8, 2014). For text of the EU document approving the safe harbor agreements, see 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance), *available at* http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0520. Among the requirements is a condition on "onward transfers" of data, which may occur only to organizations that follow adequate data protection principles. *Id.* It would seem that the NSA and its contractor who employed Snowden would be ineligible for the safe harbor.

90. *See EU Calls for Much Bigger Fines for Data Breaches*, BBC NEWS TECH. (Jan. 21, 2014), http://www.bbc.com/news/technology-25825690 (reporting on statements by Viviane Reding, Commissioner of Justice of the European Union & Vice President of the European Commission, about plans to create a single EU regulator and to impose much larger fines for data security breaches). The EU is also considering proposals to prevent European data from being shared with another country in response to Edward Snowden's allegations. *See id.* Recent fines levied against Google in the EU exceeded 1.05 million Euros. *See* Lee Munson, *EU Commissioner Calls for Larger Data Security Breach Fines* (Jan. 22, 2014), http://nakedsecurity.sophos.com/2014/01/22/eu-commissioner-calls-for-larger-data-breach-fines/.

91. Alison Smale, *Merkel Backs Plan to Keep European Data in Europe,* N.Y. TIMES,Feb. 17, 2014, at A6.

> to adopt reasonable security measures to protect personal information . . . [t]hose statutes do not define what constitutes reasonable data security. However, in a different context, the First Circuit recently addressed reasonable security under Article 4A of the Uniform Commercial Code. In a case that likely will have wide ranging implications for financial institutions and perhaps other businesses, the court in *Patco Construction Co. v. People's United Bank* held that a bank failed to provide commercially reasonable security to protect a consumer from fraud. The security procedures proved commercially unreasonable, in part, because the bank posed the same challenge questions for high-risk transactions that it did for ordinary transactions, which was particularly troubling given the prevalence of key-logging malware, about which the bank had been cautioned by its consultants.[92]

The court's fact-intensive opinion demonstrates that the *crux* of security procedures will be the use – serious or superficial – a bank, or any business, makes of them.[93]

Another commentator made two other highly instructive observations about the First Circuit's holding in *Patco*.[94] He noted, first, that failure to take action when a security alert triggers a security protocol, not only "may render security procedures 'commercially unreasonable' under the U.C.C. Article 4A and, second, that it "may deprive an originator's bank of the risk allocations and liability limits it sought in its online banking agreement with its customer."[95] Translating the sage counsel offered by both of these commentators, lawyers and law firms should be certain that they comply with any cybersecurity policies they establish, they re-evaluate how well they work periodically, and conduct regular training and re-training of all personnel to ensure maximum utility of their policies.

3. Domestic Laws

Other prospective liability may arise under common law negligence, per se negligence, breach of contract, the common law covenant of good faith and fair dealing, and unjust enrichment/restitution.[96]

VI. WHAT RESPONSIBLE STRATEGIES AND STEPS CAN LAWYERS AND LAW FIRMS CONSIDER IN RESPONSE TO THREATS POSED

92. John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 206 (2013) (footnotes omitted) (citing Patco Constr. Co. v. People's State Bank, 684 F. 3d 197 (1st Cir. 2012)).

93. *Id*.

94. Roland L. Trope, *Bearings from the Southern Cross: Cybersecurity Decisions 2012-2013,* 69 BUS. LAW. 189, 190 (Nov. 2013).

95. *Id.* at 190 (footnotes omitted).

96. Black, *supra* note 92, at 201-202.

BY HACKERS AND GOVERNMENTS?

The NSA revelations should challenge lawyers' and law firms to do more to secure the communications they have with and work-product and client-related documents they may have in storage or transmission. The 2012 Amendments to the MRPC raise the stakes for law firms in terms of protecting data and obtaining informed consent.[97] Surveillance activities like the NSA's also increase the problems that lawyers and law firms have in dealing with risks to data security and in responding to hacking incidents and internal data theft in terms of state- and EU-enacted data security breach notification responsibilities.

Additionally, high-profile data security breaches, such as that experienced by Target in late 2013, demonstrate that breaches can be perpetrated via vulnerabilities that exist in the systems of vendors whose software is allowed to interface with too many internal systems of their customers.[98]

President Obama's January 17, 2014 Directive on Signals Intelligence[99] does not reduce concerns related to files sent among computers, tablets, and other media that we identified in *Red Skies* in 2011. Its failure to prohibit future actions such as the NSA-introduced "back-door" vulnerabilities also enhances risks to law firms' and lawyers' communications and clients' data and files. The current state of play in the United States does not relieve lawyers and law firms in the United States from duties they have if they hold data pertaining to residents of the European Union or Canada from storage where it is accessible by the NSA contrary to EU provisions, and it does not absolve them from liability under the data security breach laws of the States or the European Union, described briefly in this article. This is in part because the penetration of firm-applied encryption undercuts lawyers' and law firms' ability[100] to qualify for "safe harbors" found in many data security breach notification laws here and abroad.[101] It does nothing to quell concerns that Americans' communications with clients abroad will be protected by suitable minimization procedures or stopped when the

97. *See supra* text accompanying notes 26-46.

98. *See* Mathew J. Schwartz, *Target Breach: Phishing Attack Implicated,* INFO. WEEK (Feb. 13, 2014), http://www.informationweek.com/security/attacks-and-breaches/target-breach-phishing-attack-implicated/d/d-id/1113829 (mentioning a Pennsylvania-based HVAC vendor); Nicole Perlroth, *Heat System Called Door to Target for Hackers,* N.Y. TIMES (Feb. 5, 2014), http://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html?_r=0 (reporting that vendors may have remote access to systems that create vulnerabilities).

99. Presidential Policy Directive/ PPD-28, *supra* note 23.

100. *See Cracked Credibility,* THE ECONOMIST (Sep. 14, 2013), http://www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and; *N.S.A. Able to Foil Basic Safeguards of Privacy on Web,* N.Y. TIMES (Sep. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1.

101. *See* BAKER & HOSTETLER LLP, *supra* note 82 (providing information about states that link their data security breach notification "safe harbors" to data encryption). Numerous states limit application of their notification requirements to data that is not encrypted (e.g., Ohio, Arkansas, Delaware, Florida, Georgia, Hawaii, Kansas, Massachusetts). *Id.* at 15-17.

communications involve sensitive issues that traditional concepts of privilege and confidentiality are implicated.

The stakes are about to become greater for lawyers and law firms. Relatively new demands by clients for their outside law firms to undergo cybersecurity audits adds to the pressures on lawyers and law firms to get their cybersecurity houses in order. In mid-2013, press reports revealed that Bank of America Merrill Lynch was "auditing the cybersecurity policies at its outside law firms, partly under pressure from government regulators."[102] This raises the question, as one commentator put it, "Would Your Firm Pass A Data Security Audit?"[103] Target's experience demonstrates that firms should consider whether their vendors will subject them to security breaches.[104]

All told, the revelations about the scope of the U.S. government's surveillance of telecom and other data and its "back door" capabilities, breaches at retailers such as Target, and the heightened responsibilities set forth in the MRPC should cause law firms and solo practitioners to (a) review their current data security policies and facilities and breach notification protocols and (b) re-think where and how files and data related to active projects as well as to archived projects should be managed and stored. The most sensitive data, legally and from the perspective of risks to the firm's reputation, should be reviewed and stored the most carefully to maintain the greatest degree of protection for the confidential and privileged information it contains.

To evaluate what advice lawyers and law firms already may have about how they may satisfy their duties under the MRPC, described above, to protect clients and their data, I surveyed advice given recently in public forums to lawyers and law firms seeking to fulfill their important data-protection responsibilities. From the plethora of sources of such advice, I identified tasks that lawyers and firms might be encouraged to take to ensure greater protection for their clients' and the firm's data as well as some corollaries. The most salient recent pieces of advice encourage lawyers and law firms to:

1. Understand what types of data you hold on clients' behalf, and the relative risks that each type of data may present.

---

102. Sharon D. Nelson & John W. Simek, *Clients Demand Law Firm Cyber Audits*, LAW PRAC. MAG., Nov. 2013, http://www.americanbar.org/publications/law_practice_magazine/2013/november-december/hot-buttons.html (providing a 17-step program for law firms to survive clients' cybersecurity audits of their data policies).

103. *See Would Your Firm Pass A Data Security Audit?,* LAWBIZ MGMT. (Jul. 11, 2013), http://www.lawbiz.com/coachs_corner_7-11-2013.html (providing a very brief checklist of the major categories of services and storage that lawyers should check on as they evaluate how secure their data and conduct is, including "enterprise security," "wireless security," "cloud security," "email security," and "insurance coverage.").

104. *See generally supra* note 98.

For example, one expert suggests classifying data in terms of three levels of sensitivity and reviewing whether the security procedures are sufficient in light of the differing risks.[105] These classes include: "public" information that is accessible to the public and that poses little risk to the firm's reputation, including information on the firm's public website;[106] "sensitive or confidential" information that could have a moderately adverse effect on the firm's reputation such as data covered by non-disclosure agreements, competitive market research, and the like;[107] and "restricted" information that poses the highest risks to reputation including HIPPA data, non-public personal information about clients, employees and clients' counter-parties, or the formula for Coca Cola.[108]

But even more importantly, to understand where information relative to operational issues (how many people need to staff a project in a company) and

2. Decide where the highest-value data should be stored and how access to it will be protected. One basis for choosing private clouds, as opposed to public clouds, for high-sensitivity data is that if a government agency or other person wants access to it via a form of legal process, at least the firm knows about it.[109]

3. Identify the cloud computing adoptions across the office or firm and the identity and the terms on which each cloud provider is operating with your office or firm.[110]

4. Determine which providers are involved in public and private clouds in use or that have been used. Read the contracts with each provider and any amendments to them since original execution.[111]

---

105. Karen Deuschle, *Five Things Your IT Department Wants You to Know About Data Security*, CORP. COUNS. CONNECT (Jan. 2014), https://info.legalsolutions.thomsonreuters.com/signup/newsletters/corporate-counsel-connect/2014-jan/article5.aspx [hereinafter *Five Things*].

106. *See id.*

107. *See id*.

108. *See id.*

109. *See* John P. Mello, Jr., *NSA Revelations a Mixed Bag for Private Clouds*, CSO ONLINE (Aug. 14, 2013), http://www.csoonline.com/article/738084/nsa-revelations-a-mixed-bag-for-private-clouds (citing Steve Weis, CTO and co-founder of PrivateCore). According to Von Welch, Deputy Director of Indiana University's Center for Applied Cybersecurity Research, the security of the cloud depends "technically on the acumen of those running the cloud." Email from Von Welch to Sarah Jane Hughes (Feb. 2, 2014) (on file with the author).

110. *See* Matt Asay, *IT's Losing Battle Against Cloud Adoption*, READWRITE.COM (Jan. 31, 2014), http://readwrite.com/2014/01/31/it-losing-battle-cloud-adoption-enterprise#awesm=~oA0MDGBXRcSHif (estimating that IT departments underestimate cloud adoptions within their firms "by about 10 times" and that many firms use public clouds such as AWS "without officially acknowledging it").

5. Raise all employees' understanding of the importance of strong data security habits. One commentator suggests specific annual training programs, as well as other steps such as requiring different passwords for different sites or applications, restricting software downloads to trusted sites, verifying installation of anti-virus software and firewalls, and locking computers before leaving them (even for short periods) and not storing sensitive data on removable media.[112]

6. Consider the affect on representation of clients if the storage services your firm uses, whether internal, outsourced, or in the cloud, became unavailable or was compromised.[113]

7. Create a master protocol that addresses various aspects of data management and security, including non-technical legal requirements for privacy rights, non-U.S. and out-of-state data security standards and breach notifications, and the like. This could include the firm's business continuity plan, disaster recovery plan, incident response plan, physical security plan, and bring-your-own-device/ bring-your-own-network policies.[114]

8. Be prepared for requests by clients for the firm to undergo an information security audit.[115]

9. Consider the greater risks of having computing devices on higher floors of buildings because the computer's emanations become easier to intercept.[116]

10. Expect data security vigilance from everyone in the firm and take prompt corrective action including re-training or sanctions against those who do not meet protocols or expectations.[117]

---

111. *See* Trope & Hughes, *supra* note 4, at 185-198 (discussing different cloud providers' contracts and their amendments to 2011).

112. *See id.*

113. *Id. See also Five Things*, *supra* note 105. Ms. Deuschle also recommends asking about the certifications that the cloud service provider you use or plan to use may have – viz., SOC 1, SOC 2, or SOC 3, ISO 27001, NIST 800-53, and CSA's Security, Trust & Assurance Registry (known as STAR) as well as asking whether the provider performs regular "penetration tests" using independent firms to identify risks in the application so that remedies can be devised before the breach can occur. *See id.*

114. *See* Nelson & Simek, *supra* note 102.

115. Event Announcement, *Surviving a Law Firm Information Security Audit,* THE AM. LAW INST. & THE AM. BAR ASS'N LAW PRAC. DIVISION, Feb. 24, 2014, http://www.ali-cle.org/index.cfm?fuseaction=courses.course&course_code=TSVM14. *See also* Nelson & Simek, *supra* note 102.

116. See Trope & Hughes, *supra* note 4, at 148 (citing Michael A. Caloyannides, *Forensics is so "Yesterday"*, IEEE SECURITY & PRIVACY, Mar.-Apr. 2009, at 21).

117. *See Five Things, supra* note 105.

11. Consider, if the client base includes clients not domiciled in the United States, the additional ethical requirements placed on lawyers and firms operating where those clients are based, and the likelihood that clients – or their governments – will demand that data related to their interests and persons be stored where it can enjoy the highest degree of protection from U.S. government surveillance.

12. Create and maintain a diagram showing where the firm's data is stored.[118]

13. Never let control of your digital assets out of your sight.[119]

14. Never give an order for security that you cannot obtain or you know will be disobeyed.[120] Users seek short cuts. Law firms are not likely to be different.

15. Law firms and lawyers should not bring any client data on laptops to meetings abroad and do not seek to receive client data while they are abroad, particularly if the travel involves certain nations more inclined to search electronics at their borders, such as the United States and China. Care also occasionally mandates routing of travelers who have knowledge of significant high-value details away from certain nations if they are traveling with or have substantive personal knowledge of trade secrets and the like.[121]

16. Do not assume that encryption is as much in use as you might use it.[122]

And,

17. Whatever else lawyers or law firms may do to protect their clients, never take clients' privileged or confidential data from the office on a laptop and then leave the laptop unattended.[123]

However helpful the items on the list above may seem, the big question remains whether what lawyers and law firms do will satisfy lawyers or their clients that clients' documents and data stored in the cloud are safe from unexpected or excessive government access or from other unauthorized access.

118. *See* Nelson & Simek, *supra* note 102.
119. Cormac Herley, *More is Not the Answer*, SECURITY & PRIVACY, IEEE, Jan.-Feb. 2014, at 16.
120. *Id.*
121. Conversation with Roland L. Trope, February 2, 2014.
122. *See* Nelson & Simek, *supra* note 102.
123. Susan Gainen, *6 Rules for Protecting Confidential Information,* LAWYERIST (May 8, 2010), http://lawyerist.com/rules-for-protecting-confidential-information/.

Also, clients are likely to express concerns about whether their competitors, counter-parties and opponents will find it possible to access data stored in the cloud – despite justifiable claims of privilege or confidentiality – merely because these data have been placed in the hands of third parties who may consent, perhaps limited by contracts and perhaps not, to divulge the data stored with them.

VII. SOME LUDDITE-LEANING CONCLUSIONS

Recent events including the NSA data-mining programs, including the DC law firm-Government of Indonesia incident described above, and the late 2013 Target and Neiman Marcus data security breaches compel the conclusion that lawyers and law firms should rethink their uses of cloud computing generally, as well as the manner in which they protect all files, documents, and communications with clients, and to select means to store the most sensitive data and all privileged data somewhere that still enjoys more protection from government access and surveillance than data stored in the cloud. This is true, even as described above, the privilege can only be waived by the client – and not by government interception – for the purposes of criminal prosecutions.

These events strongly suggest that, for the most sensitive files and data, lawyers and law firms should revert to old-fashioned methods to protect client communications and safeguard clients' property, including confidential and other files. Such old-fashioned methods include using manual typewriters,[124] attending meetings in person as opposed to via teleconferences, Skype or telephone calls, and locking paper and electronic records in file cabinets in lawyers' offices and storing sensitive archives in actual warehouses (where the thief would need a good map or lots of time to find the high-value records they can access electronically otherwise). These *physical and administrative security measures* – in addition to *appropriate technical security measures* – will allow lawyers and law firms to control access to sensitive information in more effective, if less technology dependent ways. It also means that in the trio of possible means of securing data – *physical, administrative and technical safeguards* – that physical and administrative safeguards are no less important, and possibly more important and easy to enforce than the technical safeguards on which we have placed so much emphasis recently.

Enhanced security for communications with clients and for data stored also means renewing restrictions on the use of smart phones and tablets, laptops and off-site desktops, flash drives and other peripherals. These restrictions for confidential and privileged data and communications also include not using

124. *See Kremlin Security Agency to buy typewriters "to avoid leaks"*, BBC (Jul. 11, 2013), http://www.bbc.co.uk/news/world-europe-23282308 (explaining that the Kremlin Security Agency's decision to use typewriters is attributed to Edward Snowden's leaks of NSA policies and data and the unique "handwriting" that enables documents to be associated with each machine).

voicemail or similar systems that involve telecomm that the NSA, other governments or the client's competitors might be able to obtain. Does it make me sound like a Luddite? I imagine that it will to many readers – particularly proponents of the technology-solves-all approaches to efficiency and productivity issues.

Revelations about data mining by the NSA and the U.K.'s spy agencies also necessitates more robust conversations with clients about the sensitivity of their files and records and of their communications with lawyers. This means staying abreast of developments and sharing findings with clients, and involving them in the cost-benefit analyses of how and where to store files and records, and how to conduct necessary communications. The 2012 additions to MRPC Rule 1.6(c)'s comments also require consideration of steps the lawyer needs to be conscious of and prepared for in terms of compliance with state or federal data security breach laws so that they can obtain informed consent from their clients.[125]

There is no question that the NSA's metadata-collection program, as well as the published reports that the NSA can reach certain content elements as well as metadata in messages,[126] will make it much harder for lawyers and law firms to protect the confidentiality and privilege of their client's communications with them and other sensitive data from the government. Commentators have predicted that the "back doors" that the NSA has introduced also threaten to facilitate unauthorized access by hackers, and possibly by competitors.[127]

The NSA surveillance of telecomm and its introduction of radio-frequency-enabled "back doors" to many computing and telecomm devices chips away at the reasonable expectation of privacy in communications and document exchanges between lawyers and their clients that have provided the framework for access by government agencies to tangible records in the hands of third parties and for other purposes in "search and seizure" jurisprudence since *United States v. Katz*[128] and *United States v. Miller*.[129] In connection with MRPC Rule 1.6,[130] this recent knowledge alters otherwise applicable protections for documents, files and communications under domestic law and, at least equally

125. *See supra* text accompanying notes 53-57.

126. *See* James Ball, *Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data*, THE GUARDIAN (Jan. 28, 2014), http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data (assessing personal data being gleaned by the NSA and GCHQ in the United Kingdom).

127. *See, e.g.,* Jason Mick, *Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years,* DAILY TECH (Dec. 31, 2013, 12:36 PM), http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm.

128. 389 U.S. 347 (1967) (holding that warrantless wiretapping of public pay phones to obtain defendant's conversations violates reasonable search and seizure protections of the Fourth Amendment).

129. 425 U.S. 435 (1976) (holding that defendant had no expectation of privacy, and hence no Fourth Amendment protections, in records held by two banks with which he dealt for which subpoenas had been issued, and no right to suppression of evidence obtained).

130. MODEL RULES OF PROF'L CONDUCT R. 1.6(c) cmt. 17 (2012).

important, it alters or jettisons terms of otherwise applicable confidentiality agreements – among the factors cited in Comment 17 to be considered in determining the reasonableness of the lawyer's normal precautions.[131] After all, as one commentator observed: "Because … [cybersecurity] standards [such as ISO 27001] are not compulsory … your protection in court against legal redress always boils down to due diligence."[132]

To make that point even more relevant to lawyers and law firms, just as I was completing the draft of this paper for this symposium, the National Institute of Standards and Technology ("NIST") issued its newest standards, the Framework for Improving Critical Infrastructure Cybersecurity.[133] The Executive Summary summarizes reasons why diligent management of cybersecurity risk is important: "Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers."[134]

So, after looking at the issues raised by lawyers' professional responsibilities in the post-Snowden era, my mind keeps spinning through Joni Mitchell's famous, pre-Internet and pre-cell phone – and definitely pre-cloud computing and storage -- refrain*:*

> I've looked at clouds from both sides now,
> From up and down, and still somehow
> it's cloud illusions I recall,
> I really don't know clouds at all.[135]

Responsible steps that lawyers and law firms can take include all of the individual cyber-smart steps mentioning in Part VI of this paper and the additional steps mentioned by Nelson & Simek.[136] They also include old-fashioned, low-tech physical and administrative steps such as mentioned above.[137] And some of these low-tech steps are as old-fashioned as meeting in person to discuss ultra-sensitive issues, using manual typewriters, and locked filing cabinets or vaults to store clients' trade secrets, medical information, non-public personally identifiable information, and negotiations over mergers and acquisitions or the like. *Some of the responsible storage and communications of clients' records and data security practices really might not include clouds at all – even if it makes me unpopular with cloud computing vendors.*

---

131. *Id.*

132. *What is an appropriate auditing standard for a law firm?,* INFO. SECURITY STACK EXCHANGE (Feb. 14, 2011, 2:03 AM), http://security.stackexchange.com/questions/2083/what-is-an-appropriate-auditing-standard-for-law-firms.html.

133. *See Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, NATI'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

134. *Id.* at 1.

135. J JONI MITCHELL, BOTH SIDES NOW (Elektra 1969).

136. Nelson & Simek, *supra* note 102.

137. *See supra,* pp. 22-23.