The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms, and Judges[†]

By

Roland L. Trope[1] and Claudia Ray[2]

I. *Introduction: Ethical Challenges from New Communications Technologies.*

New technologies often bring new technical problems, and new ethical challenges. Although data leaks undoubtedly occurred at major corporations and financial institutions long before they became the subject of frequent headlines and a recurrent company Boardroom agenda item, few such leaks were publicly reported. This approach, which likely resulted from the fear of adverse publicity, has tended to result in a state of denial among senior management and an erroneous belief that tweaking, but not significantly changing, an enterprise's information security could be adequate.

As often happens, the external threats have evolved much faster than have the safeguards against them, due to the rapid evolution of communications technologies. Spurred by these changes, the law has changed as well in an effort to enforce ethical behavior in connection with new technologies. The advent of data breach reporting statutes, beginning in California, forced U.S. enterprises to disclose the frequency of leakages and the magnitude of data released, lost, or compromised, and motivated company management to pursue radical strategies for the protection of the most sensitive and valuable data. Nevertheless, leaks continue to occur, with the attendant legal and ethical consequences, due in large part to the proliferation of at least four kinds of digital-based technologies:

(i) portable, high density, data devices (*e.g.*, multiple gigabyte memory sticks and portable terabyte storage units);

(ii) wireless communications devices providing ubiquitous web site access (*e.g.*, smart phones that can surf the web and store reams of downloaded data, emails, and attached documents);

(iii) wireless data warehouses (*e.g.*, "cloud computing services" — the outsourced storage of data in server farms accessed wirelessly); and

(iv) online social media (*e.g.*, Facebook, YouTube, Twitter) that build upon, expand the use of, and enhance the markets for wireless web-access.

 This essay is an excerpt from Roland L. Trope and Claudia Ray, *Head in the "Cloud" – Feet on the Ground: Understanding the Ethical Challenges of Web 2.0 for Lawyers, Law Firms and Judges*, 2010, a book manuscript by the authors.

Acknowledgement: The authors want to thank Michelle Berger and Marlo Leach, summer associates at Kirkland & Ellis, LLP, for their excellent assistance, which included research, editing and substantive suggestions during the preparation of this essay.

Disclaimer: The views expressed in this essay are solely those of the authors and have not been approved by, and should not be attributed to, the United States Military Academy at West Point, the U.S. Department of Defense, or the U.S. Government.

[1] Partner in the New York offices of Trope and Schramm LLP. He can be contacted at rltrope@tropelaw.com.

[2] Partner in the New York offices of Kirkland & Ellis, LLP. She can be contacted at claudia.ray@kirkland.com.

Unfortunately, increased connectivity has also been accompanied by increased concentrations of sensitive and valuable data and increased vulnerabilities, making leakages and losses of such data inevitable. As an H&R Block executive recently explained, "'I had somebody ask me, 'Can you protect this piece of information?' I said, 'Yes, as long as you promise never to use it.'…'"[3] Moreover, the changes in the market for stolen data have led data thieves to focus their attacks on larger concentrations of personal identification information. As noted in a recent study by the Verizon Business RISK Team:

> The value associated with selling stolen credit card data have dropped from between $10 and $16 per record in mid-2007 to less than $0.50 per record today.
>
> As supply has increased and prices fallen, criminals have had to overhaul their processes and differentiate their products in order to maintain profitability. In 2008, this was accomplished by targeting points of data concentration or aggregation and acquiring more valuable sets of consumer information. The big money is now in stealing personal identification number (PIN) information together with associated credit and debit accounts. … Furthermore, PIN fraud typically places a larger share of the burden upon the consumer to prove that transactions are fraudulent. This makes the recovery of lost assets more difficult than with standard credit-fraud charges.[4]

The magnitude of the vulnerability of digital data held by businesses was confirmed in a September 2008 Department of Justice report concerning information security incidents experienced by businesses in 2005. It disclosed that "Critical infrastructure businesses detected 13 million [computer security] incidents (nearly two-thirds of the total). High risk industries detected more than 4 million incidents (a fifth of the total)." Moreover, "Ninety-one percent of the businesses that detected incidents and answered questions on loss sustained" either monetary loss or system downtime, and forty-one percent sustained both kinds of loss. It is reasonable to infer that data losses were of a comparable magnitude to those involving monetary loss, since theft of data is often required for theft of funds.[5]

Some companies have concluded that some of their security processes and structures were inadequate and obsolete, and have sought to improve their policies and procedures for information security and their guidelines for employees' use of online social media. For some, this has meant adopting a presumption that yet-to-be-classified data is sensitive and must be given strong protection.[6]

The reported data leaks and other technological incidents at major corporate and financial enterprises (and at many government entities) contrast sharply with the paucity of reports of such problems at law firms. Nevertheless, it is reasonable to infer that similar problems may well have occurred but not been reported in the media, and that law firms face the same or similar threats as do their clients. When such technical problems do occur, as

---

[3] M. Eric Johnson, Eric Goetz and Shari Lawrence Pfleeger, "Security through Information Risk Management", IEEE SECURITY & PRIVACY, July/Aug. 2009, at 49.

[4] C. David Hylender, "State of Cybercrime, 2009," 2009 DATA BREACH INVESTIGATIONS REPORT (Verizon Bus. Risk Team), at 5, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

[5] Ramona R. Rantala, "Cybercrime against Businesses, 2005", U.S. Department of Justice, Sept. 2008, http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf.

[6] As one company executive explained: "We also block our data, and we have established that if data is not labeled, then it is confidential by default." Johnson et al., *supra* note 3, at 49.

seems likely to happen with the advent of the new communications technologies, the risks of reputational damage may be compounded by the risks of ethical violations under the jurisdiction's applicable rules of professional responsibility.

Web 2.0 communications technologies have increased the opportunities for attackers who seek unauthorized access to data, both personal and corporate. As noted in a 2008 study by the European Network and Information Security Agency ("ENISA"),

> Web 2.0 – user generated content, rich user interfaces and co-operative, dynamic services – has also brought with it a new and extremely virulent breed of 'Malware 2.0'. A key motivation for this study is the link between Web 2.0 and the increase in drive-by' malware infections requiring no intervention or awareness on the part of the user. To give some idea of the threat posed, a Scansafe report analyzing malware trends reports that risks from compromised websites increased 407% in the year to May 2008."[7]
>
> The ENISA highlighted the tendency of Web 2.0 services to ask users to grant the service (such as an online social network) authorization to access a variety of their accounts without specifying in a precise way what, if any, security precautions have been implemented to prevent unauthorized access to the user's accounts: "Many Web 2.0 services ask users to delegate access credentials to, for example, email accounts or bank accounts. Currently, users often have to give away the highest level of privilege, e.g., unlimited, permanent access to all features of their email account rather than just time-limited access to their address book, to access a service. The lack of finer grained authorization is a barrier to the use of such applications and a serious risk for those who do.[8]

Apparently, an attacker was able to use similar information to gain access to multiple web-based applications in a May 2009 incident that Twitter recently acknowledged.[9] The attacker reportedly took advantage of the simplicity of Yahoo's web mail password recovery or re-set system and hacked into a Twitter administrative employee's email account.[10] The hacker apparently used information obtained in that account to gain access to the employee's Google Apps account, which contained "cloud computing services" such as Google Docs, Calendars and "other Google Apps Twitter relies on for sharing notes, spreadsheets, ideas, financial details and more within the company."[11]

Twitter reported that the breach did not involve any flaw in web apps, but instead was due to a failure to follow good personal security guidelines such as selection of a strong password. But this explanation overlooks the fact that Twitter relied on web-based – i.e., cloud computing – applications and that the attacker's additional penetration of Twitter's files appears to have been facilitated by Twitter's use of such applications and the linkage of the employee's

---

[7] European Network and Information Security Agency, Position Paper: WEB 2.0 SECURITY AND PRIVACY, *Executive Summary*, Dec. 2008, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_web2.pdf [hereinafter *ENISA Position Paper*].

[8] *Id.*, "Summary of Risks: Access and Authorisation."

[9] "Twitter, Even More Open Than We Wanted", http://blog.twitter.com/2009/07/twitter-even-more-open-than-we-wanted.html (July 15, 2009) [hereinafter *Even More Open*].

[10] Josh Lowensohn and Caroline McCarthy, "Lessons from Twitter's security breach", WEBWARE – CNET, http://news.cnet.com/8301-17939_109-10287558-2.html (July 15, 2009).

[11] *See Even More Open*, *supra* note 9.

Web 2.0 accounts. Since the password reset feature at Yahoo's and Google's web applications (like many other sites) operates by asking a set of personal questions in order to authenticate the user, who may select questions and give answers that can be derived from the information that he or she posts on social networking sites, hackers interested in attacking a company can target an employee and equip themselves with data drawn from a social networking site where the employee may have posted such information:

> Like the breach of Gov. Sarah Palin's Yahoo e-mail account last fall, security researchers guessed that Hacker Croll gained access to the Twitter employee's account using Google's password reset feature, which poses several personal questions to authenticate the user. Hacker Croll likely dug up possible responses by rooting through the Web for details on the assistant, then used those to reset the password to one only he knew.[12]

The attacker stole several hundred Twitter internal documents and then forwarded them to Web sites, such as TechCrunch, that decided to publish some of them despite objections by Twitter's legal counsel as well as retransmitting some to other sites.[13] Twitter's co-founder, Biz Stone, recognized the significance of this, stating that "as they were never meant for public communication, publishing these documents publicly could jeopardize relationships with Twitter's ongoing and potential partners."[14]

In the future, the likely proliferation of such incidents will require lawyers and law firms to be prepared to address serious, complex and difficult ethical issues. Considering such issues before the problem arises will help those affected formulate better responses when problems do arise, as well help to position firms to present credible defenses to claims that they violated the applicable rules of professional responsibility.

In this essay, we examine the ethical obligations that lawyers and law firms arguably have: (i) to understand the features and operations of new communications, storage and processing technologies, (ii) to become familiar with the emerging customs and practices of persons and organizations that use such technologies, and (iii) to assess the risks that the use of such technologies may pose for a lawyer's and law firm's efforts to comply with applicable rules of professional conduct. Our focus is on the recently adopted New York Rules of Professional Conduct ("NYRPC"), which went into effect on April 1, 2009.

We also assess some of the most serious ethical risks that lawyers and law firms may face when using Web 2.0 technologies for client-related work, in pursuing new clients, and in the course of leisure activities, as well as what precautions might be taken to diminish, if not

---

[12] Gregg Keizer, *Hacker break-in of Twitter e-mail yields secret docs*, COMPUTERWORLD, July 16, 2009, http://www.computerworld.com/s/article/9135591/Hacker_break_in_of_Twitter_e_mail_yields_secret_docs. Note that in one account the vulnerable password reset was in the Yahoo web mail, and in another the vulnerable password reset was in Google Apps. It may be that the hacker breached the password reset at both Yahoo's and Google's web-based applications.

[13] *See* Keizer, *supra* note 12; Michael Arrington, "Twitter's Financial Forecast Shows First Revenue in Q3, 1 billion users in 2013", TECHCRUNCH, July 15, 2009, http://www.techcrunch.com/2009/07/15/twitters-financial-forecast-shows-first-revenue-in-q3-1-billion-users-in-2013/. As one security expert, Andrew Storms, astutely noted, users would be safer if they did not select one of the default password questions, but typed their own (if permitted). Otherwise, giving a nonsensical or false answer would enhance the user's security, because then the attacker would not have access to such information posted on a social networking website by the user or one of the user's "friends". *See* Keizer, *supra* note 12.

[14] *See Even More Open*, *supra* note 9.

avert, such risks.

In considering these issues, it is important to bear in mind that ethical issues are inherently fact dependent, and at best one can only try reasonably to infer how the issues might be decided by a disciplinary body. We believe, however, that the greatest risks from Web 2.0 technologies will probably arise from inadvertent ethical violations that result from a lack of understanding of the operations and use of these technologies, as well as an underestimation of a lawyer's and law firm's obligations under the NYRPC. For example, a firm might not understand that it arguably has an obligation to conduct meaningful risk assessments of such technologies early and repeatedly in order to reach informed conclusions and ensure that those conclusions do not need to be changed in light of rapidly evolving technologies and practices. The true potential of new communications technologies often is not immediately clear.[15] Lawyers and law firms are well advised to be among the first to explore new communications technologies and the associated customs and practices, given their access to and custody of client confidential information and ethical obligation to protect such information.

II. *Ethical Challenges to Lawyers and Law Firms from Use of Cloud Computing.*

In this section, we review cloud computing technologies, discuss some of the ethical risks that they may create for lawyers and law firms, and suggest some measures that may help to minimize those risks.

A. *Cloud Computing Services*.

1. *Overview of the "Cloud" -- Features and Potential Benefits.*

For those old enough to remember it, the proliferation of personal computers into each office of a company was preceded by time-shared computing.

> Big, expensive computers were kept behind big glass walls, tended by shrouded acolytes. For the rest of us, it was 'keep your hands off.' You rented computation by the second for your dumb terminal.[16]

Before the advent of the Web, visionaries hailed the coming era of "desktop publishing," in which each office would boast a computer linked to nearby printers, enabling each member of an enterprise to publish in hard copy. The World Wide Web's emergence made "desktop publishing" into an unexpectedly short-sighted vision of what would become computer-aided dissemination, but it still promoted the decentralization of computing – each employee would have a terminal on their desk, and later each would have a laptop to take on business trips, on the daily commute, or for working remotely from home.

Today, the amount of data to be processed has become prodigiously large, and the need for company personnel to access it from nearly everywhere has become compelling. The costs of providing such capabilities is substantial, and once invested, a company is stuck with the processing capability even if it is underutilized and therefore an inefficient investment. In

---

[15] Twitter initially left many lawyers unimpressed, if not puzzled, by its use as a published diary of mundane activities, but its hidden potential has come to be appreciated following its use in emergencies (e.g., reporting by victims of the terrorist attack in Mumbai, India) and in political crises (e.g., the post-election protests in Iran).

[16] Robert W. Lucky, *Cloud Computing*, IEEE SPECTRUM, May 2009, at 27.

response to these challenges, several of the major high tech firms have built enormous server farms and are offering to take on the computer processing and information technology responsibilities for numerous corporate clients. Potential clients are being encouraged to scrap their in-house servers and save on the associated costs by outsourcing their data storage and processing to off-premises server farms that promise to provide each customer with access to its data and to no one else's. The promise is a "virtual computing environment that's dynamically allocated to meet user needs."[17]

Such services are loosely referred to as "cloud computing." This term cannot be precisely and reliably defined because cloud services and the meaning of the term "cloud computing" (and related terms and concepts such as "virtualization") are rapidly evolving. As the National Institute of Standards and Technology ("NIST") has observed,

> Cloud computing is still an evolving paradigm. Its definitions, use cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time.[18]

NIST's proposed working definition describes "cloud computing" as follows:

> [It] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[19]
>
> NIST identifies five essential characteristics of "cloud computing":
>
> 1. On-demand, customer-initiated service that provides server time and network storage "as needed automatically";
> 2. Ubiquitous network access from thin or thick client platforms (*e.g.*, mobile phones, laptops, and personal computing devices);
> 3. Computing resources that are pooled to serve all customers with "different resources dynamically assigned and reassigned" according to customer demand;
> 4. Computing capabilities that can be rapidly and elastically provisioned allowing the customer to scale up or down its use of such capabilities accordingly to its needs and paid for on a as-used basis; and
> 5. Measured services that can be monitored, controlled and reported to the provider and the customer of the utilized service.[20]

A major objective of cloud computing is the linkage and integration of the numerous computing devices that are purchased for specialized tasks so that the data stored on each and the processing each performs can be done on commands from portable or office-based (or

---

[17] Lori M. Kaufman, "Data Security in the World of Cloud Computing," IEEE SECURITY AND PRIVACY, July/Aug. 2009, at 61.

[18] Peter Mell and Tim Grance, DRAFT NIST WORKING DEFINITION OF CLOUD COMPUTING, June 1, 2009, at 1, http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

[19] *Id.*

[20] *Id.*

home-office based) devices. "Cloud computing means that information is not stranded on individual machines; it is combined into one digital 'cloud' available at the touch of a finger from many different devices."[21]

Three delivery models for cloud computing have been developed:

(i) Cloud "software as a service" that lets customers use various applications running on a cloud infrastructure that are accessed from the customer's own devices through an interface such as a Web browser. The customer odes not manage or control the underlying cloud infrastructure, network, servers, operating systems, and storage, and thereby gives up knowledge of, and the ability to monitor or improve, the security of its data and data processing to the extent that it deploys them to the cloud.

(ii) Cloud "platform as a service" allows customers to deploy in the cloud infrastructure any applications they have created using programming languages and tools that the service provider supports. The customer turns management and control over the underlying cloud infrastructure, but may retain control over applications it has created and deployed to the cloud.

(iii) Cloud "infrastructure as a service" enables customers to use cloud resources such as processing, storage, and networks for the operation of their arbitrary software (such as operating systems and applications). The customer relinquishes management and control over the underlying cloud infrastructure, but may retain control over its operating systems, storage, deployed applications and possibly some of the networking components (such as firewalls) and thus entrusts less of the security safeguards to the cloud provider.[22]

Unless otherwise specified, most reports concerning cloud computing tend to refer to cloud "software as a service." Such services typically are marketed as "pay-per-use" with projections of substantial cost reductions because they replace costly, licensed software with purportedly less expensive access to software on an as needed basis. The charges are based on usage and allow for companies to scale up or down their use to fit their needs by accessing remotely stored programs instead of purchasing licensed software and upgrades. In essence, cloud "software as a service" is an outsourcing of data processing and storage that previously occurred within a customer's enterprise. Such services involve:

> provision of raw data processing power and storage capacity at times of need, or even to replace it altogether. Amazon.com has emerged as the unlikely leader in this business.[23] More than half the online bookseller's computing resources are being consumed by other companies, which run their own applications in its data centres … Customers include the New York Times and Nasdaq.[24]

---

[21] Steve Hamm, *Cloud Computing's Big Bang for Business*, BUSINESSWEEK, June 15, 2009, at 43.

[22] Mell and Grance, *supra* note 42, at 1.

[23] Amazon refers to its service by the awkward name of "Amazon Elastic Compute Cloud (Amazon EC2)", and states that "Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers." http://aws.amazon.com/ec2/

[24] Richard Waters, *Cloud Control*, FINANCIAL TIMES, March 25, 2009, accessed at http://cachef.ft.com/cms/s/0/c9e3bf12-1973-11de-9d34-0000779fd2ac.html?nclick_check=1.

Small to medium-size companies may benefit as they gain access to computing advantages previously available only to large companies, by "buying computing capacity from a 'cloud', rather like electricity from the grid."[25]

Two examples of cloud storage are "Amazon Simple Storage Service"[26] and Microsoft's Azure cloud computing platform, which is built on more than one million servers in the company's data centers[27] and charges "12 cents an hour for computing; 15 cents per gigabyte for storage and 10 cents per 10,000 storage transactions."[28]

In addition to the three kinds of delivery of cloud computing services, there are four different ways for such computing services to be deployed:

(i) "public clouds" operated by third-party providers and made available to the general public or a large industry group;

(ii) "private clouds" operated by companies that have the funds available to invest in off-site or on-site servers to serve their own personnel (or that can hire a third party to manage)[29]

(iii) "community clouds" located on-premise or off-premise, managed by the participating organizations or a third party, shared by participating organizations, and used to support a specific community that shares certain objectives (such as mission objectives, security requirements, or legal compliance requirements);[30] and

(iv) "hybrid clouds" composed of two or more clouds (private, public or community), each of which remains a separate entity, that are linked by shared standards or shared proprietary technology that enhances the portability and movement of data and applications.[31] For example, a "hybrid cloud" can be set up to allow a customer to operate and store data on its own private cloud, but in times of a surge in need for computing resources the customer can "burst" into and utilize

---

[25] *Gathering clouds*, THE ECONOMIST, March 21st, 2009, at 69.

[26] Amazon Simple Storage Service has been operating for three years. According to Amazon, "the service has grown to store over 52 billion objects and serve over 1 trillion requests per year from customers in over 90 countries." AMAZON SIMPLE STORAGE SERVICE (AMAZON S3), http://aws.amazon.com/s3/.

[27] Richard Waters, *Azure to boost Microsoft's online presence*, FINANCIAL TIMES, July 15, 2009, at 14.

[28] Jessica Hodgson and Scott Morrison, *"Cloud Computing" Prices Announced by Microsoft*, WALL ST. J., July 15, 2009, at B5. The same article reports that Amazon.com charges "12.5 cents an hour and 15 cents a gigabyte for storage in two of its pricing models."

[29] A recent report explained the distinction between public and private clouds as follows:

> "Thanks to ever more powerful chips and new software, servers and other hardware can now be 'virtualized', meaning physically separate systems can act as one. This enables computing power to become a utility: it is generated somewhere on the network ('in the cloud') and supplied as a service. To simplify their complex data centres and cut costs, more and more companies are thinking about building in-house computing utilities, called 'private clouds', or outsourcing computing to "public clouds" of the kind Sun [Microsystems] launched this week."

Gathering clouds, *supra* note 51.

[30] *See* Mell and Grance, *supra* note 41 at 2.

[31] *Id.*

> the resources of a "community cloud" or "public cloud" – a process known as "cloud bursting".[32]

Some observers predict that cloud-based computing will increasingly become the primary platform for Web applications.[33] Measured by the number of hours that they are accessed by users, cloud-based networks have already become a significant platform, and in some activities, the predominant platform.[34] According to the Aspen Institute's 2009 report, "Identity in the Age of Cloud Computing,"

> The cloud has become our entertainment network: we are spending hundreds of millions of hours on sites like YouTube, Hulu and Flickr. The cloud has become our social network: Facebook, MySpace, Bebo, hi5 and similar sites now claim hundreds of millions of members. The cloud has become our virtual library: when we do a Google search we are fingering the cloud. The cloud has become our workbench: we manage projects in Basecamp, share large files with Pando, tweak photos in online photo editors like Adobe Photoshop Express and Picnik, and edit videos online with JayCut and Jumpcut. The cloud has become our development network: open source programmers trade code on sites like *SourceForge.net* and *Drupal.org*."[35]

The promised benefits of cloud computing appear to have outpaced understanding of the attendant risks and what might be adequate safeguards against such risks. Such reported benefits include reduced costs, scalable use of resources, utilization of enhanced computer processing power, and almost ubiquitous availability by company personnel to company records and data. Other advantages include: "to flexibly experiment with new services, and to remove unneeded capacity when demand slackens. … The cloud is also easier to manage — you can install a single software patch to cover all of a company's users …"[36]

There are, however, serious risks, some known, some guessed at, and some that will probably arise and surprise even the vendors themselves. Technology vendors who know or suspect that risks exist may be reluctant to disclose them for fear that such disclosure would give prospective customers pause and thus undermine sales. Nonetheless, counsel should consider at least the currently known risks, particularly before they and their law firms adopt cloud computing and put themselves in a position to be not only early adopters of technology but potentially early victims of the ethical problems that cloud computing may generate.

2. *Potential Ethical Risks for Lawyers and Law Firms from Cloud Computing*.

The ethical risks for lawyers and law firms from cloud computing are most likely to originate from the security risks that cloud computing presents to all of its users, including risks from Internet facilitated breaches (malware, hackers, etc.), risks from careless or disgruntled

---

[32] For a discussion of "cloud bursting", *see Cloudbursting – Hybrid Application Hosting*, http://aws.typepad.com/aws/2008/08/cloudbursting-.html (Aug. 28, 2008).

[33] J.D. Lasica, Rapporteur, *Identity in the Age of Cloud Computing: The next-generation Internet's impact on business, governance and social interaction*, THE ASPEN INSTITUTE COMMUNICATIONS AND SOCIETY PROGRAM, Mar. 2009, at 9, http://www.aspeninstitute.org/publications/identity-age-cloud-computing-next-generation-internets-impact-business-governance-socia.

[34] The Pew Research Center reported in September 2008 that "69% of online Americans" use cloud computing services. *See* John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RESEARCH CENTER PUBLICATIONS, Sept. 12, 2008, http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

[35] *Id.* at 5.

[36] *See* Lucky, *supra* note 41, at 27.

insiders (resulting in data shared with unauthorized persons), and risks from state surveillance and interception under the auspices of legal authority. The discussion below focuses on public clouds, as it seems unlikely that law firms will initially set up their own private cloud (such investments are hard to justify during recessions and amidst widespread layoffs of personnel by law firms), or will find it practical at this time to negotiate participation in a legal community cloud or in a hybrid cloud.

a. *Security Risks Inherent in the Use of Public Clouds.*

Some of the mystery and confusion surrounding the concept of cloud computing can be eliminated by simply viewing it as a type of outsourcing. Certain risks can be predicted from the outsourcing experience, but many of the risks inherent in cloud computing are new and require an understanding of underlying features of the cloud that goes beyond what is needed in order to use cloud-based services. The cloud service providers themselves tend not to provide such information, however, and customers may be ill-equipped to assess the risks involved in placing sensitive data in the cloud.

One of BAE's deputy chief technology officers has reasoned that the cloud computing environment "requires an implicit level of trust as well as an explicit level of vigilance to ensure success."[37] Unless cloud service providers explicitly explain what is being taken on trust, customers and their legal counsel (and customers who are lawyers, law firms or judges) will be well advised to conduct an enhanced and rigorous due diligence of the cloud provider's security measures and of the particular cloud's architecture and methods of operation. Moreover, by encouraging and cooperating with an enhanced security due diligence, a cloud service provider can also avoid risks, such as learning belatedly that it is alleged to have participated in violations of laws involving certain kinds of sensitive data whose movement out of the originating jurisdiction or into a jurisdiction may be impermissible.

In the discussion below, we identify the most severe cloud security risks. In the following section, we discuss how those potential security risks can lead to ethical risks for lawyers and law firms.

(1) *Instabilities of Cloud Software.*

Program Instability and Defects. Programs like Google Docs have a relatively short track record or performance history, and thus their stability — their ability to remain operable without brief or prolonged interruption from "crashes" — has to be taken on faith. Cloud service providers offer seemingly high levels of service availability until one looks closely at the meaning of the specified availability:

> Amazon's Elastic Compute Cloud, its virtualized server offering, promises 99.95% uptime, but calculates uptime based on the whole year rather than individual months. That means uptime could fall below the promised level for an entire month without customers becoming eligible for service credits.[38]

That level would not meet the requirements set by the U.S. General Services Administration ("GSA") in the request for quotation ("RFQ") it issued on July 30, 2009 for cloud service offerings to support a "Cloud Computing Storefront to enable Government purchases to buy service offerings. Presumably to avert such shortcomings, the GSA's RFQ requires the contractor to provide availability based on a monthly calculation as follows:

---

[37] *See* Kaufman, *supra* note 42, at 62.

[38] Jon Brodkin, *U.S. government launches cloud push, demands strict uptime and service levels*, Networkworld, Aug. 5, 2009, http://www.networkworld.com/new/2009/090509-federal-government-cloud-computing.html.

> Service Availability (Measured as Total Uptime Hour / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.95%).[39]

Operating System Instability and Defects. The same risks of unproven, long term stability arise equally with regard to the operating systems that provide the foundation for the use of such software programs.

Upgrade Instability and Defects. Upgrades often introduce new instabilities or instabilities whose symptoms and recovery times are unfamiliar to the user. Law firms do not usually rush to be the "first on their block" to adopt the latest version of software, preferring instead to see the reported experiences of "early adopters". If a program is reportedly "buggy", causes frequent program or system "crashes", or wipes out data or documents that the user thought had been saved when the "Save" button was clicked, a law firm or lawyer may prudently postpone purchasing a license for the new version or upgrade. The law firm that relies on the cloud may find it has given up that control and the ability to limit its exposure to such risks. The cloud provider may insist that when it upgrades or introduces a new version of software, every customer must accept it. This may happen regardless of, whether they want the risks (and whether they are prepared for those risks and for the accompanying learning curve for using the software).

It is not possible this early in the use of cloud computing to fully assess the risks. That they are not imaginary or far-fetched has been demonstrated the recently reported "crashes" of cloud computing services, corruption of data in at least one instance, and unauthorized release of customer data. For example, on February 24, 2009, Google's e-mail service, which at the time had over 100 million customers (consumer and business), suffered a complete world-wide shut down, depriving customers of access to their Gmail accounts for over two hours. Since it occurred at 1:30 AM Pacific Standard Time, most U.S. customers were unaffected. However, users in Europe and Asia had a brief experience of a "worst case scenario" for users of public cloud, software as a service: an inability to send, receive or to gain access to their remotely stored e-mail data and attachments.[40] On March 10, 2009, Google's e-mail service went down for an undisclosed, but apparently significant number of users, some of whom found service restored within a half hour, but others reportedly remained without access to their accounts for several hours.[41] A similar shut down of Gmail occurred in August 2008.[42] A May 14, 2009 "outage at Google" disabled use of Google's cloud services for many of its customers.[43]

Google has yet to reveal the cause of the August 2008 shut down. Google eventually disclosed the cause of the February 2009 shut down, but the explanation revealed further risks that customers take when they rely on public cloud computing services. The failure occurred during routine maintenance of Google's European data centers when Google staff was moving data to a back-up center to allow for maintenance to proceed.[44]

---

[39] General Services Administration, *US Federal Cloud Computing Initiative*, REQUEST FOR QUOTATION, ATTACHMENT C, STATEMENT OF WORK, §3.1, Table 2, Item 7, July 30, 2009, http://www.scribd.com/doc/17914883/US-Federal-Cloud-Computing-Initiative-RFQ-GSA.

[40] Chris Nuttall, *Google e-mail crash hits millions and raises fears over web services*, FINANCIAL TIMES, Feb. 25, 2009, at 1.

[41] Andrew Morse, *Google Mail Hit by Outage, Second in Less Than Month*, THE WALL STREET JOURNAL, Mar. 11, 2009, at B5.

[42] *Id.*

[43] Steve Hamm, *Cloud Computing's Big Bang For Business*, BUSINESSWEEK, June 15, 2009, at 44.

[44] Richard Waters, *Rogue code led to Gmail shutdown*, FINANCIAL TIMES, Mar. 2, 2009, at 15.

> [T]he relocation triggered a software program that is designed to direct data to the centre nearest to where users are based, a measure that improves the response time for online applications.
>
> As it unexpectedly set to work on the new mass of data, the code greatly increased the workload on the reserve data centre and triggered an overload, causing data to be pushed automatically into a third centre.
>
> That in turn led to another overload, eventually triggering a series of failures that toppled Google's data centres like falling dominoes.

The so-called "rogue code" that caused the shutdown was written by one of Google's in-house programmers.[45]

A more serious problem occurred at Ma.gnolia, a cloud provider of bookmarking services, *i.e.,* that enables customers to bookmark web sites and web pages. Ma.gnolia revealed in February 2009 that it "could not recover" customer's work "from a corrupted database. There was also no recoverable back-up, meaning many users would have lost their carefully cultivated collection."[46] As one commentator noted,

> We have been led to believe that the advantage of web [cloud] services is that they are ubiquitous and always available, but instead have discovered that they are sometimes difficult to find or have disappeared altogether.
>
> …
>
> Data can be lost in the fog of cloud computing whereas with traditional local hard drives and client-based software, users have more control over, and responsibility for, the data.[47]

Data that becomes temporarily inaccessible can have profound consequences for a lawyer or law firm if work needs to be done urgently for the client. Delays in getting to the data can translate into serious disadvantages for the client's interests in a negotiated transaction or in the midst of time-pressured trial or arbitration preparations. Data that is released or made available to unauthorized persons could compromise client confidentiality. It may also deprive a client of enforceable trade secrets, or, if the data was subject to the attorney-client privilege, it might result in a waiver of the privilege. Such issues would require investigation if a cloud provider lost control over access to data it stores for customers, which occurred with Google Docs in March 2009. As Google disclosed to certain of its Google Docs customers, a glitch allowed unauthorized shared access to certain documents stored on online with Google Docs:

> We've identified and fixed a bug which may have caused you to share some of your documents without your knowledge. This inadvertent sharing was limited to people with whom you, or a collaborator with sharing rights, had previously shared a document. … The issue only occurred if you, or a collaborator with sharing rights, selected multiple documents and presentations from the documents list and changed the sharing permissions. This issue affected documents and presentations, but not spreadsheets.[48]

---

[45] *Id.*

[46] Chris Nuttall, *Global crashes spark crisis of confidence*, FINANCIAL TIMES, Mar. 12, 2009, at 2.

[47] *Id.*

[48] Stephen Shankland, *Google Docs suffers privacy glitch*, Mar. 9, 2009, http://news.cnet.com/8301-17939_109-10191463-2.html.

(a) Ethical Issues.

If a lawyer or law firm is considering the use of a public cloud for storage or processing of records that include client confidential information, certain precautions are advisable in order to protect the client's interests and thereby ensure compliance with the NYRPC. Since outsourcing such functions can reduce the extent to which a law firm customer can be sure of continuous access to such data, it also may increase the risk that the law firm might fall short of complying with NYRPC Rule 1.1(a) to "provide competent representation" and NYRPC Rule 1.1(c)(2):

> [A] lawyer shall not intentionally: … prejudice or damage the client during the course of the representation …"

The NYRPC does not define "intentionally". However, it gives this interpretive guidance for the use of the word "Knowingly": "A person's knowledge may be inferred from circumstances." Similarly, it would be reasonable to infer a lawyer's intentions "from circumstances." If circumstances surrounding a law firm's selection of a cloud provider evidenced a clear lack of care for widely publicized risks such as temporary loss of access to data, the law firm could arguably be viewed as taking the risk of prejudicing or damaging the client in breach of Rule 1.1(c)(2). Suppose a law firm engages the services of a public cloud provider that a due diligence review would have revealed to be an unreliable vendor or provider of unreliable access to data. The law firm could be at risk of appearing to have acted with insufficient care for its client's interests. Suppose that as a result of such engagement, the law firm found itself for a period of time unable to gain access to a client's documents stored in the cloud. The firm could then be at risk of having breached not only Rule 1.1(c)(2), but also Rule 1.3 (a) and (b), which provide that "[a] lawyer shall act with reasonable diligence and promptness in representing a client" and "[a] lawyer shall not neglect a legal matter entrusted to the lawyer."

(b) Considerations and Precautions:

Lawyers and law firms may need to choose between early adoption of a public cloud service (and carefully examining the provider) or postponing such adoption until the technology is mature, proven and reliable. Firms considering the early use of a public cloud should conduct a thorough due diligence review of the cloud service provider. The review might be structured to examine the service provider in light of the inherent risks of any public cloud. Such a review might also explore how the service provider would respond to incidents involving the shutdown of the system or inability to provide the law firm access to its client's confidential information.

If the law firm were outsourcing storage of hard copy to a domestic or overseas warehouse, it would be prudent to question the warehouse operator about its experience with inability to provide access to documents on short notice. Similarly, a law firm should consider questioning a cloud provider about all shutdowns it has experienced, what back-up copies it makes (if any), what formal, written policies and procedures it has for detecting loss of access to electronic records and for responding to temporary loss of access to records stored in its servers.

It may appear unrealistic to expect that major cloud providers such as Google, Microsoft, IBM, and Amazon.com will cooperate with any request for such a due diligence review. However, if law firms were to weigh the risks to their clients, their reputations and their compliance with the NYRPC, the need to conduct due diligence could appear compelling. Moreover, the New York State Bar Association's Committee on Professional Ethics ("NYSBA's Ethics Committee"), in a 2008 opinion on the use of an e-mail service provider that scans e-mails for advertising purposes, cautioned that "A lawyer must exercise due care in selecting an

e-mail service provider to ensure that its policies and stated practices protect client confidentiality."[49] A New York disciplinary body might expect a comparable exercise of due care by a lawyer or a law firm in selecting a public cloud service provider.

Reasonable care in the selection of a cloud vendor may not be sufficient to protect a client's interests to the extent we believe may be required by the NYRPC Rule 1.1(c)(2) to avoid intentionally damaging a client's interests. If there were a declining trend in security threats from the Internet and from malicious code, it might well be justifiable for a law firm to focus its precautions on finding a trustworthy and competent public cloud vendor. Such a course of action might seem all the more reasonable if a law firm decides to be guided by its experience and lessons learned in the earlier adoption of e-mail communications technologies and selection of an Internet and e-mail service provider. However, most law firms may not have an accurate history of their experiences (good and bad) in the adoption of e-mail technologies and Internet and e-mail service providers.

Moreover, the security risks and ethical challenges involved in the decision to rely on a public cloud are substantially greater than those faced by law firms when they elected to adopt e-mail communications. Some of the most costly lessons learned from the reliance on e-mail communications came from mistakes that were easy for lawyers to make and that had sometimes irreversible consequences. Selection of a trustworthy e-mail service provider may not have averted such mistakes. Such mistakes are sometimes foreseeable if one takes the time to consider ways in which lawyers working under time pressures might err in their manipulation of a computer and program software. The mistakes occurred nonetheless. And if compared to similar mistakes made with the earlier communications technology of facsimile transmittals, the consequences were much greater and the mistakes were far easier to make.

For example, a confidential document could be faxed to an unintended recipient by misdialing a number (a risk somewhat reduced as fax machines were developed with a capacity to store numbers). The number of misdirected transmittals when such a mistake occurred was usually one or only a few, a serious and potentially costly error, but one that seldom caused the transmittal to compromise a client's interests, provided that the recipient was not a party with interests adverse to the client's. Often the misdirected document arrived at an office with no relationship with or interest in the matter whatsoever, and the recipient would cooperate with efforts by the sender to mitigate the damage (such as destroying the document without making any use of it). Misdirected transmittals by e-mail have tended to cause far larger and more serious problems. Instead of one unintended recipient, there may be many. Instead of transmittals to a randomly misdialed number, the misdirected transmittals have often gone to recipients whose addresses are automatically suggested by the software. Since counsel often corresponds by email to opposing counsel, there is a heightened risk (however implausible it may seem) of an inadvertent transmittal to parties with interests adverse to those of the client. Security risks from use of public clouds are likely to be even greater than those experienced with e-mail. Therefore the lessons learned from adoption of e-mail technologies, and that continue to be applied, should be viewed as useful, but less than the minimum, precautions a law firm should take when deciding to rely on a public cloud for software services and document storage.

A helpful guide for considerations appropriate for e-mail technologies can be found in a 2008 opinion by the Association of the Bar of the City of New York's Committee on Professional and Judicial Ethics ("ABCNY Ethics Committee") on the subject of "A Lawyer's Ethical Obligations to Retain and to Provide a Client with Electronic Documents Relating to a

[49] New York State Bar Association Committee on Professional Ethics, OPINION 820, Feb. 8, 2008, at 2.

Representation" ("Opinion 2008-1"). Opinion 2008-1 summarized certain substantive changes in the realities of law practice in the digital era:

> Lawyers routinely use e-mail to formally convey important information and documents to clients, colleagues, and other counsel. Just as routinely, lawyers use e-mail to conduct informal conversations. In many law practices, lawyers are as likely to send an e-mail as to pick up the telephone or walk down the hall to a colleague's office.
>
> The growing reliance by lawyers on digital technology, of course, is not limited to e-mails. Virtually all correspondence, transactional documents, and court filings originate as electronic documents. … In addition, many lawyers and law firms, taking advantage of widely available document imaging technology, convert their paper records into electronic documents for organizational and storage purposes.[50]

In light of those changes in practice, the ABCNY Ethics Committee believed "it would be useful to address some of the ethical issues implicated by a lawyer's reliance on e-mails and other electronic documents."[51] On the issue of a client's access to electronic records, the ABCNY Ethics Committee did not believe that "a lawyer has any ethical obligation to organize electronic documents in any particular manner, or to store those documents in any particular storage medium," but added an important caution:

> From an ethical standpoint, a lawyer should ensure that the manner of organization and storage does not (a) detract from the competence of the representation or (b) result in the loss of documents that the client may later need and may reasonably expect the lawyer to preserve.[52]

Since public clouds have been temporarily shutdown and the risks of additional shutdowns will likely persist and possibly grow if the occurrences of cyberattacks increase, law firms arguably should not overly rely on a public cloud. Law firms already know not to overly rely on storage of electronic records on solely the computer used to create them, that backups are needed, and that on-site and off-site storage of backups are prudent measures. Law firms should endeavor to ensure that they do not relinquish the only current copies of any client confidential information to a public cloud. Nor should they do so for any copies of client related documents that might be needed urgently to provide the client with competent representation consistent with the requirements of NYRPC Rules 1.1(a) and (c).

Unfortunately, there is also the risk that law firms may be persuaded by a cloud provider's promised benefits and to decide against taking certain reasonable precautions. For example, if a law firm retains a digital copy on its premises of all data stored in the cloud, it might sacrifice some of the benefits of outsourcing storage but retain the ability to protect its clients' documents. The representations for Google Docs all but discourage such precautions by stating:

> Because Google Docs saves to a secure, online storage facility, you can create documents, spreadsheets and presentations without the need to save to your local hard drive. You can also access your documents from any computer. In the event of a local hard drive crash, you won't lose your saved content.

---

[50] The Association of the Bar of the City of New York, Committee on Professional and Judicial Ethics, Formal Opinion 2008-1, at 1, http://www.nycbar.org/Publications/reports/print_report.php?rid=794.

[51] *Id.*

[52] *Id.* at 3.

> While we can't give you exact figures, please be assured that we back up data almost as often as you can change it.[53]

In light of the potential ethical issues, lawyers and law firms might well be reluctant to rely too much on this assurance.

The ABCNY Ethics Committee Opinion 2008-1 also recommended a step that many firms may be reluctant to take, but that warrants strong consideration: disclosure to, and discussion with, the client. Large firms with large numbers of clients may well find such disclosure and discussion particularly burdensome and potentially risky if some clients concur in the use of a public cloud and others resist it. As explained in Opinion 2008-1 (in the context of e-mail, but applicable also to the public cloud), such disclosure and discussion recognizes that a client may be entitled to know of the risks at the start of the engagement and to reflect a shared understanding of safeguards in the letter of engagement:

> In light of the exponential growth in e-mails and other electronic documents, and the pace of technological change involving the organization and storage of electronic documents, it may be prudent for a lawyer and client to discuss the retention, storage, and retrieval of electronic documents at the outset of an engagement. Lawyer and client may find it worthwhile to discuss and reach agreement at the outset on issues such as (i) the types of e-mail and other electronic documents that the lawyer needs to retain, given the nature of the engagement; (ii) how the lawyer will organize those documents; (iii) the types of storage media the lawyer intends to employ; (iv) the steps the lawyer will take to make e-mail and other electronic documents available to the client, upon request, during or at the conclusion of the representation; and (v) any additional fees and expenses in connection with the foregoing. …[T]hose costs should accord with the lawyer's customary fee schedule and must not be excessive. By raising these issues at the outset of the representation, perhaps as part of the engagement letter, a lawyer and a client will be able to make informed decisions about the appropriate manner of retention, storage, and retrieval of electronic documents to which a client has a presumptive right of access.[54]

(2) *Diminished Ability to Locate Faults.*

When a firm runs its own network, it tends to develop the ability to locate the source of a "crash" or other fault in the system's performance (such as a plummeting pace of performance). When major functions like word processing are outsourced to the cloud, it may become quite difficult to determine whether a fault originates within the law firm's networks or within the cloud provider's networks. The law firm's partners can require its IT staff to report fully on problems they have found, but depending on the cloud service agreement such reports may not be

---

[53] "Docs Help", GOOGLE docs, accessed in August 2009 at http://docs.google.com/support/bin/answer.py?hl=en&answer=44665 and "Getting to Know Google Docs," accessed at http://cffecsd.wikispaces.com/file/view/Getting+to+Know+Google+Docs.pdf.

Note that Google has subsequently modified its description of Google Docs. Google deleted the words: "You can also access your documents from any computer. In the event of a local hard drive crash, you won't lose your saved content. While we can't give you exact figures, please be assured that we back up data almost as often as you can change it." And Google added the words, including: "Your presentation will begin saving within Google Docs almost as soon as you begin entering text." "Docs Help", GOOGLE DOCS, accessed at http://docs.google.com/support/bin/answer.py?hl=en&answer=69074. Google does not provide access to a redline of the changes it continually makes to such descriptions or to its Terms of Service.

[54] *Id.* at 5. Note that Opinion 2008-1 concludes that "[i]n New York, a client has a presumptive right to the lawyer's entire file in connection with a representation, subject to narrow exceptions."

available on demand, or complete, or contain sufficient reliable information for the firm to learn the cause of a problem. An isolated instance of a complete and prolonged loss of word processing capabilities may be as important to trace to its cause as such losses occurring briefly but repeatedly.

The significance of the ability to locate faults in the cloud becomes clearer when one considers that the architecture of a cloud service provider and its reliance on multiple entities makes the cloud increasingly likely to have vulnerabilities and for the rich store of sensitive data in the cloud to make it a highly attractive target for cyber-exploitation. Lori Kaufman explains the cloud architecture vulnerabilities as follows:

> Clouds can comprise multiple entities, and in such a configuration, no cloud can be more secure than its weakest link. If a cybercriminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target. The lack of security associated with this single entity threatens the entire cloud in which it resides. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cybercriminals. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous sites, and without proper security, hundreds of sites could be comprised [sic] through a single malicious activity."[55]

Moreover, if the cloud provider does not implement encryption of data at rest in its servers or has a breach of security concerning the encryption's keys, then the principle of "access to one gives access to all" will apply and multiple the risks to all customers' data. Put differently, a cloud that has not been optimized for security (for the customer's benefit) will be likely to have been inadvertently optimized for a breach (for the attacker's benefit):

> The best case (from an attacker's standpoint) is when the same vulnerability exists at all levels within large interconnected systems, where 'redundant' resources can be compromised, resulting in cascading effects. This situation could allow an adversary to very quickly commandeer a large and diverse population of systems, as has been witnessed in various worm outbreaks over the past few years."[56]

With such risks in mind, consider the U.S. intelligence community's 2009 annual threat assessment with respect to cyber-exploitation (a term that "refers to the penetration of adversary computers and networks to obtain information for intelligence purposes"[57]):

> A growing array of state and non-state adversaries are increasingly targeting—for exploitation and potentially disruption or destruction—our information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Over the past year, cyber exploitation

---

[55] *See* Kaufman, *supra* note 42, at 63.

[56] William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Prepublication Copy – Subject to Further Editorial Correction), National Research Council of the National Academies, Apr. 29, 2009, at viii, http://books.nap.edu/openbook.php?record_id=12651&page=R1.

[57] *Id.* at 2-57. Note that no small part of such risks is that the user may need to know, and may have no way of knowing, that its data or the system storing it has been compromised. As the cited report explains, Cyberexploitations do not seek to disdturb the normal functioning of a computer system or network from the user's point of view – indeed, the best cyberexploitation is one that such a user never notices. … [I]f the targeted party does not know that its secret information has been revealed, it is less likely to take countermeasures to negate the compromise." *Id.* at 1-2 and 2-52.

> activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year."[58]

(a) *Ethical Issues*.

The ethical issues discussed in the context of public cloud instabilities are much the same as those raised by a law firm's diminished ability to locate faults. They differ, however, in one important respect: with diminished ability to locate faults comes a diminished ability to mitigate the adverse consequences and to avert re-occurrences. That may implicate a law firm's ability to provide competent representation.

Here again, a review of the cloud provider's Terms of Service may reveal that the magnitude of risks and the probability of their manifestation in the cloud are greater than customers might anticipate. Enhanced risks and probabilities of problems will likely affect a law firm's assessment of the ethical issues. The Google Docs Terms of Service contain, in the "Exclusion of Warranties", a provision that raises such risks and probabilities with respect to a law firm's need to know the location and nature of faults that develop in the operation of the cloud:

> 14.3 IN PARTICULAR, GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT:
>
> …
>
> (C) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND
>
> (D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED.[59]

Thus, under the standard Terms of Service there appears to be no assurance that a customer would be given any explanation of faults in the system. Moreover, Google disclaims any responsibility to correct "defects in the operation or functionality" of the cloud software. A law firm user might lack the information to know whether the fault occurred within its system, in Google's, or in a conflict between software installed on the user's network and software installed in Google's cloud servers. Under the Terms of Service, a law firm would also have no right to require correction of faults or defects, nor any right to require Google to attempt to correct faults or defects or to attempt to mitigate the damage to the law firm customer. These represent potentially significant negatives that could make the promised potential cost reductions, scalability of computing power, and ubiquitous access appear transitory or illusory in the long term.

Moreover, while a commercial enterprise may decide it can accept the tradeoffs of potential benefits and potential risks, a law firm's fiduciary relationships with each of its clients, and its ethical obligations under NYRPC Rule 1.1(a) to provide "competent representation" and Rule 1.1(c) to "not intentionally … prejudice or damage the client during the course of the representation," may change the calculus of such assessments. The disclaimers may increase the law firm's need to take precautions in order to avoid seeming to "intentionally" disregard the risks of damage to the client that could arise if faults in the cloud remained uncorrected.

---

[58] Dennis C. Blair, *February 2009 Intelligence Community Annual Threat Assessment for the Senate Select Committee on Intelligence – Unclassified Statement for the Record*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, Feb. 12, 2009, at 39, http://intelligence.senate.gov/090212/blair.pdf.

[59] Google Docs Terms of Service, § 14.3 (C) and (D), accessed at http://www.google.com/accounts/TOS.

(b) *Considerations and Precautions.*

The security risks concerning faults in the cloud, and the lack of an obligation to attempt to correct them, heighten the need for lawyers and law firms, as prospective customers, to consider precautions beyond those noted above in the discussion of cloud instabilities. This may mean having contingency plans to minimize the consequences in the event such problems occur. Such issues could be addressed in the Terms of Use, to the extent such terms are negotiable. Law firms might also seek to negotiate whether the Terms of Use agreed to with the law firm would be subject to the typical practice of online service providers who reserve the right to change the terms unilaterally, at any time, without notice to the customer. Some Terms of Use or Terms of Service, such as that for Google Docs, not only claim the right to vary the terms unilaterally, but also that the continued use of the service after such changes will be treated as acceptance of those changes (even though a customer may not have been aware of the change since posting of such changes is not accompanied by any email notice to the users).[60]. A law firm entering into Terms of Use for a public cloud software service that gave such rights to the cloud provider likely would want to give careful consideration to the attendant ethical risks, as these terms may mean relinquishing the right to review and veto the terms (and therefore the risks to be taken with clients' electronic records).

It is worth noting that the Terms of Service for Google Docs[61] make interruption of access to a customer's documents a virtual certainty, given that Google requires the customer to agree that Google has the right to intentionally interrupt or to disable such access – temporarily or permanently:

> 4.2 Google is constantly innovating in order to provide the best possible experience for its users. You acknowledge and agree that the form and nature of the Services which Google provides may change from time to time without prior notice to you.
>
> 4.3 As part of this continuing innovation, you acknowledge and agree that Google may stop (permanently or temporarily) providing the Services (or any features within the services) to you or to users generally at Google's sole discretion, without prior notice to you. …
>
> 4.4 You acknowledge and agree that if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account."[62]

The significance of these provisions can readily be understood by simply substituting for "any files" the words "any files containing client related or client confidential information." Instead of assessing the probability of temporary loss of access due to a random disruption of cloud services, a law firm may find it prudent to infer from the quoted provisions a near certainty

---

[60] Google Docs Terms of Service § 19.2, http://www.google.com/accounts/TOS?hl=en.

[61] Note that the Terms of Service for Google Docs do not appear on the initial screen that loads when a user clicks on a Google search term for "Google Docs," nor is there a link on the initial screen that directly takes one to the Terms of Service. Instead, one has to intuitively deduce that the central message on the screen, stating "Welcome to Google Docs! Click the 'New' button to create a new online document or the 'Upload' button to edit a file from your desktop. You documents will show up here. Learn more," provides a portal where one can find such a link. The "Learn more" link takes the user to a screen with bulleted lists under the heading "Getting to know Google Docs: Google Docs basics." If the user scrolls down to the bottom of that screen, he or she will find a link to "Terms of Use." These Terms of Use appear to be the same as for other public cloud services offered by Google, such as G-mail, and to be intended by Google to cover its full range of public cloud offerings.

[62] Google Docs Terms of Service, *supra* note 85, at § 4 (emphases added).

that there will be temporary or permanent losses of access "or any features within the services" such as, for example, recovery of certain purportedly "saved" documents. Such provisions may make the ethical risks foreseeable (rather than speculative) and the need to address them, before consenting to binding terms of service, much more compelling.

In addition, there should probably be careful negotiation of the law firm's rights upon termination of the relationship with the public cloud provider. Will the law firm be assured that all electronic copies will not merely be "deleted" but irrecoverably purged from the cloud provider's servers wherever located? Will the law firm receive a certification that such purging of records has been completed? Unlike the usual experience with an Internet service provider where continuation of service tends to be the norm, the Google Docs Terms of Service arguably make discontinuation or termination of service significantly more likely:

> 13.3 Google may at any time, terminate its legal agreement with you if:
>
> …
>
> (C) the partner with whom Google offered the Services to you has terminated its relationship with Google …
>
> (D) Google is transitioning to no longer providing the Services to users in the country in which you are resident or from which you use the service; or
>
> (E) the provision of the Services to you by Google is, in Google's opinion, no longer commercially viable.[63]

There is no assurance of retrieval of documents stored in Google Docs at the time of termination, nor any assurance regarding Google's responsibility concerning the purge of such records after termination.

Another cloud provider, Amazon.com, takes a similar approach in its customer agreement which, unlike Google's Terms of Service, addresses post-termination issues and the issue of retrieval of electronic documents. The "Amazon Elastic Compute Cloud" service ("Amazon EC2") is governed by the "Amazon Web Services™ Customer Agreement" ("Amazon Agreement"), which devotes a section to data preservation in the event of suspension or termination. However, the Amazon Agreement only provides for preservation of data stored on Amazon EC2 if the suspension or termination is "other than for cause." The Amazon Agreement provides, in a declining sequence of assurances, that:

> (i) we will not take any action to intentionally erase any of your data stored on the Services for a period of thirty (30) days after the effective date of termination; and (ii) your post termination retrieval of data stored on the Services will be conditioned on your payment of Service data storage charges for the period following termination, payment in full of any other amounts due us, and your compliance with terms and conditions we may establish with respect to such data retrieval.[64]
>
> Under this provision:
>
> - Although Amazon says it will not "intentionally erase" a customer's data after such termination, it gives no assurance that it will take precautions to *protect* such data or to ensure that post-termination protection will equal or be in any way comparable to

[63] *Id.* at § 13.3.

[64] Amazon Elastic Compute Cloud, AMAZON WEB SERVICES™ CUSTOMER AGREEMENT, § 3.7.2, http://aws.amazon.com/agreement/.

pre-termination protection.

- Post termination "retrieval of data stored" in the cloud is not unconditional (this is not a clause addressing termination for cause). It is conceivable that Amazon might require payment of Service data storage charges post-termination, although it seems unlikely that it would require such payment be made (as well as payment in full of any other amounts due) before allowing retrieval of data by a customer who has not committed a breach.
- If Amazon elects to terminate the service, it claims the right to hold on to a customer's stored data until all outstanding invoices have been paid, which will continue to increase in amount for each day that the customer seeks to negotiate any issue during the post-termination period.
- If a law firm customer urgently needed to retrieve client-related data shortly following termination of the cloud service, even if the law firm were willing to pay for the release of the data (or for the right to attempt to retrieve it from Amazon's "Elastic Computing Cloud"), any settlement could be "hung up" if Amazon itself has not assembled a comprehensive invoice at the hour that the law firm needs to retrieve the data.
- The final condition, the customer's compliance with "terms and conditions we may establish with respect to such data retrieval," asks the customer to consent to terms and conditions that are not disclosed at the time of entry into the agreement and that may not be disclosed at the moment of termination (since the Amazon Agreement does not specify when such terms will be disclosed). A law firm should give careful consideration to the possibility of entrusting its client's data to a public cloud with such uncertain conditions attaching to its retrieval in the event of a termination for convenience by Amazon.

A law firm may want to address these potential risks in order to avert the possibility of an ethical issue arising under the NYRPC requirements for competent representation and avoidance of damage to a client.

The potential ethical issues are sharper and more difficult to address in the event of termination allegedly for cause where the law firm customer disputes that it has breached the Amazon Agreement. A termination for default releases Amazon of any responsibility for a customer's data stored in Amazon's cloud, which could ethically imperil a contractually compliant law firm if its client's data become indefinitely inaccessible:

> 3.7.3 … [In the event of a termination for cause] we [Amazon] shall have no obligation to continue to store your data during any period of suspension or termination or to permit you to retrieve the same.[65]

The Amazon Agreement uses control over the continued storage and retrieval of data as a security device without any limitations. A law firm may endeavor to renegotiate such terms and should give consideration to disclosing the resulting arrangement with its clients so that they can decide whether they are willing to allow access to their documents by their counsel under these types of conditions. Of course, if the law firm retained a copy of all such documents on its premises in its own computers or digital storage media, the ethical risks relating to competent representation would be substantially diminished. However, on-premises backups do not address the other ethical issues inherent in the arrangement proposed by the Amazon

[65] *Id.* at § 3.7.3.

Agreement: there is no mention in the termination clauses of any post-termination obligation to prevent unauthorized access to data stored on its cloud by a terminated customer, or to purge all copies of such data if the customers requests it (for example, where destruction of previously disclosed litigation material is required by settlement agreement).

Damage to, or loss of, client data and documents stored in a public cloud can pose an additional ethical risk where the client and its counsel reasonably anticipate that the client may be the subject of a federal government investigation or a party to a litigation in federal courts, thereby possibly incurring a duty under the Federal Rules of Civil Procedure to preserve all potentially relevant data and documents, including all electronically stored "records." Issuance of a "litigation hold" and supervision of its implementation has become an increasing concern for counsel as courts have, on occasion, viewed counsel as responsible for a client's compliance. If such responsibilities are not properly handled by counsel or fall short of the standard applied by a court in a given case, and the court decides to impose sanctions for spoliation, the result can be serious damage to the client's interests as well as those of the firm.

To understand the risks involved, suppose that a spoliation claim is raised as to documents that were stored in a public cloud, and that were damaged or lost or belatedly produced because of the cloud provider's failure to preserve the relevant data and documents post-termination of the law firm's relationship with the cloud provider. Suppose also that the client has been ordered to permit an adversary, an adversary's expert or government agents to make a "mirror image" of hard drives containing the potentially relevant data and documents, and that such order arguably would apply to hard drives on the public cloud provider's servers. How would a law firm address such issues to ensure fulfillment of duties under the Federal Rules, compliance with the court's orders and avoidance of potential disputes that might arise if other customers of the public cloud learned of the order and objected to having their client's data and documents "swept up" and made potentially accessible to third parties and government agents?

There appears to be a reasonable possibility of serious problems – for counsel, clients and judges – when attempting to address duties to preserve data and documents where the electronic copies are stored not on the client's controlled computers or on counsel's controlled computers, but on servers controlled by the public cloud provider. Who would be responsible for determining the locations of all such servers? Cloud providers' standard agreements typically do not explicitly provide for the maintenance of records of all locations of a customer's data or specify the locations where such data will be stored or to which it might be transferred. If a "mirror image" is ordered, would a law firm customer be entitled to notice that such an image was going to be made to obtain data of another customer but that might also include the law firm's client confidential information?

If the law firm in such a scenario had client data stored with public cloud provider Soonr, the problems arguably might be intensified by Soonr's Terms of Service and by its End User License Agreement provision on termination, which states:

> Upon cancellation by Soonr or at your direction, you may request a file of your data, which Soonr will make available for a fee. You must make such request at the notification of cancellation to receive such file within thirty (30) days of termination. Otherwise, **ANY DATA YOU HAVE STORED ON SOONR'S SYSTEMS MAY NOT BE**

> **RETRIEVED**, and Soonr shall have no obligation to maintain any data stored in your account or to forward any data to you or any third party.[66]

Law firms might find it useful to consider such scenarios and questions as well as the potential breakdowns of public cloud service in the context of a firm's efforts to monitor and supervise a client's compliance with "litigation hold" orders in order to avoid potential ethical issues arising under NYRPC Rule 1.1(c)(2)'s requirement to avoid prejudice or damage to the client. A lawyer or law firm might also want to include in such considerations a potential for an ethical issue arising under Rule 1.4(a)(2) that requires that a "lawyer shall … reasonably consult with the client about the means by which the client's objectives are to be accomplished."

Such discussions would benefit from a review of the cloud provider's applicable terms of use. It is reasonable to infer that incidents for which the cloud provider expressly disclaims responsibility are ones that it believes are reasonably likely to occur. For example, the Google Docs Terms of Service and the Amazon Agreement each address and thus highlight potential incidents involving loss of data. The Google Docs Terms of Service provide that:

> 15.1 … YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE … SHALL NOT BE LIABLE TO YOU FOR:
>
> …
>
> (B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF:
>
> …
>
> (III) THE DELETION, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER COMMUNICATIONS DATA MAINTAINED OR TRANSMITTED BY OR THROUGH YOUR USE OF THE SERVICES."[67]
>
> The Amazon Agreement provides:
>
> 7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, … you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.[68]

In preparing for issuance of a "litigation hold" and in its implementation, counsel may find it necessary to learn how a client's computers store, backup, and overwrite data and how such computers, if they "go on an excursion" or malfunction, could cause data to be corrupted, rendered inaccessible to electronic searches, or destroyed. If the law firm or the client has stored relevant data and documents in a public cloud, the "litigation hold" preparations and discussions may be aided by considering the issues that could arise from efforts to preserve

---

[66] Soonr Terms of Service and End User License Agreement § 11.3, http://www.soonr.com/security/eula.html (emphasis in original).

[67] Google Docs Terms of Service, *supra* note 74 at §15.1(B)(III).

[68] Amazon Elastic Compute Cloud, *supra* note 90 at § 7.2.

and to produce records in the public cloud. Such ethical issues may persist, and we return to them later in the discussion of other security risks.

(3) *Diminished Control over, and Knowledge of, New Software Code.*

When a law firm buys a license to use a software product, it can decide before making the purchase whether the product has been adequately tested and can control the circumstances in which new code is added to its computer networks (provided that its defenses prevent malware from intruding into its networks). Because new code may not have been tested with all of the code previously running on the law firm's networks, the issue of installing software updates ("patches") has been a difficult challenge for firms. The patch may conflict with other code residing on the firm's networks, causing degradation in performance, corruption of data, or system crashes.

A cloud service provider, however, is not subject to the decisions of any one of its customers. If it wants to load new code on its system and if the terms of service do not provide otherwise, it can do so without reporting to its customers that (i) such code will be installed, (ii) certain problems are known to be likely to occur with certain existing programs, or (iii) after installation certain problems have been found to have resulted. Indeed, cloud providers often present as a significant benefit of a public cloud that customers will all receive security patches simultaneously and will not need to involve their IT personnel in the process. Of course, it is always possible that a buggy patch will affect all customers simultaneously. Since there may be no notice to customers that the patch has even been installed, it can introduce a glitch into a law firm's networks or cause a cascading response of adverse consequences that reach beyond the cloud back to the law firm's networks. In another of its exclusions of warranties, the Google Docs Terms of Service disclaim any responsibility for problems introduced by such enforced downloads from the cloud:

> 14.4 ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.[69]

(a) *Ethical Issues.*

The security risks that arise from the unannounced installation of new code are roughly the same as those that arise from cloud instability, but with one difference: the corruption or loss of data in the cloud, caused by the new code, can migrate back to the law firm customer and threaten the data stored on its Internet-linked computers and digital storage devices. If the law firm's routine backup servers are linked directly or indirectly to the Internet, then those too could be put at risk by new code introduced by the cloud provider. If a lawyer or law firm allows a client's documents to be corrupted, lost, or destroyed, a lawyer or firm may find that they have inadvertently breached their duty to preserve a client's records and files. The former New York Code of Professional Responsibility ("Code") and its recent replacement, the NYRPC, do not expressly mandate record-retention requirements except with respect to "a small number of discrete documents, such as retainer agreements, bills to clients, bank statements and records of transactions in escrow account."[70] However, as Opinion 2008-1 observed (with respect to the

[69] Google Docs Terms of Service, *supra* note 85 at § 13.3.

[70] The Association of the Bar of the City of New York, *supra* note 69 at 1. All such documents are required to be retained for a period of "seven years after the events that they record." NYRPC Rule 1.15(d)(1), http://www.nysba.org/Content/NavigationMenu/ForAttorneys/ProfessionalStandardsforAttorneys/NYRulesofProfessionalConduct4109.pdf.

Code and that applies with equal cogency to the NYRPC),

> The Code … contains several provisions that implicitly impose on lawyers an obligation to retain documents. For instance, … a lawyer has an obligation to represent a client competently … Similarly, … '[a] lawyer shall not intentionally … [p]rejudice or damage the client during the course of the professional reputation," …
>
> …
>
> As is the case with paper documents, which e-mails and other electronic documents a lawyer has a duty to retain will depend on the facts and circumstances of each representation. Many e-mails generated during a representation are formal, carefully drafted communications intended to transmit information, or other electronic documents, necessary to effectively represent a client, or are otherwise documents that the client may reasonably expect the lawyer to preserve.[71]

(b) *Considerations and Precautions*

A lawyer's and law firm's chief concern would be to avert the loss of all copies of any document of importance to the client's interests. Opinion 2008-1 reiterated an earlier-expressed view that at the end of a representation and "before destroying any documents that belong to the client, the lawyer should contact the client and ask whether the client wants delivery of those documents."[72] It could be difficult for a lawyer or law firm to follow that recommendation if it failed to take available precautions to avert the destruction of the client's documents by rogue code from a cloud provider.

(4) *Diminished Control over, and Knowledge of, Network Defenses.*

When a law firm sets up its internal network, it can control the defenses for that network and the monitoring and reporting of, and responses to, unauthorized access (from within the firm) and unauthorized intrusions (from outside the firm). Unless provided by express terms in the cloud service agreement, however, such control and knowledge will probably be substantially diminished. Moreover, unless the cloud service agreement requires it, the law firm may be at risk of not receive *any* timely reports of a breach in the defenses. Furthermore, a firm may misunderstand the defenses that exist in the cloud. As Forrester analyst Chenxi Want notes, "[c]loud computing is optimized for performance, optimized for resource consumption, and optimized for scalability … It's not really optimized for security."[73]

One reported way in which cloud security has yet to be optimized is encryption. Although many cloud service providers offer encryption in transit (while data is moving up to the cloud or from the cloud to the customer), the encryption of data at rest within the cloud service provider's servers has prompted questions and serious doubts, such as the following:

- "Data at rest is more complex, and you may have to rely on your own resources to encrypt it."[74]
- "[A] request for encryption of stored data goes beyond the [cloud service

[71] *Id*. at 2.

[72] *Id.*

[73] Neil Roiter, *How to Secure Cloud Computing*, INFORMATION SECURITY MAGAZINE, Mar. 2009, http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349670_mem1,00.html?ShortReg=1&mboxConv=searchSecurity_RegActivate_Submit&.

[74] *Id.*

provider] industry standard and may, because of technological constrains, degrade the service."[75]

- "Encryption is less reassuring if the [cloud service] provider controls the keys. It gets back to a question of trust and verification that the provider is following strict policies regarding who has access to the keys and under what circumstances."[76]
- There is a "fundamental problem with cloud computing setups that use virtualization software to partition servers into 'images,' which are then rented out to customers. Although packing those virtual machines into cloud providers' data centers provides a more flexible and efficient setup than traditional servers … virtual machines suffer from a rarely discussed flaw: They don't always have enough access to the random numbers needed to properly encrypt data."[77]

(a) *Ethical Issues.*

Where a security incident involves intrusion into a law firm's networks leading to the loss or damage of a client's data and documents, the ethical issues raised by diminished control over a firm's network defenses are much the same as those discussed in the earlier sections of this essay. However, a breach in a law firm's network defenses can lead to a more sinister result: unauthorized access to client confidential information. Because under the NYRPC "confidential information" includes privileged information, information that could be embarrassing to the client, and information the client asked to be kept confidential, access to client confidential information could compromise the protection required for each kind of such information.

The primary ethical issue raised by such security incidents would be the requirements of NYRPC Rule 1.6(a) that a "lawyer shall not knowingly reveal confidential information." A law firm is better able to know and assess the sufficiency of the safeguards for its clients' data and documents before entrusting them to a public cloud than after. If a law firm has knowingly relinquished such control and arguably diminished its ability to safeguard its clients' data and documents, is the firm at greater risk of an ethical violation in the event of a breach of its network defenses and access to its client confidential information?

(b) *Considerations and Precautions.*

The answer to the question above likely would depend on the other precautions taken by the firm and on the manner in which such unauthorized access was achieved. Nevertheless, the question could prove troubling for a law firm, making it prudent to consider the issue before agreeing to entrust clients' confidential information to a public cloud. It would also be prudent for law firms to make routine assessments of the vulnerability of their computer networks to the most recently reported and anticipated threats (from insiders and outsiders), and to make a focused assessment of the probable change in such vulnerabilities that might result from outsourcing storage or processing of client data and documents to a public cloud. Doing so

---

[75] Barry Reingold and Ryan Mrazik, *Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy (Part I)*, CYBERSPACE LAW., June 2009, at 2, http://www.perkinscoie.com/files/upload/PS_09-06_Cloud_Computing_Article.pdf.

[76] *See* Roiter, *supra* note 98.

[77] Andy Greenberg, *Why Cloud Computing Needs More Chaos*, FORBES.COM, July 30, 2009, http://www.forbes.com/2009/07/30/cloud-computing-security-technology-cio-network-cloud-computing.html.

arguably would improve the chances that the law firm will become aware of security flaws that it may want to address before outsourcing storage of client data.

By increasing the probable protection of client confidential information the law firm will, in most instances, be increasing its own protection against the risks of an ethical breach. Such a breach becomes less likely and, if it occurs despite reasonable precautions, those precautions provide important evidence with which to defend the law firm from allegations of a violation of the firm's ethical obligations under the NYRPC.

(5) *Diminished and Delayed Knowledge of Data Breaches.*

When a law firm has exclusive control over the storage of its electronic records, it should be in a reasonably good position to monitor for and know of security incidents and data breaches. Unless the cloud service agreement requires it, however, the cloud service provider may claim it is entitled to withhold information of security incidents. It may even reserve the right to determine whether the incident involved a loss, corruption or misappropriation of personal data or client confidential information. If the cloud service provider is located in a jurisdiction that has not enacted a data breach reporting law, the cloud service provider might decide it is entitled to issue *no* report on the incident or on the data affected by the breach.

(a) *Ethical Issues*.

A data breach involving the potential release of or access to client confidential information implicates a lawyer's and law firm's ethical obligation under NYRPC Rule 1.6(a) to "not knowingly reveal confidential information." If a cloud provider's policy is not to report data breaches to its customers, those customers cannot assess on an on-going basis the security of their data and the reliability of the cloud provider's safeguards for their data. A cloud provider might take the position that commercial customers must accept the risks and have no compelling need to monitor the modulations of those risks in the cloud. However, lawyers and law firms are not ordinary customers in that they have an ethical obligation under NYRPC Rule 1.6(c) to "exercise reasonable care to prevent the lawyer's employees, associates, and <u>others whose services are utilized by the lawyer</u> from disclosing or using confidential information of a client."[78]

Public cloud providers, if engaged by a lawyer or law firm, would appear to come within the category of persons "whose services are utilized" by such lawyer or law firm. If a lawyer or law firm has not ensured that the public cloud provider will report data breaches that may involve the lawyer's or law firm's client data, how well can they fulfill the ethical obligation to "exercise reasonable care" to prevent a cloud provider from "disclosing" client confidential information? Can "reasonable care" be sufficiently exercised if the law firm contractually relinquishes its ability to supervise or even to monitor or receive timely reports on the performance of a public cloud provider's protection of client data? The answers may change substantially if instead of an isolated incident (an accident that occurs despite good precautions), the pubic cloud experiences a succession of data breaches (a systemic failure of safeguards or uncorrected vulnerabilities).

(b) *Considerations and Precautions*.

Use of a communications technology implies an ethical responsibility to evaluate the degree to which its use may put client confidential information at an increased, and perhaps

[78] NYRPC Rule 1.6(c), *supra* note 95 (emphasis added).

unreasonable, risk. As the NYSBA Ethics Committee noted in the context of an opinion on precautions needed to protect client confidential information from disclosure via metadata,

> a lawyer who uses technology to communicate with clients must use reasonable care with respect to such communication, and therefore must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances.[79]

The same duty to "assess the risks attendant on the use" of technology would appear to apply to communication of client data to and from a public cloud. Such assessments may need to be made not only before entering into agreement with a public cloud provider but continually in order for counsel to stay abreast of changes in the operation of the cloud, changes in the terms of use, and changes in the rapidly evolving security threats to web-based services and services that provide wireless access. Modes of storage and of transmission can be affected by such threats and may therefore deserve continually re-assessment. As the NYSBA Ethics Committee has observed (in the context of transmittals by e-mail):

> Reasonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission.[80]

The digital era, however, puts counsel in the uncomfortable position of being responsible for protection of client confidential information during a period when the technologies that facilitate competent representation also threaten to undermine counsel's efforts to protect client confidential information. The growing recognition that security breaches may be a near certainty makes this situation even more difficult to resolve, particularly when the likelihood of such breaches is expressed in a cloud provider's terms of service or, as in the case of Soonr, in its privacy policy:

> No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, while we strive to use commercially acceptable means to protect your information, we cannot guarantee its absolute security. When you use the Soonr Software to upload files to our servers, we will treat that information with the same security measures we afford the information we collect about you and about those you authorize to access your files.[81]

In addition, cloud providers do not usually provide much information about their security measures or security standards in their terms of use or the related privacy policies. Google Docs' Terms of Use offers no comment on those issues, and its privacy policy offers little insight into what Google actually does or the standards to which it attempts to adhere:

> We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data.[82]

---

[79] NYSBA Ethics Committee, OPINION 782, Dec. 8, 2004, at 2.

[80] *Id.* at 2-3.

[81] Soonr, Privacy, http://www.soonr.com/security/privacy.html.

[82] Google, Privacy Policy, http://www.google.com/privacypolicy.html.

We are not suggesting that a cloud provider should disclose details of its security precautions and risk releasing such information to persons intent on defeating such safeguards. However, a law firm customer may need more information than is provided by the assurances typically found in a standard non-disclosure agreement, and may well find it prudent to conduct a due diligence under appropriate conditions to satisfy itself that a client's confidential information is receiving the standard of care that is consistent with the law firm's ethical obligations to exercise reasonable care to prevent the cloud provider from disclosing client confidential information.

(6) *Diminished Control over and Knowledge of the Location(s) and Movement of Personal Information and Client Confidential Information*.

Under most standard terms of service, such as the Google Docs license and the license offered by Soonr, a cloud service provider claims the right to move, store, and process a customer's data. The customer is given no right to receive reports on the exact whereabouts or jurisdictional location of its data, the number of copies made of such data, or the locations where such copies may be stored. Moreover, some cloud service providers require customer consent to blanket permissions for transfers of data into and out of the European Union, without any assurance that such transfers will comply with applicable EU or EU member state data protection laws and regulations. Such appears to be the case for transfers by the Soonr Terms of Service and End User License Agreement:

> SOONR STORES AND PROCESSES THE INFORMATION WHICH SOONR COLLECTS FROM YOU ON COMPUTERS IN THE UNITED STATES AND OTHER COUNTRIES IN WHICH SOONR OR ITS AGENTS HAVE FACILITIES. YOUR ACCEPTANCE OF THESE TERMS AGREEMENT INCLUDES YOUR CONSENT TO TRANSFERS OF SUCH INFORMATION OUTSIDE YOUR COUNTRY.[83]

Moreover, some cloud service providers offer features that promise advantages to the user with an undisclosed reduction in security. For example, Gmail and Google Docs reportedly offer "an automatic draft saving feature, by which they periodically upload the contents" of a user's email or document to Google's servers where it is saved as a 'draft.'[84] However, researchers report that the same feature may cause confidential data to be uploaded "in-clear" to Google even as the user is composing the document, thus making it susceptible to interception.[85]

(a) *Ethical Issues*.

Data protection laws are complex and change frequently, and compliance often requires close attention to each jurisdiction in which data is stored or passes through. Because such laws often differ in significant but subtle ways, a blanket consent given with the breadth required by some cloud providers' terms of service could result in a violation of applicable data protection laws in multiple jurisdictions.

Similarly, export control regimes such as the U.S. Export Administration Regulations

---

[83] Soonr Terms of Service and End User License Agreement § 9.2, http://www.soonr.com/security/eula.html (emphasis added).

[84] Roxana Geambasu, Yoshi Kohno, Amit Levy, and Hank Levy, *Vanish Frequently Asked Questions*, http://vanish.cs.washington.edu/faq.html.

[85] *Id.*

("EAR") and the International Traffic in Arms Regulations ("ITAR") require a license for certain kinds of data to be exported from the U.S. and make it impermissible to export or re-export of certain kinds of data to prohibited destinations. If a client places such data in records it entrusts to a lawyer or law firm, and counsel then entrust such data to a cloud, such data could be moved in violation of the EAR or the ITAR as part of the service provider's routine relocation of such data to servers in other jurisdictions. The risks of such occurrences raise potential ethical issues for a law firm if it entered into such an agreement. Although a review of such issues is beyond the scope of this essay, they are likely to become matters of ethical concern as a direct result of cloud providers' use of servers located in and transferring data between multiple jurisdictions with possibly conflicting requirements for data protection.

Although a cloud provider may intend to apply its security measures consistently throughout its enterprise, such consistency may decline as the locations of servers and staff multiply and as the number of jurisdictions and cultures increases. A law firm and its clients might reasonably object to storage of client data in certain jurisdictions due to concerns for local security standards, reported incidents, or political instabilities.

Law firms whose clients include governments and government entities may need to know the exact locations of such clients' data within the cloud provider's storage system, since a failure to know such information could incur risks of violating the client's own security requirements and instructions to the law firm regarding adherence to such requirements. The firm may be under express instructions from that client to avoid storing data in servers within the jurisdiction of a known adversary. For such firms there could be ethical issues under the Rule 1.4(a)(2) to "reasonably consult with the client about the means by which the client's objects are to be accomplished" and under the Rule 1.3 requirements "to act with reasonable diligence and promptness in representing a client".

(b) *Considerations and Precautions*.

Law firms representing clients who have special security concerns based on political and geographic considerations and who insist on heightened measures and restrictions regarding the storage and transfer of their data may find that a public cloud provider's standard terms of service do not accommodate such concerns. On this subject, counsel may find helpful general guidance in a 2006 New Jersey Advisory Committee on Professional Ethics opinion on electronic storage and access of client files:

> the benefit of digitizing documents in electronic form is that they "can be retrieved by me at any time from any location in the world." This raises the possibility, however, that they could also be retrieved by other persons as well, and the problems of unauthorized access to electronic platforms and media (i.e. the problems posed by "hackers") are matters of common knowledge. The availability of sensitive client documents in an electronic medium that could be accessed or intercepted by unauthorized users therefore raises issues of confidentiality under RPC 1.6.
>
> The obligation to preserve client confidences extends beyond merely prohibiting an attorney from himself making disclosure of confidential information without client consent (except under such circumstances described in RPC 1.6). It also requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure. ...
>
> The critical requirement under RPC 1.6, therefore, is that the attorney "exercise reasonable care" against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access.

> "Reasonable care," however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax.[86]

Such concerns suggest that a law firm give serious consideration to due diligence of any public cloud provider as a condition for entering into a service agreement with such provider. There may be many client-specific checks that need to be made of a public cloud provider in order to ensure that the law firm has exercised "reasonable care" to prevent such service provider from "disclosing or using confidential information of a client."

It would also be prudent for a law firm to develop policies and procedures to be invoked in case of a data breach involving the client's data and documents stored in the public cloud. These should not be limited to the requirements of the applicable jurisdiction's data breach statutes, as there may be an ethical duty to disclose such breach to the affected or potentially affected clients under the NYRPC Rule 1.4(a)(3) requirement to "keep the client reasonably informed about the status of the matter." Moreover, if there is a reasonable possibility that such a breach could result in damage to the client, which the client mitigate if it knew the breach had occurred, then failure to report the incident to the client could risk a breach of the NYRPC Rule 1.1(c)(2) requirement that the lawyer shall not intentionally "prejudice or damage the client during the course of the representation…"

In 2009, the Illinois State Bar Association ("ISBA") reviewed the issues that may arise if a law firm elects to have its computer network managed by an off-site third party vendor. The ISBA noted that in looking at the same scenario, the American Bar Association concluded that if the third party vendor breaches the confidentiality of the firm's client files,

> a lawyer may be obligated to disclose this breach to its client if it is likely to affect the position of the client or the outcome of the client's case. Such disclosure may be required under RPC 1.4(b), pursuant to which a 'lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."[87]

(7) *Diminished Ability to Protect Data from Government Surveillance or Seizure*.

Data transmitted wirelessly can be intercepted more easily than data sent through telephone wires. Encryption may reduce the potential number of persons who can intercept it, unless they are government agents or government-sponsored entities. Moreover, the amount of data that can be intercepted will usually be less than the data that can be seized if government agents gain access to the cloud provider's servers.

Although the use of national security letters ("NSL") by the Federal Bureau of Investigation ("FBI") can result in the government gaining access to data on virtually any computer in the United States, it is equally true that a law firm likely will put up a far more resolute and vigorous defense of client confidential information than will a cloud provider. The latter may find it advantageous to cooperate with the government, offer token resistance, and/or be barred by the terms of an NSL from even informing the law firm customer that its client

---

[86] New Jersey Supreme Court Advisory Comm. on Prof'l Ethics, Opinion 701, *Electronic Storage and Access of Client Files*, Apr. 24, 2006, at 1, http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html.

[87] Illinois State Bar Ass'n, Opinion 10-01, July 2009, at 3, http://www.isba.org/ethicsopinions/10-01.pdf (quoting ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 95-398).

confidential information has been seized by federal agents.

In addition, there are reported instances in which the FBI has received overproduction of records sought from an internet service provider. For example, the FBI, when conducting a national security investigation and having obtained a court order to an Internet service provider to produce e-mails sent to a single e-mail address, received instead *all* of the emails from the entire domain because the Internet service provider improperly set filtering controls and collected data on the domain instead of the single email address.[88] That errors in instructions or in implementing instructions for such production can occur is troubling, but that the occurrences are not rare should be much more of a concern for law firms and lawyers intent on protecting their client's confidential information. As the *New York Times* reported,

> [A]n intelligence official, who spoke on condition of anonymity because surveillance operations are classified, said: 'It's inevitable that these things will happen. It's not weekly, but it's common.
>
> A report in 2006 by the Justice Department inspector general found more than 100 violations of federal wiretap law in the two prior years by the Federal Bureau of Investigation, many of them considered technical and inadvertent.[89]

Providers of web-based email may represent that they offer security against any intrusion (including by government agencies), but then fail to provide it when faced with a court order. For example, Hush Communications, Inc., a Canadian company and operator of the web-based email service Hushmail.com, reportedly represented that "not even a Hushmail employee with access to our servers can read your encrypted e-mail, since each message is uniquely encoded before it leaves your computer."[90] However, as the result of a mutual legal assistance treaty between Canada and the United States, Hush released to U.S. Drug Enforcement Agents 12 CD's containing e-mails from three Hushmail accounts.[91]

Although supposedly Hushmail could only release encrypted emails which could not be read by government agents, users reportedly had found it too burdensome to use Hushmail's most secure services, which required installing Java and loading and running the Java applet, and elected instead to use a more traditional form of web-mail offered by Hushmail in which the user stores a passphrase with Hushmail. The court order required Hushmail to use such stored passphrases to decrypt the emails before releasing them to government agents.[92]

(a) *Ethical Issues*.

NSLs present unique and unusually sensitive ethical issues for counsel in fulfilling the NYRPC Rule 1.6(c) duty to exercise reasonable care to prevent persons "whose services are utilized by the lawyer" from disclosing client confidential information. Where a law firm receives an NSL, it is on notice of the risks and can respond accordingly if it has adopted policies and procedures for handling NSLs. Such policies likely will place a priority on protecting client

---

[88] Eric Lictblau, *Through an Error, F.B.I. Gained Unauthorized Access to E-Mail*, N. Y. TIMES, Feb. 17, 2008, at 1, 20.

[89] *Id.* at 1.

[90] Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED.COM, Nov. 7, 2007, http://www.wired.com/threatlevel/2007/11/encrypted-e-mail/.

[91] Plennes Aff., UNITED STATES OF AMERICA V. TYLER STUMBO, Sept. 17, 2007, ¶¶ 4 and 15, http://www.wired.com/images_blogs/threatlevel/files/steroids.source.prod_affiliate.25.pdf.

[92] Singel, *supra* note 115.

confidential information from disclosure and may include measures to be taken in an initial review of the NSL.

There is likely to be a very different set of priorities where the recipient of an NSL is a public cloud provider, however, especially if the vendor is a major enterprise that has received many NSLs already. It is important for a law firm to be aware of the challenges that NSLs present to a public cloud provider and to the likelihood that the public cloud provider may find it in its own interests to do little to limit the intrusion of the government into files that contain a law firm's client's confidential information. A good summary of those challenges is presented in *Responding to National Security Letters,* which observes that such challenges include the following:

> The company [recipient] must be able to review the national security letter, but the federal agents may not permit the company to keep the letter or a copy of it. If the agents indicate that the company may not keep the letter or make a copy, company representatives who review the document should take notes in order to evaluate its legality and content.
>
> …
>
> In all likelihood, federal agents will deliver a national security letter that certifies that disclosure of the letter or its contents to persons beyond those to whom disclosure is permitted (e.g., legal counsel) may result in a danger to U.S. national security; interference with a criminal, counterterrorism, or counterintelligence investigation; interference with diplomatic relations; or danger to the life or physical safety of any person. Although federal courts have held that this nondisclosure requirement violates the First Amendment [footnote omitted], companies will likely be cautious and comply with the nondisclosure obligations.[93]

Once client data and documents are stored in a public cloud, they not only reside in a location whose custodian will have little, if any, incentive to protect them from government intrusion under the authority of an NSL, but also will be a more likely target for government requests for information under an NSL. Entrusting client data and documents to a public cloud would appear to increase the risks of disclosure to the federal government and of such disclosure occurring without the law firm or its clients awareness. Such risks may be significantly greater for some clients because of their activities or type of business, and such risks can be enhanced without any suggestion that the activities might be at risk of being unlawful.

(b) *Considerations and Precautions*.

A law firm customer of a public cloud provider probably will not be able to negotiate to receive notice from the provider that it has received an NSL that would cover data and documents of the law firm's clients. Thus, the decision of whether to store such documents and data in a public cloud may, for certain clients, require additional careful consideration in order to comply with the NYRPC's requirements to avoid damaging a client and to exercise reasonable care to prevent the cloud provider from disclosing client confidential information. Such considerations may deserve to be discussed with the client to ensure compliance with the NYRPC requirement to reasonably consult with the client about the means by which the client's objectives are to be accomplished.

---

[93] David P. Fidler and Sarah Jane Hughes, *Responding to National Security Letters* 42, 44 (2009).

(8) *Diminished Ability to Monitor and Ensure Secure Purging of Archived Records*

Sometimes the concern regarding client confidential information centers not on preservation but on destruction, as when a protective order or settlement agreement requires the destruction of confidential materials post-litigation. In such cases, it is not enough to shred hard copy pages or delete a digital file from a hard disk. Even after a matter ends, the confidentiality of information concerning that matter remains an imperative until such information can no longer be accessed in whole or in multitudinous parts.

Information that can be reconstructed into an incomplete and partially identifiable record are doubly dangerous. To the extent that fragments of confidential information can be extracted, pieced together in a semblance of their original structure and rendered coherent and interpretable, confidentiality and the client's interests may become compromised, risking a breach of counsel's ethical duty to protect a client's confidential information from disclosure. To the extent that extracts of confidential information can be read but remain incomplete, there is the added risk that the information may be taken out of context and seriously misinterpreted, distorting the content and its purpose. It may be the case in some situations that the publication of such mangled fragments could only be defended against by a further disclosure of client confidential information.

Hard copy information can be eradicated by fairly standard practices, including careful shredding and incineration. Unfortunately, data stored on digital media cannot be eradicated as straight-forwardly and reliably as data in hard copy. As noted by NIST in the "Guidelines for Media Sanitization", published in 2006, digital media "may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality."[94] The chief challenge is that deletion of digital files may not delete the data contained in the files, which can remain intact and recoverable on the digital media. The reasons for the data's persistence despite purportedly being "deleted" are inherent in the design of digital storage:

> A cardinal rule for product design of computers, disks, and tapes is to protect user data from accidental deletion. Computer operating systems erase disk files into recycle or trash folders to prevent accidental deletion of user data, and have file recovery commands. File deletion erases only file block pointers, links that let a file system reassemble a file.[95]

In 1985, the DoD established its standard for eradicating digital data. Document DoD 5220 required "two fixed-character overwrites and one random-character overwrite, followed by a verify read,"[96] but that procedure eventually ceased to capable of eradicating data from disk drives, because design of the disk drives made the first two overwrites ineffective:

> All drives today use partial response-recording channels, a technology that randomizes user data before recording, so the first two writes of DoD 5220 no longer function as intended. The US Defense Security Service today requires that federal agencies using

[94] Richard Kissel, Matthew Scholl, Steven Skolochenko, and Xing Li, *Guidelines for Media Sanitization: Recommendations of the National Inst. of Standards and Tech.*, NIST SPECIAL PUBL'N 800-88, Sept. 2006, at ix, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[95] Gordon F. Hughes, Daniel M. Commins, and Tom Coughlin, *Disposal of Disk and Tape Data by Secure Sanitization*, IEEE SECURITY AND PRIVACY, July/August 2009, at 29.

[96] *Id.* at p. 30.

> overwrite utilities have an authorized DoD laboratory evaluate them for proper functionality. [Footnote omitted.] NIST 800-88 replaces DoD 5220 for disk sanitization.[97]

The federal government has begun citing NIST 800-88 as the applicable standard in regulations concerning data security. For example, in the recently enacted HITECH Act:

> NIST 800-88 recommends that organizations store confidential information on media labeled in accordance with internal operating classifications and associate such media with the kind of data sanitization that will eradicate it to the extent necessary to prevent its recovery.[98]

Unfortunately, it does not appear that most law firms or lawyers are familiar with NIST 800-88 and its standards. It also is doubtful that most law firms and lawyers or their clients have their confidential information so well organized that it is stored on media labeled by the level of confidentiality as recommended by NIST 800-88.

NIST 800-88 encourages that plans for data sanitization be made based on the media and the level of risk to confidentiality: "categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then decide on the appropriate type of sanitization."[99] Ideally such plans would be made before or at the same time that the data is stored, but in most cases such plans will likely be made much later. But in any event, they need to be made carefully before entrusting data to storage media that are not controlled by the law firm or its lawyers, because there is little or no evidence at present that cloud service providers have made secure sanitization of data a high priority or included it in their plans for customers.

For example, in Google Docs' Terms of Service there is no mention of "data sanitization" or any provision that addresses Google's responsibilities for eradicating confidential data entrusted to its cloud or even a covenant to verify eradication of data if requested by a customer. If plans for secure data sanitization were a priority for a cloud service provider, one would think that the service provider would add that to the list of excluded or disclaimed warranties and/or limits of liability, but there is no provision on the subject in, for example, Google Docs Terms of Service.[100] Similarly, in the Amazon Web Services Customer Agreement the provisions on "Data Preservation in the Event of Suspension or Termination" and on "Post-Termination Assistance" mention possible preservation or retrieval, but say nothing about secure data sanitization or customer-authorized eradication of data from the hard drives of Amazon's cloud servers.[101]

NIST 800-88 identifies three methods of data sanitization suitable for eradicating confidential information from digital media – clearing, purging, and destroying – and the level and kinds of risk that each is best at protecting against. There is no established standard for what level of data eradication needs to be achieved by lawyers or law firms to fulfill the objective of protecting client confidential information stored in digital media. Nonetheless, there are federal standards that can be used as guidance and that would help a lawyer or law firm document and demonstrate that reasonable measures had been taken to protect the

---

[97] *Id.*

[98] Kissel at al., *supra* note 120 at 7.

[99] *Id.*

[100] Google Docs Terms of Service, *supra* note ___ at §§ 14-15.

[101] Amazon Web Services Customer Agreement, *supra* note ___ at §§ 3.7-3.8.

confidentiality of such information. For example, the recently enacted HITECH Act defines that "unprotected personal health information" to mean such information that is not secured by a technology or methodology identified by the Secretary of the Department of Health and Human Services ("DHHS") in guidance the Secretary is required to issue annually in order for holders of such information to render it "unusable, unreadable, or indecipherable to unauthorized individuals."[102]

The DHHS in April 2009 issued guidance for security of such information, and explained that "protected personal health information" would be deemed "unusable, unreadable, or indecipherable to unauthorized individuals" only if certain measures had been taken, and explained that such information when stored or recorded on electronic media would eventually need to be "cleared, purged or destroyed consistent with" NIST 800-80.

Lawyers and law firms should give serious consideration to adopting a similar standard, *i.e.,* that when eradicating client confidential information such information, when in digital media, should be rendered "unusable, unreadable, or indecipherable to unauthorized individuals" by implementing the guidance provided in NIST 800-80.

(a) *Ethical Issues*.

Entrusting client confidential data to a cloud service provider means moving a copy of such records outside of counsel's immediate control and placing it on digital media under the control of at least one third party – the service provider – and potentially multiple third parties, depending on the extent to which the service provider itself outsources or subcontracts the management of its cloud servers. With such data located off-site in on a third party's digital media a number of data sanitization issues arise, among which are:

- *Re-location of Data.* Will the cloud service provider relocate the data to other servers in the same site or to servers in other sites? If so, there is the risk that the cloud service provider will not eradicate the data from the original server(s). Any party gaining unauthorized access to such servers, from onsite or wirelessly via the Internet might thereby gain access to residual confidential data of the client.
- *Retirement of Servers.* Will the cloud service provider replace the server during the storage period? If so, there is the risk that the cloud service provider will not eradicate the data when disposing of (or selling) the server. Any party gaining possession of the discarded server might gain access to the residual confidential data of the client.
- *Backup Media*. Will the cloud service provider be making backup copies of the data? If so, there is the risk that upon replacement of such media, the client's confidential data will remain on the discarded media, and thus be potentially accessible by unauthorized persons.
- *Custody of Discovery Records.* When a firm produces client electronic records in fulfillment of discovery obligations, is the recipient firm entitled to store such records in the cloud without an express commitment to take "reasonable precautions" to ensure that such records at not thereby put at heightened risk of

[102] DEPARTMENT OF HEALTH AND HUMAN SERVICES, GUIDANCE SPECIFYING THE TECHNOLOGIES AND METHODOLOGIES THAT RENDER PROTECTED HEALTH INFORMATION UNUSABLE, UNREADABLE OR INDECIPHERABLE TO UNAUTHORIZED PERSONS FOR PURPOSES OF THE BREACH NOTIFICATION REQUIREMENTS UNDER SECTION 13402 OF TITLE XIII (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT) OF THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009, 74 Fed. Reg. 19006, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.

disclosure to unauthorized parties? When the litigation concludes, will the firm be obligated to ensure that any such records entrusted to a cloud service provider have been securely sanitized (in accordance with NIST 800-88)? If not, the client's confidential information could be at continuous risk for years thereafter, and if clients believe that their data will be put at such heightened risks, counsel may find it increasingly difficult to coax and persuade clients to fulfill their discovery obligations.

- *Expiration of Preservation Order.* If a court issues a protective order that requires destruction of confidential information at the conclusion of a trial, will the court include (and should counsel propose) a detailed statement of the measures to be taken to ensure that such data, if entrusted to a cloud, will be securely sanitized in all media used to store it by the cloud service provider? Would failure to propose such measures risk an ethical violation?
- *Failure of a Cloud Server's Storage Media.* If hard drives or other storage media of the cloud service provider fail while still under warranty by the original equipment manufacturer ("OEM"), will the cloud service provider send the drive back to the OEM for a warranty repair or replacement? If so, it is unlikely that an effort will be made to eradicate the confidential data contained on such media before releasing them to the OEM. In that event, either the OEM and its repair personnel will have access to the confidential data (and may not be under any confidentiality agreement concerning accessing such data), or if the OEM elects to replace the media and discards the failed media there is the risk that the OEM will invest no effort to eradicate the confidential data contained on the media and will thereby place such data at risk by failing to sanitize such data. It is important to note that in such instances, the cloud service provider will probably have relinquished all control over the failed media when it sends it back to the OEM for warranty repair or replacement.
- *Termination of Cloud Relationship*. Will the cloud service provider eradicate all copies of client confidential data if requested by counsel upon termination of the relationship with the service provider? If not, the risks of residual client data may be multiplied.
- *Termination of Client Relationship.* Will the cloud service provider eradicate all copies of client confidential data if requested by counsel in the event of termination of the attorney-client relationship? What if the client asks that the data be transferred from its former counsel's cloud service provider to the cloud service provider of its new counsel? Will the cloud service provider comply and, if so, will it then securely sanitize the client's data from the media on which it had been stored? If not, the client may be at continuing risks of unauthorized access to its confidential data.

In each of those instances, failure to ensure secure sanitization of client confidential information from each of the media in which it has been recorded or stored in the cloud raise the possibility that counsel will fall short of the standard set by NYRPC Rule 1.6(c):

> A lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and *others whose services are utilized by the lawyer* from disclosing … confidential information of a client …[103]

[103] NYRPC Rule 1.6(c), *supra* note 95.

If the client has terminated the relationship with counsel, there is also the risk of failing to meet the standard set by NYRPC Rule 1.9(c)(2):

> A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter …
>
> (2) reveal confidential information of the former client protected by Rule 1.6 except as these Rules would permit or require with respect to a current client.[104]

Although NYRPC Rule 1.6 requires that a lawyer exercise "reasonable care" to prevent service providers, including a cloud service provider, from disclosing a current client's confidential information, there is no similarly express requirement in NYRPC Rule 1.9(c)(2) regarding a former client's confidential information. Perhaps the NYRPC's drafters did not have an opportunity to consider the ramifications of cloud computing, or perhaps they considered the ethical challenges of cloud computing but did not take into account the risks inherent in a former client's confidential data continuing to reside on cloud servers. Absent an ethical provision directly addressing the issue of a former client's confidential data remaining on a third party's servers, counsel will have to make their own evaluation of the risk under the NYRPC.

It is important to note that the client confidential information of concern here includes all such information that a lawyer or law firm is not otherwise required to retain for seven (7) years under NYRPC Rule 1.15(d), such as "copies of all retainer and compensation agreements with clients,"[105] "copies of all bills rendered to clients,"[106] and "copies of all records showing payments to lawyers, investigators or *other persons*, not in the lawyer's regular employ, for services rendered or performed."[107] (Note also that the seven year record retention rule would appear to apply to the "payments" to the cloud service provider.)

Client confidential information not covered by the seven year retention rule is put at risk when it is entrusted to a cloud service provider and thereafter the attorney-client relationship terminates. Counsel does not have an obligation to retain such records, but clearly counsel has not ceased to be responsible for the protection of client confidential information of a former client. But what precisely is counsel's obligation for such information when it remains on a cloud service provider's servers, even after its former counsel, at the client's request, has arranged for digital copy of all such information to be transferred to the client's new counsel? Surprisingly, this issue is not addressed in the NYRPC, although it just came into effect in April 2009.

At present, cloud service providers have not demonstrated in their marketing materials or terms of service an intention to seriously consider the eradication of residual confidential data entrusted to them by customers such as lawyers, law firms and their clients. As a result, there appears to be a significantly high risk that confidential data of a lawyer's or law firm's clients, if entrusted to a cloud, will remain on one or more cloud servers after termination of the client's relationship with the lawyer or law firm. Once that happens, the risks to the client's confidential data, and the ethical risks to its counsel, start to multiply prodigiously as the data become increasingly removed from the control of parties who have an interest in protecting its confidentiality.

The first loss of control may occur when the relationship between the client and counsel

---

[104] NYRPC Rule 1.9(c)(2), *supra* note 95.

[105] *Id.*, Rule 1.15(d)(i).

[106] *Id.*, Rule 1.15(d)(iii).

[107] *Id.*, Rule 1.15(d(vi) (emphasis added).

terminates. The client may instruct counsel to transfer the electronic records to a new counsel. However, copies of the client's confidential data may nonetheless remain on the cloud provider's servers after a copy has been forwarded to the new counsel (or its cloud service provider) as requested. The client's original counsel may now have lost effective control of the client's confidential data, particularly if counsel is unaware that the data continues to reside on the cloud service provider's servers. Counsel will not be aware of the continuing need to exercise reasonable care to prevent the cloud service provider from disclosing such data or keeping such data from being accessed by unauthorized third parties. Quite simply, counsel may not realize the need to insist on secure sanitization of the residual confidential data.

Loss of control may also occur if the original cloud service provider's storage media fails and the service provider sends the media back to the OEM for warranty repair or replacement. At that point, as noted by NIST 800-88, the party sending the media back to the OEM may be at risk of relinquishing control over that media (and over confidential data contained on it), if the cloud service provider has not required in an agreement with the OEM that the cloud service provider retain effective control over the media and that the OEM preserve the data's confidentiality throughout the warranty repair period. Unfortunately, there appears to be little incentive for a cloud service provider to negotiate (and pay) for such control and confidentiality safeguards, particularly if its own customers are not pressing it to demonstrate such precautions. Thus, NIST 800-88 draws a clear distinction between circumstances in which control over the media and its data is retained and those in which control is relinquished:

> Media being turned over for maintenance are still considered under organization control if contractual agreements are in place with the organization and the maintenance provider specifically provides for the confidentiality of the information."
>
> …
>
> Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization are considered to be out of organizational control.[108]

When an organization plans to take an action that will cause it to relinquish or lose control over media containing confidential information, NIST 800-88 recommends that the organization "purge" all confidential information on such media and verify that the "purge" eradicated the confidential information. NIST 800-88 explains that

> A representative sampling of media should be tested for proper sanitization to assure the organization that proper protection is maintained. Verification of the process should be conducted by personnel without a stake in any part of the process.[109]

If the cloud service provider relinquishes control over the storage media and a client's confidential data stored on such media, the client's former counsel will no longer have any way of exercising control over the media and security of the confidential data. Counsel has no contractual relationship with the OEM, and its contractual relationship with the cloud service provider may have terminated or does not expressly apply to data of a former client a copy of which has been forwarded to a new counsel or its cloud service provider. The risk remains, however, that the client's confidential data could be disclosed to, or accessed by, unauthorized third parties once the client-attorney relationship has terminated or once the storage media has

---

[108] Richard Kissel, Matthew Scholl, Steven Skolochenko, and Xing Li, *Guidelines for Media Sanitization*, NIST SPECIAL PUBLICATION 800-88, Sept. 2006, at 7, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[109] *Id.* § 4.7.2, at 15.

been sent to the OEM for repair. To the extent that one views such risks as significant, there would appear to be a serious gap in the NYRPC.

Until that gap is corrected by amendment of the NYRPC, it would be prudent for counsel to interpret NYRPC Rule 1.9(c)(2) as implying a duty to do more than avoid revealing confidential information of a former client protected by Rule 1.6, but to take steps before losing control of such data to ensure that a former client's confidential information will receive the same level of protection as it received when counsel represented the client.

Put differently, since Rule 1.6(c) requires a lawyer or law firm to exercise reasonable care to ensure that *others whose services are utilized by the lawyer* will not disclose the client's confidential information, one could construe entrusting such information to a cloud service provider's digital media as nullifying an underlying assumption of Rule 1.6(c), namely that the client's confidential information will only be at risk from counsel's service providers during the representation. In the pre-digital era, that assumption was fundamentally sound: when the attorney-client relationship terminated, the attorney would usually return or arrange for secure destruction of the hard copies containing client confidential information. If counsel retained such information in a warehouse, it nonetheless remained under an obligation to ensure that the warehouse did not reveal or grant access to the former client's confidential information. However, if counsel ordered the secure destruction of such records, there was little or no risk of confidential data persisting in the way it does on a cloud service provider's digital storage media. It appears to be consistent with the spirit of Rule 1.6(c) that if counsel entrusts client confidential information to a cloud service provider and its digital media, counsel has an ethical obligation to exercise reasonable care to ensure that the service provider does not reveal (or allow access to) that information from the time it receives it until such time as it securely sanitizes such data in accordance with the standards set forth in NIST 800-88. Reading the NYRPC more narrowly and accepting the gap that appears to exist with respect to protection of a former client's confidential information would appear to be inconsistent with the intent of the Rules of Professional Conduct and risk damage to counsel's reputation and to the reputation of the legal profession.

(b) *Considerations and Precautions*.

If counsel discusses with a client the security issues that may arise from entrusting the client's confidential information to a cloud service provider and its digital media, it would also seem prudent for counsel to discuss carefully with the client the security issues that may need to be addressed in order to ensure that data sanitization measures will be sufficient to protect such information in the circumstances we have reviewed.

Before discussing such issues with a client, counsel will need to consider carefully whether its arrangement with the cloud service provider includes contractual terms that cover the full range of risks of confidential data remaining on digital storage media. Counsel should anticipate that cloud service providers might strongly resist being required to provide such safeguards. The omission from the cloud service providers' terms of service of any discussion of the secure eradication of confidential data suggests that the issue is for now being ignored, but counsel cannot safely ignore or postpone addressing such issues. Once the client's confidential information has been entrusted to a cloud service provider, the problem of such data's eventual eradication will inevitably arise. Delaying addressing it will likely reduce counsel's leverage in negotiating such issues with the cloud service provider, and risks having a data breach occur, with all of the attendant risks.

In order to address such issues adequately, it may be necessary for lawyers and law firms to confer with prospective cloud service providers and, at a minimum, map out in detail each digital storage or digital recording of client information that may occur once a copy of the

data is transferred from counsel's computer's to the cloud's servers. From that map, counsel can identify the probable circumstances under which the media will leave the cloud service provider's control and require "purging" at the standard set by NIST 800-88.

But is this a realistic expectation for counsel? Will any cloud service provider be willing to underwrite the expense of secure data sanitization every time that client confidential information may be put at risk by remaining on digital media? Counsel's response needs to meet the standard set by the NYRPC of "reasonable care". Counsel's ethical obligations cannot be fulfilled by accepting a vendor's insistence that the required precautions are too burdensome, expensive, and would impose operational inefficiencies. Cost and efficiency are not unimportant, but the ethical obligations to protect a client's confidential information remain an imperative. Protecting client confidences and client confidential information are essential for a client to trust its counsel. The promised benefits of cloud computing appear to be significant, but they also appear to have so far obscured the need to address how and when the cloud service provider must securely sanitize client confidential data in order to prevent its disclosure to unauthorized persons.

With so much attention focused on getting data into the cloud and on the possible loss of data while in the cloud, the promoters of cloud computing and their customers risk overlooking the problem of data remaining on a cloud service provider's servers long after they were supposedly "deleted," transferred, or backed up. The proliferation of storage sites will likely multiply the risks that such data may be disclosed to or accessed by unauthorized persons. Since counsel appear to remain ethically obligated to protect such data, even when the data relates to matters of a former client, the increase in the risks to the data would appear to also increase the ethical risks for counsel.

With cloud computing, as with each new communications technology, there are multiple possibilities for brave new ethically challenging worlds for law firms, lawyers, and judges.

R.L.T.

C.R.