2011

Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing

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

Roland L. Trope
United States Military Academy

RED SKIES IN THE MORNING—PROFESSIONAL ETHICS AT THE DAWN OF CLOUD COMPUTING

Roland L. Trope[†] and Sarah Jane Hughes[††]

---

† Mr. Trope is a partner in the New York office of Trope and Schramm LLP. He serves on the Senior Advisory Board at IEEE Security & Privacy and is an adjunct professor at the United States Military Academy at West Point. Mr. Trope earned his B.A. from the University of Southern California, a B.A. and M.A. from Oxford University (where he was a Marshall Scholar and Danforth Fellow), and a J.D. from the Yale Law School. He represents clients in various fields including government and defense procurement, regulatory compliance in cross-border transactions, licensing of technology and intellectual property, cyberspace law, ethics regulations for government contractors, and mobile payments. He is the co-author of two books published by the American Bar Association (ABA), *Checkpoints in Cyberspace: Best Practices for Averting Liability in Cross-Border Transactions* (2005) and *Sailing in Dangerous Waters: A Director's Guide to Data Governance* (2005). Other publications relevant to this article that Mr. Trope authored or co-authored are *Hardening the Target,* IEEE SECURITY & PRIVACY, Sept.–Oct. 2008, at 77 (with Monique Witt and William J. Adams) and *Emergent Duties to Harden Targeted Enterprises and Their Digitized Data,* 64 BUS. LAW. 219 (2009). At West Point, Mr. Trope lectures on copyright, project management, and ethics in the Electrical Engineering and Computer Science and in the Civil and Mechanical Engineering Departments. He frequently lectures to a broad array of professional audiences, including as a presenter of CLE programs for the ABA and the Association of the Bar of the City of New York. He can be reached at rltrope@tropelaw.com.

†† Ms. Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law at Indiana University. She is a graduate of Mount Holyoke College and of the University of Washington School of Law. Hughes is the co-author of *Responding to National Security Letters: A Practitioner's Guide* (ABA, 2009) (with David P. Fidler), and of articles on payments and banking law, policies and regulations related to the deterrence of money laundering, and data security and privacy.

Red sky at night,
Sailor's delight;
Red sky at morning,
Sailor's warning.[1]

The research for this article originated in essays prepared for two CLE presentations in 2009 and 2010. Roland Trope and Claudia Ray, *The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms and Judges,* Essay for CLE Program, ABA Annual Meeting, San Francisco, August 2010; Roland 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,* ABA Annual Meeting, Chicago, August 2009. Copies of both essays are on file with the authors. The research for this article was current as of August 4, 2011.

The authors would like to thank Claudia Ray for her earlier work and Vince O. Polley, a former Chair of the Cyberspace Law Committee and Chair of the ABA's Standing Committee on Technology, Col. Barry L. Schoop, Col. Nathaniel Causey, Geoffrey Schwartz, and Dr. Monique Witt for comments related to specific cyber risks and duties that are discussed in this article.

In addition, the authors want to acknowledge the gracious invitation from the editors of the *William Mitchell Law Review* to publish this article, and to extend special thanks to Professor Christina Kunz, who is a faculty member at William Mitchell College of Law and until recently a vice chair of the American Bar Association's Cyberspace Law Committee—the committee which sponsored one of the two CLE programs—for her suggestion to the editors to invite us to contribute to this issue.

Three exceptional research assistants contributed to this article in

Lady Gaga has made herself a paragon of pop ambition and a spokeswoman for equal rights, but on Monday she became an unwitting symbol for something else: the pitfalls of cloud computing.[2]

---

significant ways, Christina Clark, E. Sebastian Arduengo, and Peyman Yousefy, Maurer School of Law, Classes of 2011, 2012, and 2013, respectively. Finally, the authors thank Marion Conaty and Max Exter of the Maurer School of Law whose timely assistance was instrumental when this manuscript (with exquisite irony) became corrupt. Without the contributions of these five individuals, this article would never have been finished. Regardless of their talents, any remaining errors are the authors' responsibilities.

The views expressed in this article are solely those of the authors and have not been approved by, and should not be attributable to, the U. S. Military Academy at West Point, the U.S. Department of Defense, the U.S. Government, the Maurer School of Law, or the Trustees of Indiana University.

1. NURSERY RHYMES—LYRICS, ORIGINS & HISTORY!, http://www.rhymes.org.uk/red_sky_at_night.htm (last visited Oct. 18, 2011). The website http://www.rhymes.org.uk/red_sky_at_night.htm attributes the rhyme's origins to the Bible:

> He answered and said unto them, When it is evening, ye say, It will be fair weather; for the sky is red. And in the morning, It will be foul weather today [sic]; for the sky is red and lowering. O ye hypocrites, ye can discern the face of the sky, but can ye not discern the signs of the times?

Id. (quoting *Matt.* 16:2–3). Shakespeare also paraphrased this old adage in *Venus and Adonis* (1593). WILLIAM SHAKESPEARE, THE ARDEN SHAKESPEARE COMPLETE WORKS 55 (Richard Proudfoot et al. eds., 1998) ("Like a red morn, that ever yet betoken'd, Wreck to the seaman, tempest to the field, Sorrow to shepherds, woe unto the birds, Gusts and foul flaws to herdmen and to herds."); *see also* EVERYDAY MYSTERIES: FUN SCI. FACTS FROM THE LIBR. OF CONGRESS, http://www.loc.gov/rr/scitech/mysteries/weather-sailor.html (last visited Oct. 18, 2011) (explaining the history behind the saying).

2. Ben Sisario, *Lady Gaga Sale Stalls Amazon Servers*, N.Y. TIMES, May 23, 2011, *available at* http://www.nytimes.com/2011/05/24/business/media/24gaga.html?ref=technology. In May 2011, on the release of Lady Gaga's new album, "Born This Way," Amazon.com offered "a one-day sale of the MP3 version of the album for ninety-nine cents, a full $11 less than its price at iTunes, the Web's dominant music retailer." *Id.* The discount reportedly provides Amazon a means of promoting its new "Cloud Drive" service that "allows users to store music files on remote servers and stream them over the Internet to their computer or smartphone." *Id.* However, the promotion proved so popular that the requests for the "99 cent" download overwhelmed Amazon's cloud computing servers, which "stalled" and prevented many users from completing the download or from listening to the full album. *Id.* In addition, in late May 2011, a staff developer at the Tenafly, New Jersey school district employed a Lady Gaga impersonator to deliver a presentation about bullying over the Internet. Karen Sudol, *Tenafly School Officials Reviewing 'Lady Gaga' Incident*, NORTH JERSEY.COM (May 31, 2011), http://www.northjersey.com/news/Tenafly_school_officials_reviewing_Lady_Gaga_incident.html. After a student queried administrators as to the true identity of the speaker, the school district called the developer's actions "a clear lapse in judgment." *Id.* Though the employee has not been formally disciplined, her case also highlights the pitfalls that may be encountered when utilizing new technologies in the workplace. *Id.*

I. INTRODUCTION

For three decades, the practice of law has adjusted to the incoming tide of the Digital Era. The tide has not raised all boats. What has required so much adjustment is the arrival of a succession of new communications technologies. These new technologies promise far-reaching benefits including decreased processing time, enhanced reach of communications (with e-mail eclipsing faxes), global transmission of text messages and "tweets," compression of reams of documents into portable storage devices and thumb drives, and finally, global access to entire libraries via website data banks. However, these extraordinary advances have not been without cost.

Counsel have had to adjust to these new technologies and with each new advance learn how to take the best advantage of their greater efficiencies, and most importantly (although often underestimated), how to evaluate the hidden impact of each technology on counsel's professional responsibilities and ethical duties. But the ethical and professional obligations that arise when lawyers and law firms become "early adopters" of a new communications technology are not always immediately apparent.

Nor is it clear that the profession's ethics have kept pace with the incipient risks of these new technologies. The need to keep pace with technologies, the risks they may present to counsel and the client confidential information entrusted to them, and the relationship of those tasks to the professional ethics rules is the focus of this article. These needs will shape the policies that counsel establish for their legal practices and for their acquisitions of new technologies and will give them an increasingly influential role in the legal profession's operations. We would therefore suggest that the professional ethics rules be accompanied by fresh inquiries in light of recently emerging communications technologies, particularly cloud-based Web 2.0 applications and cloud computing services—and the vulnerabilities that they bring unnoticed into the enterprises that adopt and deploy them. This article will attempt to define broad areas of risk created by the new technologies and offer guidance to counsel on identifying such risks, assessing whether they can be mitigated by reasonable precautions, and if not, what counsel may need to do to fulfill their professional ethical obligations. In it, we examine obligations that include (1) understanding the features and operations of Web 2.0 communications, storage, and processing technologies; (2) increasing familiarity with emerging practices and customs of users

of such technologies; and (3) assessing risks that these technologies may pose for lawyers and law firms with obligations to comply with applicable rules of professional conduct.

This inquiry is timely given the vulnerabilities to cyber attacks that all enterprises, including law firms, face if they have adopted and deployed the communications technologies of the Digital Era. In Part II of this article, we discuss the damage done to the targeted enterprises and the latent but very real risks to which an enterprise exposes itself when it adopts a new communications technology. These technologies perforce contain innumerable security vulnerabilities whose existence, nature, location, and significance are largely unknown to the enterprise. Upon deployment, moreover, they create additional, unquantifiable vulnerabilities in an enterprise's cyber-based systems and provide covert access to an enterprise's privileged, proprietary, or other sensitive digital assets and records.

Thus, the enterprise becomes "porous" and is at high risk of having its digital assets targeted for misappropriation or destruction and the operations of its computer networks (and any machinery and equipment) brought under an adversary's command and control that can direct the enterprise to sabotage itself or to launch attacks on other enterprises. Cyber attacks occur by stealth, do their harm unopposed, and cease (often without detection or even awareness of the harm suffered). Company data often survives the attack; supervisory control and data acquisition ("SCADA") systems appear to function properly and it is only later (sometimes months later) that damage to targeted data or equipment becomes apparent. Often enterprises or information networks succumb to exploits that utilized data stolen from another enterprise. Trade secrets believed to be tightly protected are taken advantage of elsewhere, with no trail of misappropriation or clear evidence of the identity of the adversary. Finally, the enterprise's most sensitive data—the design of its cyber security safeguards and procedures—have been compromised, subverted to become part of the exploit that enables the attack to succeed.

The enterprise in essence engineers its own damage. Any new communications technology should therefore be examined for the presence of cyber vulnerabilities, lest a time-saver become a technology Trojan horse. Such a latent threat circumvents the enterprise's own physical safeguards and its cyber defenses.

An enterprise whose capabilities have been enhanced by innovations in communications technologies may belatedly realize

that such technology has compromised its cybersecurity, its digital assets, its ability to operate, its corporate integrity, in short, its existence. Technology vendors do not inform customers of the risks a new technology introduces into an enterprise—perhaps because they are aware or anticipate that they have not discovered all such vulnerabilities or made cybersecurity their highest priority. Some firms have recognized the need to change their priorities—and other firms have not.

The marketing literature for technologies seldom alerts potential buyers to the latent vulnerabilities created in deploying it, particularly if developers (or vendors) failed in design reviews and testing to discover these. Unlike a faulty wire in hardware, or short on a motherboard, or "bug" that impairs the operation of software, cyber vulnerabilities do not announce their presence by system malfunctions. A cyber attack reveals such vulnerabilities belatedly, and misplaced trust can allow the vulnerabilities to persist, amplifying the damage, as Cynthia E. Irvine (of the Naval Postgraduate School) and J.R. Rao (of IBM Thomas J. Watson Research Center) explained:

> [S]ecurity is a behind-the-scenes service that we don't concern ourselves with until something goes wrong. Most of us probably don't expect our systems to allow criminals to obtain or manipulate our valuable information, nor do we expect catastrophic failures of large-scale systems due to manipulation by adversaries.
>
> A typical developer might think that a system is acceptable if it provides the customer's requested functionality; a wise developer might also ensure that the system isn't a danger to the user's health or safety. The result can be a carefully constructed system that also provides the intended services. But wait! What if the system does its job, but still leaves an entryway so that cyber miscreants can slip in and steal or modify valuable information? What if these miscreants wreak havoc by causing systems to go off kilter? Even if our wise developer could construct the system carefully, many such systems are used in ways that were neither intended nor anticipated—for example, *systems designed for the enterprise but used in multitenant settings such as the cloud*. This scenario highlights the problem of misplaced trust: *the system we trust isn't as trustworthy as we had imagined* and now exhibits some mixture of both expected and unexpected functionality. A disconnect exists between user assumptions regarding what the system was supposed to

> do and what it ended up doing. How did this happen? The answer is that the system does something unexpectedly because it contains unspecified or misused functionality in the form of flaws or, worse, clandestine artifices.
>
> Unspecified functionality is rampant in many of today's systems.[3]

In this article, we take a cold, hard look at the frequency of successful cyber attacks and the consequent transfers of valuable information (often an unlicensed export of export controlled technology and with this a transfer of an enterprise's hard-earned competitive edge). The transfers include source code, intellectual property, and cybersecurity information. These unauthorized transfers are not limited to data stored within an enterprise's computers and servers. Enterprises store such data increasingly in servers of cloud computing service vendors where it can be similarly breached and misappropriated. And, enterprises frequently entrust some of their most sensitive data to their outside counsel who may store it on computers and servers that are no less vulnerable to attack than those of their clients and the clients' cloud storage vendors. For counsel, such unauthorized access to client confidential information may result in damage to clients' interests as well as to the counsel's relationship with affected clients. The rising incidence of cyber attacks and the damage they cause radically redefine the risk evaluations in which counsel routinely engage. And, the misplaced trust in technology and the high costs it imposes should be seen, we believe, as "handwriting on the wall," intimating that our Digital Era's technologies are compromising the enterprise.

Nearly ubiquitous connectivity disperses nearly ubiquitous vulnerability. Users demand connectivity, enterprises attempt to enhance their competitive edge by purchasing the technology without weighing the latent cost of the technological benefits—cyber defenses may become eroded and porous. The Digital Era's technology has allowed for unprecedented concentration of valuable information assets in digital media. Once stored there, however, the data becomes easily transferrable worldwide in seconds: it can be saved to light-weight portable computing devices and easily concealed memory sticks that can be taken outside the enterprise; information can be uploaded to cloud computing

3. Cynthia E. Irvine & J.R. Rao, *Engineering Secure Systems,* IEEE SECURITY & PRIVACY, Jan.–Feb. 2011, at 18.

servers where the vendor may elect to make multiple copies, stored in multiple jurisdictions or where the data may be under the control of other outsource contractors with unverifiable cyber defenses. Multiplicity of copies and their dispersal creates an infinite number of data treasure troves. An adversary need only attack one to infiltrate an enterprise's valuable information. If copies of the enterprise's source code have been secreted on numerous media, the attacker needs only to exploit one of the media in order to misappropriate the complete code.

Enterprises that rely on the benefits of technology must create protocols to reassess the costs of such technology. They must factor the calculable damage to digital assets, and they may well conclude that the costs in misappropriated intellectual property, compromised cyber security, and reputational or enterprise damage dim the luster of the benefits. Given this cost/benefit analysis, future investments in new technology may well prove unjustifiable unless cyber security can be appropriately reinforced and maintained. This is the analysis in which we believe law firm management and their clients' Boards of Directors must engage when asked to approve a technology acquisition strategy.

As destructive cyber attacks increase in frequency and severity (a pattern already in evidence), we believe they will force a sea-change in regulations governing critical infrastructure enterprises, in the creation of new or enhanced legal duties of care, in legal liability, and *in the actions required to be taken by responsible personnel to fulfill professional ethical duties*. The interpretations of such ethical duties are bound to change to reflect the increased risks presented by the technology and by users' failure or inability to mitigate or neutralize those risks. We believe that vulnerabilities to cyber attacks and the profusion and continuous onslaught of such attacks will prompt officers and directors and their counsel to give serious consideration to treating cyber security as material to the financial condition of the enterprise. Cyber attacks could well become material events for disclosure purposes.

Underlying each enterprise's decision to adopt a new communications technology are decisions that have in common three questions:

- *First, can we trust the new technology?* (i.e., what are the worst-case scenarios?);
- *Second, can we trust ourselves to use the new technology advantageously?* (i.e., can our personnel evaluate the benefits, identify the vulnerabilities, and guard against the risks?); and

- *Third, if we deploy the new technology throughout the enterprise, can we trust the enterprise's cyber defenses?* (i.e., will the cyber defenses protect against misappropriation of the enterprise's cyber security designs, plans, and procedures? Will the cyber defenses detect and repel an adversary intent on manipulating our SCADA systems or damaging the enterprise's machinery, networks, and information systems?).

Counsel have an additional question. This is a question that really confronts any licensed professional (e.g., lawyer, physician, accountant, or engineer) whose practice is subject to ethical standards:

- *Fourth, if we adopt the new technology, can we fulfill our ethical duties and protect our client's interests?*

In our haste to gain the benefits of a new technology, there is a strong institutional temptation to implement prior to vetting fully the risk factors. In most cases, to forgo is to forget.

When military operations are planned there is often a carefully prepared advantage/risk ratio adjusted to reflect updates provided by intelligence assessments. Enterprises, including law firms, may find it in their best interests to require carefully prepared advantage/risk ratios when they undertake to decide whether, when, and to what extent to adopt and deploy a new communications technology. Counsel will need to be more proactive in these decisions as cybersecurity becomes part of their professional ethical duties.

We are not advocating raising the ethical standards applicable to counsel. But, bar associations may review ethical standards with the advent of round-the-clock cyber attacks on corporate enterprises.

The effort we undertake in this article is designed to help counsel by improving their understanding of the nature of the risks and by recommending ways that those risks can be mitigated such that counsel can avoid inadvertent mistakes. We offer some guidelines for "best practices" of cybersecurity such that counsel may make these an integral part of the practice of law.

Impregnable cyber defenses may exceed current skills. Restoration of the secure enterprise may not be possible, or only intermittently achievable. Attack skills have advanced so far, but we ought to be able to reverse the trend of decisions that increase an enterprise's vulnerabilities. Stemming that tide should not be mistaken for the folly of trying to oppose the Digital Era's incoming tide. And, what is interesting is that a heightened understanding of

professional ethical duties amidst the waves of cyber attacks may prove to be a valuable skill in that pursuit. As expressed in the old saw, "measure twice, cut once," a concern for professional ethical duties can remind counsel to ensure that the second "measuring" of a technology acquisition decision involves an accurate assessment of what it will do to the enterprise's cybersecurity.

The organization of this article is as follows: Part II discusses the ethical challenges presented by ever-evolving communications technology.[4] Part III reviews what some lawyers believe has come to be an *implicit duty* under the applicable rules to stay abreast of new communications technologies and considers the basis for such an implicit duty under the ethical rules that require counsel to provide competent representation and to protect client confidential information.[5] Part IV provides an extensive analysis of cloud computing and its security risks, discusses some of the ethical risks they may create for lawyers and law firms, and suggests some measures that may help put counsel in a good position to minimize those risks.[6]

We have concentrated on cloud computing for three reasons. First, most if not all of the ethical risks that arise under other Web 2.0 technologies, and particularly social networking technologies, are present in cloud computing. Second, most Web 2.0 technologies rely heavily on cloud computing platforms for their operation. Third, although most Web 2.0 technologies can be understood through "hands-on" use, and such use will also reveal many of the most serious security risks to an observant lawyer, that is decidedly not the case for cloud computing. Cloud computing vendors tend to disclose little of the workings of their platforms, their security precautions, their policies in the event of outages and data breaches, and their procedures for the location, storage, copying, movement, and purging of customer data. Moreover, when security incidents or outages occur that impair or disrupt a vendor's cloud computing services for prolonged periods, the vendor's explanations have tended to arrive after recovery, not during the outages when customers urgently need to know what is happening so that they can implement contingency plans. Also, the explanations have tended to be expressed in impenetrable jargon (notwithstanding considerable detail provided to unpack the jargon), as illustrated in Amazon's explanation of the four-day

4. *See infra* Part II.
5. *See infra* Part III.
6. *See infra* Part IV.

outage of its cloud services in April 2011[7] in terms of a "re-mirroring storm":

> Now that we have fully restored functionality to all affected services, we would like to share more details with our customers about the events that occurred with the Amazon Elastic Compute Cloud ("EC2") last week . . . .
>
> . . . .
>
> **Primary Outage.** At 12:47 AM PDT on April 21st, a network change was performed as part of our normal AWS scaling activities in a single Availability Zone in the US East Region. The configuration change was to upgrade the capacity of the primary network. During the change, one of the standard steps is to shift traffic off of one of the redundant routers in the primary EBS network to allow the upgrade to happen. The traffic shift was executed incorrectly and rather than routing the traffic to the other router on the primary network, the traffic was routed onto the lower capacity redundant EBS network. For a portion of the EBS cluster in the affected Availability Zone, this meant that they did not have a functioning primary or secondary network because traffic was purposely shifted away from the primary network and the secondary network couldn't handle the traffic level it was receiving. As a result, many EBS nodes in the affected Availability Zone were completely isolated from other EBS nodes in its cluster. Unlike a normal network interruption, this change disconnected both the primary and secondary network simultaneously, leaving the affected nodes completely isolated from one another.
>
> When this network connectivity issue occurred, a large number of EBS nodes in a single EBS cluster lost connection to their replicas. When the incorrect traffic shift was rolled back and network connectivity was restored, these nodes rapidly began searching the EBS cluster for available server space where they could re-mirror data. Once again, in a normally functioning cluster, this occurs in milliseconds. In this case, because the issue affected such a large number of volumes concurrently, the free capacity of the EBS cluster was quickly exhausted, leaving many of the nodes "stuck" in a loop, continuously searching the cluster for free space.

7. Maija Palmer, *Security: Internet is Industry Achilles Heel*, FIN. TIMES, June 28, 2011, http://www.ft.com/intl/cms/s/0/19f14406-a118-11e0-9a07-00144feabdc0.html#axzz1bAGTdn5D.

> This quickly led to a "re-mirroring storm," where a large number of volumes were effectively "stuck" while the nodes searched the cluster for the storage space it needed for its new replica. At this point, about 13% of the volumes in the affected Availability Zone were in this "stuck" state.[8]

Probably very few, if any, lawyers knew that the Amazon cloud computing service had such constituent elements as described in that account or were aware of the disarray that could occur among them during routine maintenance. Hands-on use of the cloud would not reveal such facts. Moreover, explanations like Amazon's, albeit well intended, and the withholding of such critical information until after the vendor restores cloud computing services, puts clients and counsel in a poor position to assess risks. The more sensitive and valuable the data to be entrusted to the cloud (and the more that counsel may have ethical obligations concerning the proper care of such data), the greater the probability that a premature decision to move such data to the cloud could result in unintended consequences and inadvertent ethical lapses. These challenges may become more complicated as vendors, seeking to appear to be offering cloud computing, engage in marketing strategies that make unclear the extent to which the customer is, or is not, embarking on a cloud computing exercise if it purchases the vendors' services. Such marketing practices, referred to as "cloud washing," tend to involve placing "cloud" labels on data storage advertisements and in vendor pitches.[9] For these reasons, of all the Web 2.0 technologies, we believe the one that is probably going to have the most far-reaching effects on counsel's presentation of clients, and the one most poorly understood by clients and counsel, is cloud computing, and it, therefore, deserves the greatest attention. Moreover, as noted previously in this introduction, recent developments, and particularly high-profile data security breaches involving the

---

8. Amazon Web Servs. Team, *Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region*, AMAZON WEB SERVICES, http://aws.amazon.com/message/65648 (last visited Oct. 18, 2011).

9. Rachel Kossmann, *Cloud Washing Defined: How to Avoid This Marketing Trend*, SEARCHCLOUDSTORAGE.COM, http://searchcloudstorage.techtarget.com/podcast/Cloud-washing-defined-How-to-avoid-this-marketing-trend (last visited Oct. 18, 2011). For examples of "cloud washing," see Larry Dignan, *Oracle's Exalogic Box: Cloud Washing at Its Best?*, ZDNET (Sept. 20, 2010), http://www.zdnet.com/blog/btl/oracles-exalogic-box-cloud-washing-at-its-best/39343.

cloud,[10] suggest that the risks described in this article are not speculative, trivial, or financially insignificant.[11]

Part V briefly describes new cybersecurity attacks that have changed the landscape of information security.[12] Part VI reviews the National Institute of Standards and Technology's (NIST) revised standards and recommendations that appear in its "DRAFT Cloud Computing Synopsis and Recommendations," Special Publication 800-146,[13] that was published in May 2011. Because NIST highlights certain problematic views of cloud computing, we discuss those and assess the ethical challenges they may pose for lawyers and law firms.[14] Part VII concludes the discussion with a brief review of representative examples of ethical risks that other Web 2.0 technologies may pose for lawyers and law firms.[15]

II. ETHICAL CHALLENGES FROM NEW COMMUNICATIONS TECHNOLOGIES

New technologies often create new and unsuspected technical problems as well as new and unanticipated ethical challenges. Although data leaks undoubtedly occurred at major corporations and financial institutions long before they became the subject of frequent headlines and recurrent boardroom agenda items, few such leaks were publicly reported.[16] This approach, which probably 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

10. *See* Ben Kuchera, *PlayStation Network Hacked, Data Stolen: How Badly Is Sony Hurt?*, ARSTECHNICA (Apr. 26, 2011, 6:37 PM), http://arstechnica.com/gaming/news/2011/04/sonys-black-eye-is-a-pr-problem-not-a-legal-one.ars.

11. For discussion of some of the ethical risks that may arise in the use of other Web 2.0 technologies, see, for example, H. Christopher Boehning & Daniel J. Toal, *The Ethics on Evidence from Social Networking Sites,* 246 N.Y. L.J. 5, 7 (2011) and Margaret M. DiBianca, *Ethical Risks Arising from Lawyers' Use of (and Refusal to Use) Social Media*, 12 DEL. L. REV. 179 (2011).

12. *See infra* Part V.

13. *See* BADGER ET AL., NAT'L INST. OF STANDARDS & TECH., DRAFT CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS (MAY 2011) [hereinafter NIST CLOUD SYNOPSIS], *available at* http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.

14. *See infra* Part VI.

15. *See infra* Part VII.

16. *See* M. Eric Johnson et al., *Security Through Information Risk Management*, IEEE SECURITY & PRIVACY, May–June 2009, at 45, 49.

faster than the safeguards against them, due to the rapid evolution of communications technology. 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 state data breach reporting statutes, beginning in California,[17] forced U.S. enterprises subject to those statutes to disclose the frequency of leakages and the magnitude of data released, lost, or compromised. They also motivated company management to pursue radical strategies for the protection of the most sensitive and valuable data. Nevertheless, data leaks and data breaches continue to occur with significant damage to financial and reputational interests, with the attendant legal and ethical consequences. For perspective on these incidents, consider the findings of a study published in 2011 and conducted by the Verizon RISK Team in cooperation with the U.S. Secret Service and the Dutch High Tech Crime Unit:

> 361 million >> 144 million >> 4 million. Thus goes the tally of total records compromised across the combined caseload of Verizon and the United States Secret Service (USSS) over the last three years . . . .
>
> . . . .
>
> It is fascinating from a research standpoint that the all-time lowest amount of data loss occurred in the same year as the all-time highest amount of incidents investigated . . . . We witnessed highly automated and prolific external attacks, low and slow attacks, intricate internal fraud rings, country-wide device tampering schemes, cunning social engineering plots, and much more . . . .
>
> . . . .
>
> Cloud, Aurora, Mobility, Zeus, APT,[18] Wikileaks, Stuxnet,[19] Anonymous. If a word cloud were created using

17. *See* CAL. CIV. CODE § 1798.82 (West 2009).

18. The acronym APT stands for "advanced persistent threats," which are campaigns to steal intellectual property using cyber-attacks including malware by a human or an organization. Greg Hoglund, Info. Sys. Sec. Assoc., Conference Presentation, Advanced Persistent Threat: What APT Means to Your Enterprise (Feb. 19, 2010), *available at* http://www.issa-sac.org/info_resources/ISSA_20100219_HBGary_Advanced_Persistent_Threat.pdf. For an anatomy of advanced persistent threat campaigns, see *id.*

19. For an account of the Stuxnet worm, the effect it had on Iranian nuclear processing facilities, and the threats that similar malware—using "man-in-the-middle" attacks—pose to the increasingly widespread supervisory control and data acquisition (SCADA) systems, see Roland L. Trope & Geoffrey Schwartz, *Cyber Security for U.S.-Based Nuclear Power Plants*, Continuing Legal Education Program at the ABA Cyberspace Law Committee's Winter Working Meeting (Jan. 2011) (on

> infosec headlines from 2010, these would certainly be rendered big and bold . . . . While the Cloud and mobile devices increasingly allow us to do anything from anywhere with anyone at any time, Aurora, Zeus, Advanced Persistent Threats (APTs), Wikileaks, and Stuxnet remind us of the difficulty of protecting our information assets in a usability-driven world . . . .
>
> . . . .
>
> . . . [W]e constantly see breaches involving hosted systems, outsourced management, rogue vendors, and even VMs[20] (though the attack vectors have nothing to do with it being a VM or not). In other words, it's more about giving up control of our assets and data (and not controlling the associated risk) than any technology specific to the Cloud.[21]

The severity of the advanced persistent threats, particularly those reported based in and launched from China, and the ubiquity of risks created, in part, by the nearly ubiquitous access to treasure troves of companies' digital data assets is attested to in the release in August 2011 of the McAfee report, authored by Dmitri Alperovitch, that observed:

Having investigated intrusions such as Operation Aurora

---

file with the authors).

20. The acronym VM stands for "virtual machine."

21. VERIZON, 2011 DATA BREACH INVESTIGATIONS REPORT 2, 4 (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf. As for the sharp decline in the number of records compromised in 2010, the report offers this explanation:

> The Secret Service has focused attention on numerous "bullet proof hosters," who provide web hosting services that allow their customer's [sic] considerable leniency in the types of materials they may upload and distribute. Seizures in excess of 200TB [terabytes] of data, [sic] belonging to bullet proof hosters, [sic] have made the proliferation of malware more challenging for cybercriminals and provided a substantial number of investigative leads.
>
> With all these factors taken into account, it is not surprising that the number of compromised records significantly decreased during 2010. After any major investigation and arrest, the cybercriminal underground evaluates what happened and evolves from the lessons learned during the prosecution of their peers.
>
> It appears that cybercriminals are currently satisfied with compromising Point of Sale (POS) systems and performing account takeovers and Automated Clearing House (ACH) transaction fraud. There has been an increase in these areas in 2010. *In relation to prior years, it appeared that there were more data breaches in 2010, but the compromised data decreased due to the size of the compromised company's databases.*

Id. at 6 (emphasis added).

and NightDragon (systemic long-term compromise of Western oil and gas industry), as well as numerous others that have not been disclosed publicly, I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact. In fact, I divide the entire set of Fortune Global 2,000 firms into two categories: those that *know they've been compromised* and those that *don't yet know.*

Lately, with the rash of revelations about attacks on organizations such as RSA, Lockheed Martin, Sony, PBS, and others, I have been asked . . . whether the rate of intrusions is increasing and if it is a new phenomenon. I find the question ironic because these types of exploitations have occurred relentlessly for at least a half decade, and the majority of the recent disclosures in the last six months have, in fact, been a result of relatively unsophisticated and opportunistic exploitations for the sake of notoriety by loosely organized political hacktivist groups such as Anonymous and Lulzsec. On the other hand, the targeted compromises we are focused on—known as advanced persistent threats (APTs)—are much more insidious and occur largely without public disclosures. They present a far greater threat to companies and governments, as the adversary is tenaciously persistent in achieving their objectives. The key to these intrusions is that the adversary is motivated by a massive hunger for secrets and intellectual property; this is different from the immediate financial gratification that drives much of cybercrime, another serious but more manageable threat.

What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition (SCADA) configurations, design schematics, and much more has 'fallen off the truck' of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of

dogged adversaries.[22]

From such reports, it is reasonable to infer that the widespread occurrence of data breaches is due in large part to the opportunities created by proliferation of at least four kinds of digital-based technologies:

(1) portable, high density, data devices (e.g., multiple gigabyte memory sticks and portable terabyte storage units);
(2) wireless communications devices providing ubiquitous website access (e.g., smartphones that can surf the web and store reams of downloaded data, e-mails, and attached documents);
(3) wireless data warehouses (e.g., "cloud computing services"—the outsourced storage of data in server farms accessed wirelessly); and
(4) online social media (e.g., Facebook, YouTube, and Twitter) that build upon, expand the use of, and enhance the markets for wireless web-access.

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 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."'[23] Moreover, the changes in the market for stolen data have led data thieves to focus their attacks on larger concentrations of personal identification information.[24] As noted in the earlier 2009 study by the Verizon Business RISK Team:

> The value associated with selling stolen credit card data [has] 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

22. DMITRI ALPEROVITCH, REVEALED: OPERATION SHADY RAT, 2 (McAfee 2011), *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf. "Operation Aurora" is the term given to the infiltration of Google's networks and those of at least twenty other major companies in 2009, by what apparently was a China-based espionage network that specifically targeted certain companies. *See* Robin Wauters, *McAfee Calls Operation Aurora a "Watershed Moment in Cybersecurity," Offers Guidance*, TECHCRUNCH (Jan. 17, 2010), http://techcrunch.com/2010/01/17/mcafee-operation-aurora-2.

23. Johnson et al., *supra* note 16, at 49.

24. WADE H. BAKER ET AL., 2009 DATA BREACH INVESTIGATIONS REPORT 5 (2009), *available at* http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

> 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.[25]

The magnitude of the vulnerability of digital data held by businesses became publicly evident back in a September 2008 Department of Justice report concerning information security incidents experienced by businesses in 2005.[26] The report discloses that "[c]ritical infrastructure businesses detected 13 million [computer security] incidents (nearly two-thirds of the total).[27] High risk industries detected more than 4 million incidents (a fifth of the total)."[28] Moreover, "[n]inety-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.[29] 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.[30] The annual loss of intellectual property and investment opportunities across all industries has reportedly reached "$6 billion to $20 billion, with a big part owing to oil industry losses."[31] The magnitude of the costs to a single company is evident in the consequences to RSA, the security service vendor that provides tokens that companies and governments use to log on remotely to workplace systems: EMC Corp (one of whose divisions is RSA) has disclosed that "it had taken a $66 million charge to cover remediation costs associated with a March [2011] intrusion of its

25. *Id.*

26. RAMONA R. RANTALA, CYBERCRIME AGAINST BUSINESSES, 2005, at 1–9 (2008), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf.

27. *Id.* at 6.

28. *Id.*

29. *Id.* at 4.

30. *See id.* at 2.

31. Ellen Nakashima, *Report on 'Operation Shady RAT' Identifies Widespread Cyber-spying*, WASH. POST (Aug. 2, 2011, 6:00 AM), http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html?wpisrc=nl_tech.

RSA division."[32]

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.[33] As one company executive explained, "[w]e also block our data, and we have established that if date is not labeled, then it is confidential by default."[34] However, the corporate response appears to be failing to keep pace with the cyber-threats to corporate digital assets. As noted in Ernst & Young's thirteenth annual *Global Information Security Survey*, "60% of respondents perceived an increase in the level of risk they face due to the use of social networking, cloud computing and personal devices in the enterprise."[35] However, despite that awareness, the report noted a paradoxical lack of enterprise interest in the emerging risks:

> The fact that only 10% of respondents indicated the examination of new and emerging IT trends as a critically important function is further evidence that few organizations have assessed the impact of social networking . . . . As the use of social networking and Web 2.0 sites continues to increase and become a part of the standard work environment, the behaviors related to sharing personal information are often being transferred to sensitive business information, where they are not appropriate. If no action is taken, this will likely lead to an increase in the disclosure of business information or protected privacy-related data, either intentionally or accidentally through the use of social media.[36]

The reported data leaks and other technological incidents at

---

32. *Id.*

33. Gregg Keizer, *Hacker Break-in of Twitter E-mail Yields Secret Docs*, COMPUTERWORLD (July 16, 2009, 1:16 PM), 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. *Id.* It may be that the hacker breached the password reset at both Yahoo!'s and Google's web-based applications.

34. Johnson et al., *supra* note 16, at 49.

35. ERNST & YOUNG, BORDERLESS SECURITY: ERNST & YOUNG'S 2010 GLOBAL INFORMATION SECURITY SURVEY 2 (2010), *available at* http://www.ey.com/Publication/vwLUAssets/Global_information_security_survey_2010_advisory/$LLE/GISS%20report_final.pdf.

36. *Id.* at 12–13.

major corporate, governmental, and financial enterprises contrast sharply with the paucity of reports of such problems at law firms.[37] 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 their clients. When such technical problems do occur, as 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.[38]

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 . . . malware infections [increasingly require] no intervention or awareness on the part of the user. To give some idea of the threat posed, a Scansafe report analyzing malware trends reported that risks from compromised websites increased 407% in the year to May 2008."[39]

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 authorisation is a barrier to the use of such applications and a serious risk for those who do.[40]

Apparently, an attacker was able to use similar information to

37. *But see* Josh Halliday, *Law Firm Could Face £500,000 Fine Over Data Breach*, THE GUARDIAN (Sep. 28, 2010, 11:04 EDT), http://www.guardian.co.uk/media/2010/sep/28/filesharing-acs-law.

38. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007) (describing ethical violations that may result from technological problems).

39. EUR. NETWORK & INFO. SEC. AGENCY, WEB 2.0 SECURITY AND PRIVACY 2 (2008), *available at* http://www.ifap.ru/library/book392.pdf.

40. *Id.* at 3.

gain access to multiple web-based applications in a May 2009 incident that Twitter acknowledged.[41] 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 e-mail account.[42] 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."[43]

Twitter reported that the breach did not involve any flaw in web applications, but instead was due to a failure to follow good personal security guidelines, such as selection of a strong password.[44] 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 Web 2.0 accounts.[45] Because 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

41. Biz Stone, *Even More Open than We Wanted*, TWITTER BLOG (July 15, 2009, 11:15 AM), http://blog.twitter.com/2009_07_01_archive.html.

42. Josh Lowensohn & Caroline McCarthy, *Lessons from Twitter's Security Breach*, CNET (July 15, 2009, 12:45 PM), http://news.cnet.com/8301-17939_109-10287558-2.html.

43. Stone, *supra* note 41.

44. For example, in April 2011, Amazon's cloud computing "Web Services" experienced a prolonged outage with significant consequences to companies that depended on it:

> Cloud computing is learning the harsh reality of resiliency as Amazon Web Services' outage has crossed its second day. Meanwhile, startups and a host of other AWS customers are in uncharted waters. On Wednesday, the common belief was that startups could build their infrastructure on AWS completely. Set the servers up and forget them . . . . Given that AWS' North Virginia data center has been out of whack for more than 24 hours, it's clear you need to procure more than one cloud. You need a backup for your cloud provider's backup.

Larry Dignan, *Amazon's Web Services Outage: End of Cloud Innocence?*, ZDNET (Apr. 22, 2011, 7:27 AM), http://www.zdnet.com/blog/btl/amazons-web-services-outage-end-of-cloud-innocence/47731.

45. The hacker gained access to the employee's Yahoo! Mail as a means to accessing Twitter's Google Apps. *See* Lowensohn & McCarthy, *supra* note 42.

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 [in 2008], 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.[46]

The attacker stole several hundred Twitter internal documents and then forwarded them to websites, 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.[47] Twitter's co-founder, Biz Stone, recognized the significance of this, stating, "as they were never meant for public communication, publishing these documents publicly could jeopardize relationships with Twitter's ongoing and potential partners."[48]

More recent data security breaches[49] and outages at cloud providers[50] demonstrate the types and magnitude of risks that may

---

46. Gregg Keizer, *Hacker Break-in of Twitter E-mail Yields Secret Docs*, COMPUTERWORLD (July 16, 2009, 1:16 PM), http://www.computerworld.com/s/article/9135591/Hacker_break_in_of_Twitter_e_mail_yields_secret_docs.

47. Devin Coldewey, *Twitter's Financial Forecast Shows First Revenue in Q3, 1 Billion Users in 2013*, TECHCRUNCH (July 15, 2009), http://techcrunch.com/2009/07/15/twitters-financial-forecast-shows-first-revenue-in-q3-1-billion-users-in-2013.

48. Biz Stone, *supra* note 41.

49. As reported in August 2011:

> A widespread cyber-espionage operation has penetrated 72 government and other organizations, most in the US, copying everything from military secrets to industrial designs. Analysts said circumstantial evidence pointed to China as the most likely suspect . . . . News of the newly discovered effort will put additional pressure on Washington policymakers grappling with the challenge posed by such espionage.

Joseph Menn, *Cyberattacks Penetrate Military Secrets and Designs*, FIN. TIMES, Aug. 3, 2011, http://www.ft.com/cms/s/0/d4f09016-bda3-11e0-babc-00144feabdc0.html#axzz1YFednwOg.

50. Examples of 2011 cloud service, or cloud based product, outages at major vendors include Sony, Microsoft, and Amazon:

> In April, technology giant Sony (www.sony.com) faced an outage to its Playstation Network that compromised approximately 100 million users private information. Now, nearly a month later, the system is still down and many experts are suggesting that this outage could have a much larger impact on the way people perceive the security of the cloud.
>
> . . . .
>
> According to a report by Arik Hesseldahl on CNET, Sony first became aware of the attack on April 19 after it discovered "several

be present in cloud computing environments and online social networking systems such as Twitter. Although the White House, in May 2011, proposed an *International Strategy for Cyberspace*,[51] its implementation and effectiveness remain unclear and may be hampered by budgetary constraints, which suggest that clients and

---

> PlayStation Network servers had rebooted themselves unexpectedly. Four servers were immediately taken offline in order to figure out what was going on. By the next day, it was clear that another six had been attacked, and they were taken offline as well.

Nicole Henderson, *Noise Filter: Sony PlayStation Network Outage Raises Cloud Security Concerns*, THE WHIR (May 11, 2011), http://www.thewhir.com/web-hosting-news/051111_Noise_Filter_Sony_PlayStation_Network_Outage_Raises_Cloud_Security_Concerns.

> Microsoft has served up another apology for the unreliability of its cloud after burning converts to its BPOS collaboration service by killing their email.
>
> . . . .
>
> Customers on BPOS in the US and worldwide were kicked off their hosted Exchange email systems, being unable to read, write, or access their messages. All users were affected—from down in the cubicle farm all the way up to the CEO's corner office. The outages started Tuesday and came after weeks of the service slowly degrading.

Gavin Clarke, *Microsoft BPOS Cloud Outage Burns Exchange Converts*, CHANNEL REGISTER (May 13, 2011, 23:45 GMT), http://www.channelregister.co.uk/2011/05/13/microsoft_bpos_apology.

> Amazon's cloud crashed, taking sites like Reddit, Foursquare, Quora, Hootsuite, Indaba, GroupMe, Scvngr, Motherboard.tv and a few more down with it. As reported several components of Amazon Cloud portfolio like, EC2, Elastic Block Store (EBS), Relational Database Service (RDS), Elastic Beanstalk, CloudFormation and lately MapReduce were all impacted.
>
> . . . .
>
> . . . [T]his has created a huge impact on the Cloud Adoption for the large enterprises.

Srinivasan Sundara Rajan, *Lessons from the Amazon Cloud Outage*, CLOUD COMPUTING J. (Apr. 27, 2011, 12:00 PM EDT), http://cloudcomputing.sys-con.com/node/1805849.

51. THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. If a reader of the Strategy looks in it for some enforcement or protection mechanisms it probably rests in the asserted right of self-defense in cyberspace as in territorial defense: "Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace." *Id.* at 10. However, in light of the reported incidents that appear to have originated outside of the countries attacked, it is increasingly unclear what threshold countries will eventually settle upon as constituting an attack that warrants a self-defense response or that might justify preemptive action in self-defense. For further discussion of these issues, see David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*, IEEE SEC. & PRIVACY, July–Aug. 2011, at 56.

their legal counsel cannot wait for such measures to safeguard their digital assets from cyber-threats. Nor will such measures address the ethical challenges that will probably accompany the adoption of new communications technologies and the vulnerabilities that such technologies bring with them in their design and in ways that users manage them. To the extent that data security incidents, and the occasional enforcement[52] or private action related to them, continue, they provide additional information on the nature of risks that lawyers and law firms should be prepared to manage. These are serious and complex ethical issues. Considering such issues before the problem arises will help those affected formulate better responses when problems do arise, as well as help to position firms to present credible defenses to claims that they violated the applicable rules of professional responsibility.

The Ethics Essays,[53] focused on the New York Rules of Professional Conduct (NYRPC), which became effective on April 1, 2009.[54] This article retains the original presentation of the NYRPC and expands the analysis to include the American Bar Association's Model Rules of Professional Conduct (MRPC). It also evaluates selected opinions by state and local bar associations and decisions by courts under both the NYRPC and MRPC.

The Ethics Essays anticipated the conclusions that bar associations and courts have reached when asked to set forth policies involving use of Web 2.0 and cloud computing. This article reaches beyond the opinions and decisions of bar and bench to probe the scope of lawyers' and law firms' ethical obligations to their clients that may arise as new communications technologies continue to evolve. New technologies will probably require adjustments by lawyers and law firms in order to ensure that they

52. *See* Twitter, Inc., Docket No. C-4316 (F.T.C. Mar. 2. 2011), *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf (deciding and ordering settling charges against Twitter, Inc. and ordering the corporation, among other things, not to misrepresent the "extent to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, including . . . misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users").

53. The Ethics Essays are Roland Trope & Claudia Ray, *The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms, and Judges,* Essay for CLE Program, ABA Annual Meeting, San Francisco, August 2010 and Roland Trope & Claudia Ray, *Head in the "Cloud"–Feet on the Ground: Understanding the Ethical Challenges of Web 2.0for Lawyers, Law Firms and Judges* (2010), each of which is on file with the authors.

54. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200 (2011).

continue to be in good positions to make the common sense applications of the profession's ethical precepts to the risks created by the availability of new technologies and the choices in conduct such technologies present. It is our belief that the development and adoption of new communications technologies will seldom require significant changes to the long-standing professional ethical rules, however surprising, rapid, and disruptive the technologies prove to be upon their emergence. When properly understood, each new communications technology will be seen to have advantages and drawbacks, competitive benefits and unanticipated risks, and to the extent that those are not fully explored, assessed, and appreciated early, they may put lawyers and law firms that use them in positions where inadvertent ethical lapses can occur. The lessons we try to draw during the course of this discussion are intended to apply to any new communications technology, not merely those under review at the time of this writing. For that reason, this article will include discussion relevant to three representative aspects of the most serious ethical risks that lawyers and law firms may face when using Web 2.0 technologies: those that may arise (1) in performing client-related work; (2) in pursuing new clients; and (3) in the course of leisure activities. Having identified what we believe to be the salient ethical risks, we will suggest precautions that lawyers and law firms might consider in order to put themselves in a good position to diminish, if not avert, such risks.

In considering these issues, we assume that readers understand that ethical issues are inherently fact dependent. To date, there are few bar opinions or court decisions to guide this analysis. At best, one can try to infer how a future disciplinary body might decide these issues. We believe, however, that the greatest risks from Web 2.0 technologies are likely to arise from inadvertent actions or oversights that result from a lack of understanding of the operations and use of these technologies, as well as an underestimation of lawyers' and law firms' obligations under applicable rules of professional conduct, such as the NYRPC and the MRPC.[55] For example, a firm might not understand that it may

55. The essays from which this article grew contained a discussion of the kinds of risks that judges and members of their chambers might face in using Web 2.0 technologies and of the risks to lawyers and law firms from engaging in the use of Web 2.0 technologies to make surreptitious recordings. *See* sources cited *supra* note 53. Those issues are no less important than the issues on which we concentrate in this article, but we have opted to defer discussion of that material

arguably have 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.[56] 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, confidential client information and ethical obligation to protect such information.

III. IMPLICIT DUTY UNDER THE NYRPC TO STAY ABREAST OF NEW COMMUNICATIONS TECHNOLOGIES AND COMPARISON OF DUTIES IMPOSED BY THE MRPC

Although neither the NYRPC nor the MRPC expressly require counsel to stay abreast of the latest advances in communications technologies, several of their provisions appear to imply a duty to monitor such developments and understand the potential benefits and risks of new communications technologies. The basis for this implicit duty is derived from two explicit duties: (1) the duty to provide "competent representation" in NYRPC Rule 1.1; and (2) the duties to protect clients' confidential information in NYRPC Rule 1.6, including protection of the attorney-client privilege, prevention of client embarrassment or detrimental disclosure of information, and protection of information deemed confidential by the client.

The next part of this article focuses on the origins and applications of the implicit duty to stay abreast of new communications technologies.

A. The Duty to Provide "Competent Representation" Implies a Duty to Stay Abreast of New Communications Technologies

Rule 1.1 of both the NYRPC and the MRPC obligate lawyers to "provide competent representation to a client."[57] This arguably requires lawyers and law firms to make reasonable efforts to

---

to a later article.

56. *See* Richard Waters, *Cloud Control*, FIN. TIMES, Mar. 25, 2009, http://www.ft.com/intl/cms/s/0/c9e3bf12-1973-11de-9d34-0000779fd2ac.html#axzz1YcY9x6gn [hereinafter *Cloud Control*].

57. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.1 (2011); MODEL RULES OF PROF'L CONDUCT R. 1.1 (2007).

recognize the risks inherent in a new communications technology and to advise the client accordingly. For example, suppose counsel has been engaged to advise on compliance with U.S. "dual use" export controls under the Export Administration Act (EAR)[58] or with U.S. military export controls under the International Traffic in Arms Regulations (ITAR).[59] "Competent representation" in that case would require a clear understanding of the ways in which digital transmissions can result in unlicensed, and thus illegal, releases of EAR-controlled or ITAR-controlled data.[60] Such risks have substantially increased with each new communications technology, including the advent of Web 2.0 technologies.

The advent of e-mail increased risks of non-compliance with ITAR and EAR, because such transmissions could cause an extraordinary amount of ITAR-controlled or EAR-controlled data to be exported overseas in an instant or to be a "deemed export" to a foreign national within the United States. Similarly, the ease with which videos can be discretely or covertly made and uploaded to a Web 2.0 host such as YouTube now makes it possible for unlicensed, unauthorized exports of a much broader range of technical knowhow. A lawyer cannot meet the requirements of MRPC Rule 1.1 in this context if he or she fails to become aware of the emergence of new communications technologies and the changes that they make in the capabilities to communicate—and transfer—sensitive information in violation of applicable laws and regulations.

Even if a lawyer does not have extensive knowledge of communications technology, the comments to the MRPC appear to contemplate that a lawyer can accept representation where the requisite level of competence can be achieved by preparation and study.[61] As with legal issues, if a lawyer could either educate herself on the risks, or associate herself with individuals who have a greater understanding of the risks posed by new technologies, she will be in a stronger position to fulfill the competence requirement. The Initial Draft Proposals—Technology and Confidentiality composed by the ABA Commission on Ethics 20/20 (ABA Commission's Draft Proposals)—supports this position. The ABA Commission's Draft

58. 50 U.S.C. §§ 2401–20 (2006).

59. International Traffic in Arms Regulations, 22 C.F.R. §§ 120–129.10 (2010).

60. *See* Roland L. Trope, *Immaterial Transfers with Material Consequences*, IEEE SECURITY & PRIVACY, Sept.–Oct. 2006, at 74.

61. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 1 (2007).

Proposals concluded that a competent lawyer should be aware of the benefits and risks of new technology and accordingly recommended the following change to Comment 6 of MRPC Rule 1.1:

> **Maintaining Competence.** [6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[62]

Although, at the time of this writing, the ABA has not voted on the measure, the ABA Commission's Draft Proposals reflect the Commission's carefully considered view that to maintain competence in representation of clients a lawyer should be aware of the potential need to keep abreast of new technologies. Moreover, the proposals appear to recommend that the standard for keeping abreast in such circumstances involve, at a minimum, understanding the technologies' benefits and risks, both to the client and to the lawyer.

Whether or not the proposals are adopted in the form proposed, they contain prudent guidance. Consider, for example, that a court issues an order of protection prohibiting a client from contacting a particular person. It would be prudent for counsel to advise the client that such a court order may well extend to and prohibit even indirect communications via online social networks. Doing less might, in some circumstances, evince a failure to provide competent representation. If counsel is unfamiliar with the use of such networks to communicate, he or she might overlook or underestimate the ease with which the client could contact the party named in the court order, thus violating the order.[63] Whether keeping abreast of new communications technologies is ultimately an ethical duty, express or implicit, the fact remains that the competence of a lawyer's representation will be enhanced by making the often considerable effort it takes to keep abreast of such new technologies. Notice that in the following

62. ABA Comm'n on Ethics 20/20, Initial Draft Proposals—Tech. and Confidentiality 5 (2011), *available at* http://www.abanow.org/wordpress/wp-content/files_flutter/1304367997ethics2020_technologyproposals050211.pdf.

63. *See* People v. Fernino, 851 N.Y.S.2d 339, 341 (N.Y. Crim. Ct. 2008) (holding that defendant violated orders of protection mandating "NO CONTACT" by sending a "friend request" message through the MySpace.com Friend Request Manager system).

commentary on the subject the ethical question may be open to debate, but common sense nonetheless leads one to the conclusion that keeping abreast of new communications technologies will probably improve counsel's ability to represent the client:

> Given the increasing use of social networking sites, does the duty of competent representation require that lawyers obtain a basic understanding of navigating social networking sites, and keep informed of rulings on the discoverability and admissibility of evidence obtained from these sites?
>
> In at least some instances, standard practice among practitioners of a particular legal discipline may dictate the minimum amount of familiarity with social networking sites that lawyers within that discipline should have.
>
> The American Academy of Matrimonial Lawyers, for instance, "reports that 66 percent of divorce attorneys use Facebook as their primary source of online evidence." It would seem, therefore, that divorce attorneys lacking familiarity with social networking sites would be hampered in their ability to provide competent representation, particularly when their adversaries are likely availing themselves of all available online content.[64]

The need to learn new or upgraded communications technologies will probably become a priority for many practitioners due to the enactment of statutes or promulgation of regulations that mandate adoption of technology-based capabilities. Federal examples include the Federal Trade Commission's promulgation of the Red Flags Rule Regulations and Guidelines[65] pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003 (under which "financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs—or 'red flags'—of identity theft").[66] Counsel to financial institutions and other entities to which the Red Flags rules apply would find it difficult to advise on compliance with such regulations without continuously updating their knowledge and

64. Boehning & Toal, *supra* note 11, at 7.

65. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718, 63,718–75 (Nov. 9, 2007) (to be codified at 12 C.F.R pts. 41, 222, 334, 364, 571, 717, and 16 C.F.R pt. 681), *available at* http://ftc.gov/os/fedreg/2007/November/071109redflags.pdf.

66. Red Flag Program Clarification Act of 2010, Pub. L. No. 111–319, 124 Stat. 3457 (excluding lawyers and law firms from the scope of the Red Flags regulations).

understanding of the latest techniques used in identity theft and of the indicia that must be detected early in order to protect against such digitally based theft.[67] Another example is the enactment of the Digital Millennium Copyright Act (DMCA), with its provisions prohibiting circumvention of technological measures that control access to copyrighted works, and the U.S. Copyright Office's successive rulemaking proceedings (mandated by the DMCA) in 2000, 2003, 2006, and 2009.[68] Copyright and copyright litigation counsel cannot fully appreciate the Copyright Office's rules changes without being up to date on the technologies addressed by the rulemaking proceedings.

At the state level, examples include the continuing enactment of certain state data breach reporting statutes,[69] some of which include requirements for various degrees of data encryption.[70] Counselors who advise on such matters would find it prudent to ensure that they have expertise on the mechanics of encryption, as well as the problems it can solve or may create, in order to advise clients competently on the application of such statutes.[71] The capabilities of new communications technologies may not be fully disclosed to users. Counsel advising clients in such circumstances probably cannot do so competently under the applicable ethics rules without ensuring that they are fully briefed on the technology and have worked with it sufficiently to appreciate its usefulness and risks.

Risks from specific kinds of software, particularly anti-piracy programs, help explain why this "keep abreast" philosophy may

---

67. Peter McLaughlin, Remarks at the United States Federal Trade Commission Conference on Securing Personal Data in the Global Economy 19–21 (Mar. 16, 2009) *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/031609_sess2.pdf.

68. *See* 17 U.S.C. § 1201(a)(1) (2006). Discussions about exemptions for copy-protection circumvention took place in 2010. *See generally* Memorandum from Marybeth Peters, Register of Copyrights, United States Copyright Office, to James H. Billington, Librarian of Congress, Library of Congress, Recommendation of the Register of Copyrights in RM 2008-8; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Prot. Sys. for Access Control Techs. (Jun. 11, 2010), *available at* http://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf.

69. As of September 2011, new security breach legislation had been introduced in fourteen states. For a complete list, see *Security Breach Legislation 2011*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 12, 2011), http://www.ncsl.org/default.aspx?tabid=22295.

70. *E.g.*, S.B. 267, 2011 Leg., 79th Reg. Sess. (Nev. 2011); MINN. STAT. § 62J.321 subdiv. (b) (2010).

71. McLaughlin, *supra* note 67, at 17.

have an under-appreciated importance. For example, counsel to software companies that experimented with creating "back doors" and "time bombs" in their products to enforce their rights to royalties[72] may not have known of the existence of such devices until a crisis arose from their use. One can imagine the challenges faced by counsel to Amazon and the owners of the copyrights to George Orwell's *1984* and *Animal Farm* as they dealt with the problems caused by buyers' complaints to Amazon that copies of those works sold by Amazon to its Kindle customers were removed without the customers' permission.[73] Amazon's customers apparently were unaware that Amazon had the technological capability to issue an electronic command that could wirelessly communicate with every Kindle (within the wireless range) and cause selected works to be completely erased. Amazon's customers were surprised (and reportedly outraged) when Amazon did just that after learning that it had inadvertently sold unauthorized copies of Orwell's works:

> An Amazon spokesman, Drew Herdener, said in an e-mail message that the books [*1984* and *Animal Farm*] were added to the Kindle store by a company that did not have rights to them, using a self-service function. "When we were notified of this by the rights holder, we removed the illegal copies from our systems and from customers' devices, and refunded customers," he said.[74]

Customers who had made notes on or annotated their Kindle copies of the books lost those materials as well, despite the assurance in Amazon's terms of service that states that the customer is granted a right to keep a "permanent copy of the applicable digital content."[75] Copyright counsel advising in such circumstances would probably need to understand not only the technology, but also the potentially unforeseen results of remotely

72. In fact, a federal court in New Jersey has ruled that allegations of "time-bombs" in software were sufficient to overcome a motion to dismiss claims under the Computer Fraud and Abuse Act. Kalow & Springnut, LLP v. Commence Corp., No. 07-3442 (FLW), 2009 WL 44748, at *3 (D.N.J. Jan. 6, 2009). More benign time-bombs are typically found on trial or "shareware" software. Alexia Gaudeul, *Software Marketing on the Internet: the Use of Samples and Repositories* 2 (Dep't of Econ. and ESRC Centre for Competition Policy Univ. of East Anglia, CCP Working Paper No. 08–23, 2008), *available at* http://www.uea.ac.uk /polopoly_fs/1.104681!ccp08-23.pdf.

73. Brad Stone, *Amazon Erases Two Classics from Kindle (One Is "1984")*, N.Y. TIMES, July 18, 2009, at B1.

74. *Id.*

75. *Id.* at B5.

erasing infringing content along with a customer's own additional or even copyrighted material.

The significance of the undisclosed remote erasure capability goes far beyond the Kindle episode; it demonstrates the capability of wireless service providers to create electronic links that not only give a customer access to data, but also can be used (and potentially misused) to change, corrupt, or erase the customer's data even on a device the customer believes is within the customer's exclusive control. As companies and law firms come increasingly to rely on wireless devices and on third-party providers of remote and wirelessly accessible "cloud" data storage, the need for counsel to keep abreast of new security risks will continue to grow.

One of the most broad-ranging examples of a law making it necessary for counsel to improve their knowledge and use of communications technology is the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which requires the digitalization of health records.[76] Under the HITECH Act, the Secretary of Health and Human Services (Secretary) must "issue guidance on the most effective and appropriate technical safeguards for use in carrying out" certain sections of the Act, including certain security standards.[77] The Act further requires the Secretary to update "guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals" on an annual basis.[78] The HITECH Act also imposes on vendors of personal health records a duty to report the "discovery of a breach of security of *unsecured* PHR[79] [personal health record] identifiable

76. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 2009 U.S.C.C.A.N. (226 Stat.) 123 (2009).

77. *Id.* § 13401(c).

78. *Id.* § 13401(h)(2).

79. The HITECH Act defines a "personal health record" as "an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." *Id.* § 13400(11). In addition, section 13407(f)(2) defines "PHR identifiable health information" as:

> [I]ndividually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6), and includes, with respect to an individual, information—(A) that is provided by or on behalf of the individual; and (B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Id. § 13407(f)(2).

Moreover, the term "unsecured PHR health information" is defined in section

health information that is in a personal health record maintained or offered by such vendor . . . ."[80] The security breach notice must be sent to each U.S. citizen or resident whose "unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security" and to the Federal Trade Commission (FTC).[81]

Dispatch of such security breach notices under the HITECH Act can involve a substantial cost,[82] and notice to the FTC may trigger an investigation resulting in a settlement agreement with additional costly compliance burdens.[83] Vendors seeking to avoid such consequences might retain counsel to reduce the probability of a security breach of *unsecured* PHR identifiable health information, which the Act defines in terms of failure to adhere to the Secretary's annual guidance: "'[U]nsecured PHR identifiable health information' means PHR identifiable health information that is *not protected through the use of a technology or methodology specified by the Secretary in the [annual]* guidance issued under section 13402(h)(2)."[84] Thus, counsel advising the affected vendors appear to have an implied duty to keep abreast of the technologies and methodologies that keep such electronic records "unusable, unreadable, or indecipherable to unauthorized individuals," and in

---

13407(f)(3) as:

> (A) IN GENERAL.—Subject to subparagraph (B), the term "unsecured PHR identifiable health information" means PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2). (B) EXCEPTION IN CASE TIMELY GUIDANCE NOT ISSUED.—In the case that the Secretary does not issue guidance under section 13402(h)(2) by the date specified in such section, for the purposes of this section, the term "unsecured PHR identifiable health information" shall mean PHR identifiable health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

Id. § 13407(f)(3).

80. *Id.* § 13407(a) (emphasis added).

81. *Id.* § 13407(a)(1)–(2).

82. A Colorado hospital spent more than $3 million on notifications alone after a physical security breach. Jaikumar Vijayan, *Insurer Says It's Not Liable for University of Utah's $3.3M Data Breach*, COMPUTERWORLD (June 4, 2010, 8:12 PM), http://www.computerworld.com/s/article/9177702/Insurer_says_it_s_not_liable_for_University_of_Utah_s_3.3M_data_breach?taxonomyId=144.

83. *See* Genica Corp., F.T.C. File No. 082 3113 (2008) (Agreement Containing Consent Order).

84. HITECH Act § 13407(f)(3)(a) (emphasis added).

particular, to those to be identified annually by the Secretary.

Depending on the nature and complexity of the applicable laws, the level of understanding that lawyers and law firms need to achieve may be significant. For example, as of 2004, merely knowing how to use e-mail was probably not sufficient for trial counsel to fulfill their duties to monitor and oversee a client's obligations to preserve electronic records in anticipation of litigation, as it might not have alerted a lawyer or firm to the fact that deletion of an e-mail does not necessarily purge it from a hard drive (where it may remain recoverable). Nor would it necessarily be apparent that daily, automatic backups of a company's e-mails might overwrite and render irrecoverable certain electronic records that the company had a duty to preserve. The minimum depth of understanding that counsel practicing in the Southern District of New York need to have of such digital communications technology was made clear in Judge Scheindlin's *Zubalake* decisions,[85] and particularly in *Zubalake V*, where Judge Scheindlin provided this instruction to counsel for a party obligated to preserve electronic records:

> Once a "litigation hold" is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed "on hold," to the extent required in *Zubulake IV*. To do this, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy.[86]

Web 2.0 technologies have almost certainly expanded the scope of potentially accessible and discoverable electronic records beyond e-mail to include text messaging, Facebook postings, Twitter broadcasts (tweets), videos uploaded to social network websites, and cloud data storage.[87] Litigants and courts may be

85. Zubulake v. UBS Warburg LLC (*Zublake V*), 229 F.R.D. 442 (S.D.N.Y. 2004); Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

86. *Zubulake V*, 229 F.R.D. at 432 (footnotes omitted).

87. As some commentators have observed, New York Rules of Professional Conduct Rule 1.3, which requires that lawyers "act with reasonable diligence and promptness in representing a client," may obligate counsel to make enhanced use

drawn into controversies over the discoverability of records generated by such technologies and stored in multiple locations, whether they persist in mobile devices in possession of the sender and the recipient (as in tweets and video stored on mobile phones or display devices such as an iPod Touch), have been preserved in company backups (if the transmission or reception became recorded on company media) or have been stored on third-party servers (as appears to be the current practice for tweets, Facebook postings and geotagging features of social networking sites such as foursquare),[88] or in other cloud storage environments. The litigation value of such "works" and the risks resulting from creating and "sharing" them, if overlooked by litigation counsel, may expose such counsel to serious risks of failing to fulfill the ethical duty to provide clients with "competent representation" and diligent representation.

To understand and appreciate the litigation value and risks, counsel are likely to decide to do more than read newspaper or blog accounts about the use and misuse of such technologies. There is no substitute for understanding gained from hands-on experience. Moreover, repeated use of a new technology can reveal to the user unreported utilities and undisclosed capacity to create vulnerabilities. It is worth remembering that "the most far-reaching effects of new technology are normally ones that were not

---

of new technologies:

> Presumably this rule [NYRPC 1.3] would require lawyers to search the internet not only for information favorable to his or her client's case, but also for information detrimental to the client for the sake of being better prepared to advocate on the client's behalf. Not knowing that a client routinely posts information on social networking sites, and not knowing how to navigate such sites for information, could compromise a lawyer's ability to identify where relevant information is located, and may thus hamper a lawyer's effective and diligent representation.

Boehning & Toal, *supra* note 11, at 7.

88. *See, e.g.*, Leanne Italie, *Divorce Lawyers: Facebook Tops in Online Evidence*, WPTV.COM (June 29, 2010), http://www.wptv.com/dpp/news/local_news/water_cooler/divorce-lawyers%3A-facebook-tops-in-online-evidence-1277832262612 ("Oversharing on social networks has led to an overabundance of evidence in divorce case."); Belinda Luscombe, *Facebook and Divorce: Airing the Dirty Laundry*, TIME, June 22, 2009, *available at* http://www.time.com/time/magazine/article/0,9171,1904147,00.html (describing how online social networking sites provide lawyers an "evidentiary gold mine"); Molly McDonough, *Facebook Is 'Unrivaled Leader' for Online Divorce Evidence, Survey Says*, ABA JOURNAL (Feb. 12, 2010), *available at* http://www.abajournal.com/news/article/facebook_is_unrivaled_leader_for_online_divorce_evidence_survey_says/ (noting how clients should nix Facebook accounts during divorce proceedings due to heightened levels of personal scrutiny).

anticipated."[89]

Although the risks and benefits might be most apparent in the litigation context, such knowledge can also benefit counsel in other contexts. Incautious creation of electronic records and use of technologies that facilitate their generation, dissemination, and preservation cannot be avoided by actions of litigation counsel. Thus, it is important for non-litigation counsel to understand the new communications technologies and the customs and practices that can cause indiscreet or recklessly foolish transmittals, whether in e-mails, instant messages (IMs), tweets, or geotagging. Once released, such electronic records may be lost to the sender's company, but may have been preserved at the recipient's company, giving the recipient's company a litigation advantage that may not be suspected by the sender's company until it is used for impeachment in a cross-examination.

Since the original essay and CLE were prepared, the authors believe that many litigation counsel have continuously updated their knowledge and understanding of the limitations to, and potential fallacies in, the use of computer forensics on which so much of electronic discovery depends. Just because electronic records exist on a company employee's computer, the company's servers, or a third-party provider of off-site electronic storage—a cloud or otherwise—does not necessarily mean that the employee or the company allowed it to be there or knew of its existence. It may be incorrect and misleading for counsel to assume that the owner of an electronic device intentionally placed digital data on it, allowed the data to be stored there, or was aware of its existence and presence. As a computer security expert observed:

> [T]he data in "our" computers and other devices that overzealous adversaries and prosecutors present as evidence to courts as being "obviously" ours often isn't. Just because we paid the bill for a home computer doesn't mean that we placed an invisible force-field around it to shield it from hackers and others who . . . could add, remove, or alter any and all data in that computer without our knowledge.
>
> . . . .
>
> Classical computer forensics creates the illusion of an airtight investigatory process by diverting attention away from the crucial fact that forensics can't determine who put the data on a device, and focusing instead on the

89. *Cloud Control*, *supra* note 56.

> mechanics of the forensic ritual: investigators create an exact copy of data found on a digital device and present it to a decision authority (court, employer, and so on) without any ability to address the key question of who put the data in that device . . . .
>
> . . . Files can and do end up on our computers in myriad ways without our knowledge, let alone our consent.[90]

Several of the ways for data to become lodged in a hard drive, such as by remote hacking, Wi-Fi hacking, war driving, malicious e-mail attachments, and "web bugs"[91] are familiar to many lawyers, but nonetheless could be overlooked during the pressures and exigencies of discovery. Other vulnerabilities that may be less familiar to lawyers include the electromagnetic "compromising emanations," "Tempest radiation," or "Van Eck radiation" that tend to be broadcast by desktops, laptops, display monitors, and cables (functioning as parasitic antenna) and that can be intercepted and reconstructed by electronic eavesdroppers.[92] When a computing device is located on a high-elevation floor, its emanations become all the easier to intercept because the signal has minimum attention on its way to an interceptor's device.[93]

An ethical issue could arise if a law firm or its lawyers failed to take reasonable precautions to shield their computers and other devices from such emanations and client confidential information is subsequently intercepted. Ethical issues might also arise if a law firm or lawyer outsourced the storage of client data to a third party off-site provider and did not make a "due diligence" inquiry to determine if the provider had failed to implement reasonable precautions against such interception of client confidential

---

90. Michael A. Caloyannides, *Forensics is so "Yesterday,"* IEEE SECURITY & PRIVACY, Mar.–Apr. 2009, at 18, 19.

91. A "web bug" is a concealed HTML code that can cause a computing device connected to the Internet to connect to a particular website each time the user opens the document containing the bug or copies of such document. *See* Aaron Burstein, Will Thomas DeVries & Peter S. Menell, *The Rise of Internet Interest Group Politics*, 19 BERKELEY TECH. L.J. 1, 5 n.12 (2004) (noting "web bugs," among tools that constantly monitor and record individual users' activities, are "shattering" anonymity on the Internet).

92. *Id.; see also* Marcus G. Kuhn & Ross J. Anderson, *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, INFORMATION HIDING 124 (David Aucsmith ed. 1998), *available at* http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf (observing that the discovery of such electronic data leakage dates back to the 1960s, when the British government discovered the leakage of electronic data in the process of attempting to intercept enciphered traffic among French government officials).

93. Caloyannides, *supra* note 90, at 21.

information.[94]

94. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008) [hereinafter ABA Formal Op. 08-451] (setting forth standards for outsourcing that would apply to cloud computing services as "nonlegal support services"). The opinion concludes that under MRPC Rule 1.1 there is "nothing unethical about a lawyer outsourcing legal and nonlegal services, provided the outsourcing lawyer renders legal services to the client with the 'legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation,' as required by Rule 1.1." *Id.* at 2. However, the opinion adds several important cautions, including that "[a]t a minimum, a lawyer outsourcing services for ultimate provision to a client should consider conducting reference checks and investigating the background of the . . . nonlawyer providing the services as well as any nonlawyer intermediary involved, such as a . . . service provider." *Id.* at 3. Furthermore, of particular importance to cloud computing services, which can store client sensitive information offshore in possibly undisclosed countries, is the opinion's caution that "[c]onsideration also should be given to the legal landscape of the nation to which the services are being outsourced, particularly the extent that personal property, including documents, may be susceptible to seizure in judicial or administrative proceedings notwithstanding claims of client confidentiality." *Id.* at 4; *see also* Benjamin W. Heineman, Jr., *European Rejection of Attorney-Client Privilege for Inside Lawyers*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Oct. 2, 2010), *available at* http://blogs.law.harvard.edu/corpgov/2010/10/02/european-rejection-of-attorney-client-privilege-for-inside-lawyers (stating that such cautions are particularly relevant in light of the 2010 decision of the European Court of Justice in *Akzo Nobel Chemicals Ltd I v. European Commission* that ruled that the attorney-client privilege applied solely to communications connected to a "client's right of defence" and in circumstances where such communications came from "independent lawyers," which the Court defined as lawyers "not bound to the client by a relationship of employment," i.e., those who are not in-house counsel). Furthermore, the ABA opinion identified several additional considerations that it stated "must be taken into account under the Model Rules[,]" including that "at the outset, it may be necessary for the lawyer to provide information concerning the outsourcing relationship to the client, and perhaps to obtain the client's informed consent to the engagement of . . . nonlawyers . . . ." Formal Op. 08-451, *supra*, at 4. As we note elsewhere in this article, it would be a prudent precaution to inform clients, and obtain their consent, before taking on the additional and still uncertain risks of placing the client's sensitive information in a cloud computing vendor's servers.

Additional guidance on the issue can be found in the recent opinions issued by the New York State Bar Ass'n Comm. on Prof'l Ethics (NYSBA Op. 842 (2010)) that addresses the ethics of online storing of confidential information and the opinion issued by the Arizona State Bar Ass'n Comm. on the Rules of Prof'l Conduct (AZ Bar Ethics Op. 09-04 (2009)). NYSBA Op. 842 (2010) provides:

> We conclude that a lawyer may use an online "cloud" computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. "Reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps**:**
>
> - Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

In short, as information technology (IT) has become a cornerstone of corporate enterprises and critical to a company's communications both internally and with strategic allies, suppliers, and customers, it has become increasingly important for boards of directors and their lawyers to understand IT and each wave of new communications technologies that impact it. Not infrequently, however, such changes and their commercial significance are difficult for a board to appreciate, making it all the more important for legal counsel to stay abreast of changes in new communications technologies. For example, there were reports that companies and their boards were struggling to figure out the advantages of Web 2.0 technologies, and particularly those supporting online social networks and the collaborative ways of working such networks can facilitate. As a June 2009 report stated:

> Company boards don't recognize what IT is or does any more . . . . It used to be a thing that you used to increase productivity or automate processes, but that's been done. Even chief information officers, who thoroughly understand enterprise IT, have been left behind by social IT—which they can't control.[95]

Given such developments, competent representation arguably implies a duty to stay abreast of new communications technologies. The failure to do so can quickly erode counsel's ability to anticipate, prepare for, and offer advice about the actions, communications, contexts, and crises that such technologies can create or alter. New communications technologies may be most risky when a client has achieved a comfort level with such technology without being aware of recent changes made to the technology by its developer that may have enhanced its features, deleted features, and created new risks for users. In addition, a company's business culture may be changed by use of a technology with little awareness (or only belated understanding) of the consequences. For example, companies that have fully integrated

---

- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored . . . .

New York State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 842 (2010) [hereinafter New York Op. 842], *available at* http://www.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions825present/EO_842.pdf.

95. Peter Whitehead, *Does Business Understand Technology Anymore?*, FIN. TIMES, June 17, 2009, http://www.ft.com/cms/s/0/9dabb29e-5a0d-11de-b687-00144feabdc0.html?nclick_check=1.

e-mail use into their business often regret their over-reliance on internal e-mails, which are rarely if ever drafted with an eye to their possible disclosure in the context of litigation.[96] The same thing can happen with records created and published with Web 2.0 technologies.

B. The Duties to Protect Client Confidential Information Imply a Duty to Keep Abreast of New Communications Technologies

A second source of an implied duty for lawyers and law firms to keep abreast of new communications technologies may be found in NYRPC Rule 1.6 "Confidentiality of Information," which defines "confidential information" as consisting of:

> [I]nformation gained during or relating to the representation of a client, *whatever its source*, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential.[97]

We conclude that the "confidential information" category is broader than information covered by the "attorney-client privilege," and arguably includes all information covered by the "attorney work product" doctrine (given that disclosure of such information would be "detrimental to the client"). Even information that has been obtained indirectly through the use of a new communications technology should probably be treated as "confidential information" under the NYRPC, if it contains or may subsequently become client confidential information.

NYRPC Rule 1.6(a) requires that, unless certain specified conditions have been met,[98] a "lawyer shall not *knowingly* reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of

---

96. *See, e.g.*, Ann O'Neill, *E-mail Can Bounce Back to Hurt You*, CNN (Nov. 7, 2005), http://articles.cnn.com/2005-11-03/justice/email.legal_1_e-mail -office-cubicle-fema?_s=PM:LAW (explaining that e-mails are in the range of litigation discovery, and therefore, improperly drafted e-mails can have significant consequences).

97. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(a) (2011) (emphasis added).

98. *Id.* (specifying three alternative conditions: (1) informed consent by the client; (2) the disclosure is impliedly authorized to advance the client's best interests; or (3) the lawyer reasonably believes the disclosure is necessary to avert serious harm such as death, bodily injury, commission of a crime, etc.).

the lawyer or a third person."[99]

It is unclear whether such disclosure would be considered "knowing" if a lawyer or law firm disregarded well-known risks that could lead to an inadvertent disclosure. Although NYRPC Rule 1.6 does not explicitly adopt a "knew or should have known" standard, counsel who do not keep abreast of new communications technologies could find themselves being held to such a standard if the risks involved were brought to their attention (in, for example, a commissioned risk assessment) or were the subject of widely reported incidents.[100]

The MRPC, on the other hand, does not have a "knowing" requirement for disclosure. Rather, MRPC Rule 1.6 states instead that a "[l]awyer shall not reveal information relating to the representation of a client unless the client gives informed consent, [or] the disclosure is impliedly authorized in order to carry out the representation . . . ."[101] The Rule adds that a lawyer "may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary."[102] under certain specified circumstances. However, based on the nature of the circumstances listed in the Rule, it does not appear that disclosure through communications technologies is "necessary." Rather, MRPC Rule 1.6(b) seems to contemplate that disclosure is necessary only in situations where the safety or financial viability of an individual or an entity is at risk due to the client's actions or potential actions. MRPC Rule 1.6(a) ultimately embodies the general principle underlying attorney-client relationships: that, absent informed consent, the lawyer shall not reveal information relating to the representation. The absence of a qualifying subjective mental element in 1.6(a) suggests that the MRPC impose a higher standard than under the NYRPC. Thus, it is possible that a lawyer's inadvertent failure to understand the risks posed by

99. *Id.* at 1.6 (2011) (emphasis added).

100. Henry Blodget, *Amazon's Cloud Crash Disaster Permanently Destroyed Many Customer's Data,* BUS. INSIDER (Apr. 28, 2011, 7:10 AM), http://www.businessinsider.com/amazon-lost-data-2011-4; Richard Waters, *Technology: Grand Theft Data*, FIN. TIMES, Apr. 29, 2011, http://www.ft.com/intl/cms/s/0/1718ec22-7290-11e0-96bf-00144feabdc0.html#axzz1Whhbzxxu (providing that the security breach at Sony not only compromised private information, but it also temporarily prevented the online multiplayer functionality in PlayStation 3 games from working as Sony found it necessary to take the network offline after discovering that an unknown hacker had misappropriated names, e-mail addresses, user IDs and passwords of over 77 million participants in the PlayStation Network).

101. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007).

102. *Id.* at 1.6(b).

communications technologies—risks that could result in unauthorized disclosure of client information—would increase the likelihood of putting the lawyer at risk of violating MRPC Rule 1.6(a).

However, Comment 5 to MRPC Rule 1.6 appears to diminish the strength of such an argument by stating, "[e]xcept to the extent that the client's instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation."[103] This guidance seems to indicate, first, that a lawyer should be aware of the risks that communications technologies pose, and second, that a lawyer should inform the client of such risks in order to determine whether the client has any special requests for guarding the confidentiality of its information. Nevertheless, it seems that there might be room for the lawyer to utilize his or her traditional method of storing client information in spite of some risk of disclosure. A properly vetted communications technology, for example, which is standard for the firm or for the lawyer, would seem to be "appropriate" in representing the client, although it would be prudent to disclose to the client the use of any new communications technology that could put the confidentiality or secure storage of the client's information at enhanced risk and to obtain the client's consent before subjecting the client's information to such risks.

NYRPC Rule 1.6(c) arguably sets *an elevated standard*, however, when the source of the disclosure is a non-lawyer whose services are utilized by the lawyer or law firm, stating that "[a] lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client . . . ."[104] The underlying principle appears to be that where the disclosure or use might be committed by a non-lawyer, such persons should not be assumed to be as aware of the risks and sensitivities of the information as would be a lawyer.

A provision similar to NYRPC Rule 1.6(c) can be found in Comment 16 of the MRPC. As it currently reads, Comment 16 to MRPC Rule 1.6 states that a lawyer must act "competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or

103. *Id.* at 1.6 cmt. 5 (2007).
104. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(c) (2011).

other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."[105] In borrowing the competence language of MRPC Rule 1.1, Comment 16 indicates that with reference to protecting client information, a lawyer must recognize the risks that technology poses, particularly where a third party might have access to the information.[106] The competence requirement embodied in the MRPC does not seem to differ substantially from the "reasonable care" requirement of the NYRPC. Thus, in addition to recognizing risks, to competently safeguard information, the lawyer must similarly assume and provide for the fact that third-party communications providers are not likely to protect client information as zealously as the client's advocate should.[107]

The ABA Commission's Draft Proposals for amendments to the MRPC and comments has recommended that MRPC Rule 1.6 be amended by the addition of a new section (c) that states: "A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."[108]

The Proposals also recommended that additional guidance be inserted in Comment 16 containing, among other changes, the following statement concerning the obligations under the proposed new section (c) to MRPC Rule 1.6:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure

105. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2007).

106. ABA Formal Op. 08-451, *supra* note 94 (concluding that a lawyer may outsource support services, but recognizing that the lawyer ultimately remains responsible for rendering competent legal services to the client).

107. This view is consistent with the guidance provided by the New York State Bar Association, Committee on Professional Ethics, Opinion 842 from 2010 on the topic of "[u]sing an outside online storage provider to store client confidential information," which observes, in pertinent part:

> Rule 1.6(c) provides that an attorney must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except to the extent disclosure is permitted by Rule 1.6(b). Accordingly, a lawyer must take reasonable affirmative steps to guard against the risk of inadvertent disclosure by others who are working under the attorney's supervision or who have been retained by the attorney to assist in providing services to the client. We note, however, that exercising "reasonable care" under Rule 1.6 does not mean that the lawyer guarantees that the information is secure from *any* unauthorized access.

New York Op. 842, *supra* note 94, ¶ 5.

108. ABA Comm'n on Ethics 20/20, *supra* note 62, at 6.

> if additional safeguards are not employed, and the cost of employing additional safeguards. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.[109]

In explanation, the ABA Commission acknowledged that the duty to protect a client's confidential information was "already implicit in MRPC Rule 1.6[,]" but that "in light of the pervasive use of technology to store and transmit confidential client information, this obligation should be stated explicitly in the black letter of MRPC Rule 1.6."[110] The Commission may also have been mindful that some lawyers may check the black letter rules without taking time to also consult the comments, and therefore, thought it was advisable to ensure the widest possible audience for this enhancement of the existing guidance. We remind readers that our purpose in writing this article is not to create liability for lawyers and law firms, but to assist them in identifying and avoiding the vulnerabilities that they are facing now and will face in the future.

We would note also that the proposed addition to Comment 16 basically makes "reasonable efforts" subject to a common sense judgment call by the lawyer, rather than imposing stringent duties that might quickly become obsolete in light of technologies that may emerge in the near future. However, it should be remembered that the ethical standards set forth in the NYRPC and the MRPC are not intended as the highest standard to which a lawyer should adhere. They set standards below which lawyers should not allow their conduct to go. Common sense and what is for most lawyers the relentless pursuit of their clients' interests will often motivate a lawyer to implement safeguards that exceed those required or recommended in the MRPC. Such common sense often appears most clearly in the ethics opinions thoughtfully prepared by state and city bar associations, as illustrated in the New York State Bar's additional observations in its opinion on using an online system (such as the cloud) to store a client's confidential information, which emphasizes the need to stay abreast of new technologies:

---

109. *Id.* at 9.
110. *Id.* at 2.

> Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. . . .
>
> This Committee's prior opinions have addressed the disclosure of confidential information in metadata and the perils of practicing law over the Internet. . . . [T]he duty to "exercise reasonable care" to prevent disclosure of confidential information "may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks" in transmitting information electronically. N.Y. State 782 (2004), *citing* N.Y. State 709 (1998) (when conducting trademark practice over the Internet, lawyer had duty to "stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost") . . . . The same duty to stay current with the technological advances applies to a lawyer's contemplated use of an online data storage system.[111]

A 2008 ABA Opinion on outsourcing legal services provides additional insight into the precautions that a lawyer would be wise to take in retaining outside services. The Opinion states that at a minimum, a lawyer outsourcing services, which will ultimately involve client information, should "consider investigating the security of the provider's premises, [and] computer network . . . ."[112] Only through a proper vetting process of the communications technology provider will the lawyer have made an attempt to carry out his or her services competently. Additionally, a lawyer's obligations under MRPC Rule 1.6 arguably extend to outside service providers under MRPC Rule 5.3(b). The rule requires lawyers who retain outside services of non-lawyers to make "reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."[113]

Given these obligations, it could be argued that both MRPC Rule 1.6(a) and NYRPC Rule 1.6(c) impose an implicit duty on

111. New York Op. 842, *supra* note 94, ¶¶ 11–12.
112. ABA Formal Op. 08-451, *supra* note 94, at 3.
113. MODEL RULES OF PROF'L CONDUCT R. 5.3(b) (2007).

lawyers and law firms to keep abreast of new communications technologies. Yet new communications technologies may be adopted without a clear understanding of the attendant risks of inadvertent disclosure. For example, Bluetooth, as a wireless transmission method, arguably makes the conversations it transmits vulnerable to interception.[114] Similarly, users of ear-buds for mobile phones often do not realize that the voice of their interlocutor can be overheard in elevators if the volume has not been adjusted to account for the close proximity of third parties.[115]

A lawyer or law firm that ignores such vulnerabilities may be at risk of violating NYRPC or MRPC Rule 1.6(a) if they use such technologies for communicating confidential information. Moreover, as upgrades boost or enhance a communications technology and as "potential adversaries"[116] probe and identify vulnerabilities in the new technologies and plan attacks that exploit such vulnerabilities, it is important for lawyers and law firms to understand those developments and to implement appropriate precautions. For example, counsel to financial institutions would find it prudent to ensure that their review and assessment of such developments and their responses with appropriate updated precautions should not lag behind that required by regulators of their financial institution clients. In that regard, the Federal Financial Institutions Examination Council (FFIEC) decided in 2011 that the guidance it had issued in 2005 for a risk management framework for financial institutions offering Internet-based products and services to customers, entitled *Authentication in an Internet Banking Environment* (the 2005 Guidance), needed reinforcement and a substantive upgrade to keep abreast of the subsequent evolution of external and internal cyber-threats and to ensure that financial institutions responded accordingly. For example, the FFIEC explained that its 2005 Guidance had stated that "institutions should use effective methods to authenticate the

114. Indeed, mobile application developers are developing programs that will only make eavesdropping easier. *See Amplify'd*, JOONITI, http://jooniti.com/products/amplifyd (last visited Oct. 18, 2011).

115. Even more common is the use of smart phones and e-mail-enabled PDAs while in an elevator in the apparent belief that the information displayed on the device's brightly lit and easily read display screen is not visible to others.

116. We use the term "potential adversaries" to refer to any individual, group, organization, government, or government-sponsored entity that seeks unauthorized access to an enterprise's digital assets with the objective of gaining advantage over the enterprise and damaging its defenses, financial well-being, or reputation.

identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information."[117] The FFIEC further explained the standards and measures it expected as a minimum that financial institutions would implement and maintain, such as periodic reassessments of the risks and implementation of layered defenses:

> The Guidance provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties. The 2005 Guidance also provided that institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external threats.[118]

Apparently, the FFIEC had concluded that the 2005 Guidance had ceased to be sufficiently effective, and that the enhancements by adversaries of their capabilities to attack and successfully penetrate financial institution defenses was outdistancing the efforts to defend against and avert such exploits. Thus, the release of updated guidance, entitled *Supplement to Authentication in an Internet Banking Environment* (the 2011 Guidance), came with several strong cautions that reflected the FFIEC's assessment of the growing gap between attacker's capabilities (and successes) and the regulated financial institutions' defenses (and breaches):

> The Agencies are concerned that customer authentication methods and controls implemented in conformance with the Guidance several years ago have become less effective. Hence, the institution and its customers may face significant risk where periodic risk assessments and appropriate control enhancements have not routinely occurred.
>
> . . . .
>
> *Since virtually every authentication technique can be compromised*, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security, as described herein.[119]

117. Press Release, FFIEC, Supplement to Authentication in an Internet Banking Environment 1 (2011), *available at* http://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

118. *Id.*

119. *Id.* at 2 (emphasis added).

> . . . .
> . . . [T]he Agencies are concerned that fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of customer accounts, and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement.[120]

The 2011 Guidance requires at least annual review and update of a financial institution's online risk assessment, which should consider, but not be limited to, "changes in the internal and external threat environment" (focusing apparently on the capabilities of those posing the threats) and "changes in the customer functionality offered through electronic banking" (focusing apparently on the vulnerabilities that new technologies would bring or create).[121] The 2011 Guidance, in its Appendix, highlighted forms of attack that, in some instances, may have been only theoretical possibilities at the time of the 2005 Guidance's publication, but that by 2011 had led to widely reported, severely damaging attacks, such as the following noted in the 2011 Guidance Appendix:

- Fraudsters use of keyloggers to obtain the logon IDs, passwords, and challenge question answers of financial institutions' customers.
- Sophisticated malware allowing fraudsters to perpetrate man-in-the-middle (MIM) or man-in-the-browser (MIB) attacks.[122]

It would not be surprising if many lawyers, even those who advise financial institutions, were not acquainted with and may not even have ever read accounts of MIM/MIB attacks. However, counsel who advise defense contractors and nuclear power plant operators should have at least seen mention of MIM since it was one of the more sophisticated elements of the Stuxnet worm that attacked the uranium processing facilities in Natanz, Iran and was finally discovered and reported in 2010.[123] As explained by the 2011 Guidance:

> In a MIM/MIB attack, the fraudster inserts himself between the customer and the financial institution and

120. *Id.* at 9.
121. *Id.* at 3.
122. *Id.* at 9.
123. William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

> hijacks the online session. In one scenario, the fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account. In another scenario, the fraudster does not intercept the credentials, but modifies the transaction content or inserts additional transactions not authorized by the customer which, in most cases, are funds transfers to accounts controlled by the fraudster. The fraudsters conceal their actions by directing the customer to a fraudulent website that is a mirror image of the financial institution's website or sending the customer a message claiming that the institution's website is unavailable and to try again later. Fraudsters may have the capacity to delete any trace of their attack from the log files.[124]

MIM attacks on SCADA systems have come to be viewed by security experts as the "ultimate aggressive attack," because:

> [N]ot only [is] the controller . . . no longer in control, but the controller doesn't even recognize that [it is] no longer in control. And certainly the SCADA, the HMI, and the operators also do not recognize . . . what's going on . . . . If you were to implement this type of an attack on a pipeline leak detection system, back in the control center [they] would think everything is fine because [they would be] getting replay data showing that the liquids were flowing through as [expected] and there were no leaks, when in fact [liquids] could be gushing out somewhere.[125]

---

124. FFIEC, *supra* note 117, at 9–10. The MIM reportedly used by Stuxnet, resembled deceptions illustrated in the film *Ocean's Eleven* (where the thieves substitute fictitious pre-recorded video for what is supposed to be the real-time video feed from the on-site surveillance observation cameras). Stuxnet's MIM reportedly concealed from the uranium processing plant's SCADA system and the plant operating personnel the unauthorized changes that Stuxnet was executing in the speed of the centrifuge motors, causing them to spin intermittently at excessively high, then excessively low, speeds. As explained by security expert Ralph Langner:

> Rogue code intercepts physical I/O [inputs/outputs] and provides the legitimate program running on the controller with 'normal' input patterns that are actually pre-recorded by Stuxnet . . . .The controller is no longer controlling I/O, but doesn't recognize that. The same is true for the HMI [human machine interface] and for operators. In the meantime, Stuxnet writes to outputs at its discretion [to cause the variations in the frequency of the centrifuge motors].

Ralph Langner, *How to Hijack a Controller: Why Stuxnet Isn't Just About Siemens' PLCs*, CONTROLGLOBAL (Jan. 13, 2011), http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html.

125. Interview by Dale Peterson with Ralph Langner, at 21:05–23:40, DIGITAL

In light of the 2011 Guidance and the reported exploits that occurred in 2010 and 2011, we believe that in interpreting the scope of an ethical requirement to keep abreast of new technologies, it would be reasonable and prudent to infer that such scope could well include not only the development of new communications technologies and the vulnerabilities they bring or create, but also the development of new and enhanced forms of attacks launched by adversaries, since clients will need to defend against and respond to such attacks and, counsel will be in a far better position to advise clients in such situations if counsel has kept abreast of such developments. However, we understand that client and counsel will probably always be attempting to catch up with such developments.

Such an interpretation would be prudent to apply also to the use of new technologies by associates, employees, and others whose services the lawyers and law firms utilize. Supervising lawyers need to be aware of the potential risks and vulnerabilities that may be introduced into their legal practice in order to take appropriate precautions, which may include instructing such personnel on the potential risks and ways to avoid disclosing confidential information. Of course, the adequacy and timeliness of such supervision depends on law firms and lawyers remaining abreast of emerging developments in communications technologies.[126]

On initial reading, Comment 17 to MRPC Rule 1.6, which has no parallel in the NYRPC, seems to address several of these technological concerns. Comment 17 states that when a lawyer is "transmitting a communication" that includes client information, "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[127] However, the Comment goes on to state that the duty does not require the lawyer to put special security measures in place "if the method of communication affords a reasonable

---

BOND (Dec. 15, 2010), *available at* http://www.digitalbond.com/2010/12/15/december-podcast-ralph-langner-stuxnet-interview.

126. As observed in an article in the ABA Journal: "If the history of technology in the legal profession is any guide, most lawyers will eventually understand the utility of today's latest technology as well as any of today's college students do. And they'll come to that understanding about the same time as those college students make partner." Edward A. Adams, *Web 2.0 Still a No-go: Lawyers Slow to Adopt Cutting Edge Technology*, ABA JOURNAL, Sept. 1, 2008, at 52, http://www.abajournal.com/magazine/article/web_20_still_a_no_go.

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

expectation of privacy."[128] In light of the rapid and extensive erosion of privacy that has resulted from the development and use of Web 2.0 technologies, such guidance is far from clear and may appear, to some, to amount to putting lawyers in the position of trying to speculate on the present and future boundaries of an already admittedly controversial grey area—that of what constitutes a "reasonable expectation of privacy."[129]

As a 2010 California State Bar opinion illustrated, courts have come to different conclusions on the degree of privacy that lawyers should expect from communications technologies, such as e-mail.[130] Some courts have indicated that, unlike postal mail, e-mails are generally not sealed or secured in the same fashion and thus pose a greater security risk.[131] Nevertheless, a majority of state bar associations have taken the position that e-mails enjoy the same sense of security as traditional postal mail.[132] An ABA Formal Ethics Opinion from 1999 supports this view.[133] In that opinion, the ABA states that lawyers may transmit information relating to client representation through *unencrypted* e-mail without violating the MRPC "because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[134] Furthermore, the ABA found that the same privacy afforded to U.S. mail applies to e-mail, but it noted that the lawyer should nevertheless consult with the client regarding any specific instructions about transmitting highly sensitive information.[135] Although there is a threat that information transmitted through either method will be intercepted, lawyers are under no greater

128. *Id.*

129. Some privacy experts have begun to argue that the focus on "reasonable expectation of privacy" is misplaced and that the locus of discussion should be changed. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 114 (2011) ("For a long time, I believed the fix was for the Supreme Court to adopt a more sophisticated and forward-looking view of privacy. I now realize that I was wrong. The entire debate over reasonable expectations of privacy is futile, for it is not focused on the right question.").

130. *See* California State Bar Ass'n Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179, at 3 (2010) [hereinafter California Formal Op. 2010–179], *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket =wmqECiHp7h4%3D&tabid=837.

131. *See id.*

132. *Id.*

133. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) [hereinafter ABA Formal Op. 99-413].

134. *Id.* It should be noted, however, that the Committee's conclusions in this opinion were based upon the information available to it in 1999.

135. *Id.*

security obligations when using technological transmission than they would be in using postal services.[136]

However, it is possible that Comment 17 is not broad enough, or that it was not intended to address the expansion of technologies such as Bluetooth or products and services based on cloud computing platforms. Arguably, Comment 17 suggests that lawyers can expect a reasonable degree of privacy when transmitting e-mails through the lawyer or the law firm's secure system.[137] But where a lawyer utilizes a third party mechanism or a less secure communications technology, additional precautions may be warranted, particularly if it becomes apparent—as it should be with data stored in the cloud—that counsel will have less control over the handling of client data stored, processed, copied, and relocated at off-site server farms, and if, in relinquishing such control, counsel is unable to satisfy herself or himself that the client's data is as well protected against unauthorized access, disclosure, damage, or destruction as it was before moving such data to the cloud.[138]

---

136. *See id.* ("It is not . . . reasonable to require that a mode of communicating information . . . be avoided simply because interception is technologically possible.").

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

138. ABA Formal Op. 99-413, *supra* note 133; MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2007). As Alabama Bar Ethics Opinion 2010-02 observes and cautions:

> The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider.

Alabama State Bar, Formal Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf.

Moreover, even the experts that counsel may consult in attempting to assess risks to digital systems and data stored and processed on them may find that the experts have underestimated the capabilities of really determined, well-funded, potential adversaries. As noted in a recent Scientific American article:

> [T]he average control system engineer would have once dismissed out of hand the possibility of remotely launched malware getting close to critical controllers, arguing that the system is not directly connected to the Internet. Then Stuxnet showed that control networks with no permanent connection to anything else are still vulnerable. Malware can piggyback on a USB stick that technicians plug into the control system, for example. When it comes to critical electronic circuits, even the

IV. MINIMIZING LAWYERS' ETHICAL RISKS IN CLOUD COMPUTING SERVICES

In this section, we provide an overview of how cloud computing services work as a general proposition. Next, we evaluate the risks that at present appear inherent in the use of such services and some of the ethical challenges and risks that may arise when lawyers and law firms consider whether to entrust client data to cloud computing service vendors. And, finally, we suggest some measures that may help to minimize those risks.

A. Cloud Computing Services

By 2007, individuals and enterprises were already deciding to migrate various kinds of data to third party vendors who maintained large server farms in order to store, process, and make wirelessly accessible such data to the data customers. Referred to by names such as "grid, utility, or cloud computing," such services promised the data customer that if it would outsource the hosting of hardware and software, the customer could "just link" to the data and software when needed.[139] The more companies that decide to locate, at least, part of their data in the cloud and the more sensitive the data that they entrust to the cloud, the greater the probability that potential adversaries will come to view cloud servers as a treasure trove of digital assets and may be tempted to probe such servers for vulnerabilities and to design attacks to exploit them. Our concern is that the decision for clients, lawyers, and law firms about whether to make use of cloud services carries with it risks that are difficult to assess, in part because the vendors keep the structure and operation of their cloud computing services remarkably opaque to customers, and in part because the use of cloud computing involves creation of potentially multiple copies

---

smallest back door can let an enterprising burglar in.
David M. Nicol, *Hacking the Lights Out*, SCI. AM. (July 2011), *available at* http://www.cs.virginia.edu/~robins/Hacking_the_Lights_Out.pdf. For at least two years, it has for such reasons been impermissible for faculty at Department of Defense (DoD) educational institutions, such as the U.S. Military Academy, to insert USB sticks into the institution's networked computers. Of course, for the military, as for counsel, the problem with such safeguards is whether they can be consistently enforced, or whether human nature and the pressure of coping with exigencies will lead someone to violate the prohibition in order to achieve a valuable convenience without realizing that it only takes one such lapse for the locked door to swing open to a potential adversary's malware.

139. M. Mitchell Waldrop, *Data Center in a Box*, SCI. AM. (Aug. 2007), *available at* http://www.angelfire.com/folk/thegrieves/transfer/200708.pdf.

whose location the data customer will not be aware of. As a result, clients may be at risk of underestimating the risks to their intellectual property of keeping sensitive data in the cloud (e.g., it would seem a premature and perilous exercise for an enterprise to authorize the storage of any copy of its trade secret information in the cloud), and counsel face a double risk: the challenge of advising clients and ensuring that their interests will be protected if they decide to move their data to the cloud and the challenge of deciding in what circumstances a lawyer or law firm may authorize the uploading of client data to the cloud without putting at risk their obligations to the client, the client's trust, and their professional ethical duties. We will explore such issues in this section and attempt to identify the most important considerations that lawyers and law firms should inform themselves of and assess before deciding whether any client data should be stored in the cloud, and if so, what kinds of data can be and what kinds should probably not be moved there.

1. Overview of the "Cloud" —Features and Potential Benefits

Time-shared computing preceded the proliferation of personal computers into each office of a company.[140] "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."[141]

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.[142] The World Wide Web's emergence made "desktop publishing" into an unexpectedly shortsighted vision of what would become computer-aided dissemination, but it still promoted the decentralization of computing—where each employee would have a terminal on their desk, and later each would have a laptop, a smart phone, or a tablet to take on business trips, on the daily commute, or for working remotely from home.

140. *See* Robert W. Lucky, *Cloud Computing*, IEEE SPECTRUM (May 2009), http://spectrum.ieee.org/computing/software/cloud-computing (remembering the days of time-shared computing).

141. *Id.*

142. *See History of Desktop Publishing*, TEXAS SCHOOL FOR THE DEAF, http://www.tsd.state.tx.us/cte/careertech/desktoppublishing/historyDTP.HTM (last visited Oct. 18, 2011).

Today, the amount of data processed is growing daily, and the need for company personnel to access it from nearly everywhere has become compelling.[143] The costs of providing such capabilities are substantial, and once invested, a company is stuck with the processing capability even if it is underutilized and, therefore, an inefficient investment. In response to these challenges, 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.[144] 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.[145] The promise is a "virtual computing environment that's dynamically allocated to meet user needs."[146]

The term "cloud computing" is imprecise and ambiguous, because cloud services and the meaning of the term "cloud computing" (and related terms and concepts such as "virtualization") are rapidly evolving. As NIST has observed, "[c]loud 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."[147]

In 2009, NIST proposed a working definition that described "cloud computing" as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications,

143. *See* Roger Cheng, *So You Want to Use Your iPhone for Work? Uh-oh*, WALL ST. J. Apr. 25, 2011, http://online.wsj.com/article /SB10001424052748704641604576255223445021138.html.

144. *See, e.g.*, Mark Milian, *What Makes Apple's iCloud Different from Google and Amazon Services,* CNN TECH (June 6, 2011), http://www.cnn.com/2011/TECH /web/06/06/apple.icloud/index.html?iref=allsearch (discussing Apple's new iCloud service and how it compares to Google and Amazon's similar services).

145. Sharon K. Sandeen, Kenneth L. Dorsey, Theodore F. Claypoole, James Garrity & Christopher Kudlick, *Protecting Trade Secrets in the Cloud: What Efforts are Reasonable Enough?*, CLE Presentation, Boston (Apr. 2011) (copy of handout on file with the authors).

146. John Harauz, Lori M. Kaufman & Bruce Potter, *Data Security in the World of Cloud Computing*, IEEE SECURITY & PRIVACY, July–Aug. 2000, at 61, *available at* http://www.idi.ntnu.no/emner/tdt60/papers/05189563.pdf.

147. Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing (Draft)*, NAT'L INST. STANDARDS & TECH., 1 (June 1, 2009), *available at* http://www.newinnovationsguide.com/NIST_Cloud_Definition.pdf.

and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[148] NIST identified five essential characteristics of "cloud computing":

> [1.] *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
>
> [2.] *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
>
> [3.] *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
>
> [4.] *Rapid elasticity.* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
>
> [5.] *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of utilized service.[149]

NIST announced changes to its standards in May 2011.[150]

---

148. *Id.*

149. Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing (Draft)*, NAT'L INST. STANDARDS & TECH., 2 (Jan. 2011) [hereinafter 2011 *NIST Standards*], *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

150. NIST CLOUD SYNOPSIS, *supra* note 13, at 2-1. These changes are discussed, to the extent relevant to this article, in Part VI, *infra*.

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 home-office based) devices. As one observer emphasized, "[c]loud 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."[151]

At present, three main delivery models for cloud computing have been developed:

> [i] *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
>
> [ii] *Cloud Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
>
> [iii] *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select

151. Steve Hamm, *Cloud Computing's Big Bang for Business*, BUS. WK., June 15, 2009, at 43.

networking components (e.g., host firewalls).[152]

Unless otherwise specified, reports concerning cloud computing tend to refer to cloud "software as a service."[153] 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 companies to scale up or down their use to fit their needs by accessing remotely stored programs instead of purchasing licensed software and upgrades.[154] 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 a vendor's provision of raw data processing power and storage capacity at times of need, or even to replace in-house capacities altogether.[155]

Two examples of prodigious cloud storage are "Amazon Simple Storage Service"[156] and Microsoft's Azure cloud computing platform. Microsoft Azure is built on more than one million servers in the company's data centers[157] and charges "12 cents an hour for computing, 15 cents per gigabyte for storage and 10 cents per 10,000 storage transactions."[158] Amazon has emerged as one leader in this business.[159] As one observer noted, "[m]ore than half the online bookseller's computing resources are being consumed

152. 2011 *NIST Standards*, *supra* note 149, at 2–3.

153. *See, e.g.*, Gene Marks, *Beware the Hype for Software as a Service*, BUS. WK. July 24, 2008, http://www.businessweek.com/technology/content/jul2008/tc20080723_506811_page_2.htm (describing cloud "service as software" myths).

154. *See, e.g.*, Jessica Hodgson & Scott Morrison, *"Cloud Computing" Prices Announced by Microsoft*, WALL ST. J., July 15, 2009, at B5 (detailing Microsoft's pricing model for Azure, Microsoft's new "cloud computing" platform).

155. *See, e.g.*, *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2 (last visited Oct. 18, 2011) ("[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.").

156. *Amazon Simple Storage Service (Amazon S3)*, AMAZON WEB SERVICES, http://aws.amazon.com/s3 (last visited Oct. 20, 2011). 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." *Id.*

157. Richard Waters, *Azure to Boost Microsoft's Online Presence*, FIN. TIMES, July 15, 2009, http://www.ft.com/cms/s/0/6203b286-70d4-11de-9717-00144feabdc0.html#axzz1Ynwuf4MJ.

158. Hodgson & Morrison, *supra* note 154, at B5. The article also reports that Amazon charges "12.5 cents an hour and 15 cents a gigabyte for storage in two of its pricing models." *Id.*

159. Blodget, *supra* note 100.

by other companies, which run their own applications in its data centres . . . . Customers include the New York Times and Nasdaq."[160] 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."[161]

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

(1) "public clouds" operated by third-party providers and made available to the general public or a large industry group;[162]
(2) "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);[163]
(3) "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);[164] and
(4) "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.[165]

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 the resources of a "community cloud" or "public cloud"—a process known as "cloud bursting."[166] One commentator explained the distinction between public and private clouds as follows:

---

160. *Cloud Control*, *supra* note 56.

161. *Gathering Clouds: The Takeover Talks Between IBM and Sun Highlight a Shift in the Industry*, THE ECONOMIST, Mar. 19, 2009, http://www.economist.com/node/13331334 [hereinafter *Gathering Clouds*].

162. *Id.*

163. *Id.* For a distinction between public and private clouds, see *infra* note 167 and accompanying text.

164. *See* 2011 *NIST Standards*, *supra* note 149, at 2.

165. *Id.*

166. For a discussion of "cloud bursting" see Jeff Barr, *Cloudbursting—Hybrid Application Hosting*, *Amazon Web Services Blog*, AMAZON WEB SERVICES (Aug. 28, 2008), http://aws.typepad.com/aws/2008/08/cloudbursting-.html.

> 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.[167]

In 2009, some observers predicted that cloud-based computing would increasingly become the primary platform for web applications.[168] As measured in 2011 by the subsequent actions of major software and cloud computing developers, the forecast appears to have been accurate. For example, in October 2010, Microsoft announced that the next generation of its Office suite software, Office 365, would be a cloud-based version.[169] In June 2011, Apple announced its iCloud services that reportedly would include storage of documents created using iCloud Storage APIs and that would "automatically" push them to the user's mobile devices; Apple deployed iCloud in October 2011.[170] Measured by the number of hours that they are accessed by users, cloud-based networks already have become a significant platform, and in some activities, the predominant platform.[171] 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

---

167. *Gathering Clouds, supra* note 161.

168. J.D. Lasica, *Identity in the Age of Cloud Computing: The Next-Generation Internet's Impact on Business, Governance and Social Interaction*, THE ASPEN INSTITUTE, 9 (Apr. 21, 2009), *available at* http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/Identity_in_the_Age_of_Cloud_Computing.pdf.

169. Press Release, Microsoft Inc., Microsoft Announces Office 365 (Oct. 19, 2010), *available at* http://www.microsoft.com/presspass/press/2010/oct10/10-19office365.mspx.

170. Press Release, Apple Inc., Apple Introduces iCloud (Jun. 6, 2011), *available at* http://www.apple.com/pr/library/2011/06/06Apple-Introduces-iCloud.html.

171. The Pew Research Center reported in September 2008 that sixty-nine percent of "online Americans" use cloud computing services. *See* John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RES. CENTER (Sept. 12, 2008), http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

> 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 (now closed). The cloud has become our development network: open source programmers trade code on sites like *SourceForge.net* and *Drupal.org*.[172]

The promised benefits of cloud computing, however, appear to be outpacing many users' ability to identify and understand the attendant risks and what might qualify as adequate safeguards to avert or minimize such risks. The reported benefits of cloud computing 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.[173] Other advantages purportedly include "[allowing users] 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 . . . ."[174]

There are, however, serious risks—some known, some guessed at, and some that will probably arise and surprise even the vendors themselves. For example, as reported in early August 2011, security researchers at the Black Hat USA security conference demonstrated ways in which users of Amazon's Elastic Compute Cloud (EC2) services had been "tricked into using virtual machines that could have included 'back doors' for snooping."[175] It would be naïve to assume that cloud computing, unlike previous new communications technologies related to cyberspace, will not result in serious data breaches. Although it is a difficult fact for vendors, clients, customers, and lawyers to accept, if data needs to be kept secure and safe from unauthorized access (as needed to protect trade secrets, privacy of personally identifiable data, safeguards for

172. Lasica, *supra* note 168, at 5.

173. Peter Laudenslager, *Six Cloud Computing Benefits for SMBs*, INFORMATIONWEEK (June 2, 2010, 7:00 AM), http://www.informationweek.com/news/225200751.

174. *See* Lucky, *supra* note 140.

175. Joseph Menn, *Security Experts Find Flaws in Cloud Computing*, FIN. TIMES, Aug. 2, 2011, http://www.ft.com/intl/cms/s/2/6cc04ca2-7f8e-11de-85dc-00144feabdc0.html#axzz1UFSXDpwA.

nuclear power plants, national security information, etc.), then such data should not be accessible from the Internet and should be kept "air gapped" from the Internet. Otherwise, it is probably only a matter of time before it will be compromised, often without the owner's or custodian's knowledge. These concerns have been echoed by analysts seeking to get security taken seriously, as illustrated in the following three observations by such analysts: "The security of these cloud-based infrastructure services is like Windows in 1999. It's being widely used and nothing tremendously bad has happened yet. But it's just in early stages of getting exposed to the internet, and you know bad things are coming."[176] Ryan Rubin, U.K. head of security and privacy at Protiviti, an IT security company, says: "There aren't many people putting mission-critical data in the cloud. The crown jewels—customer records, for example—are still very much embedded in the organisation."[177] A director at one London investment bank says: "We use the cloud for things such as e-mail. We would never put our client services on it."[178]

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.[179] Nonetheless, counsel should consider at least the currently known risks, particularly before they and their law firms adopt cloud computing and put their own and their clients' records into the cloud. This article also argues that lawyers and law firms should review developments in cloud computing and risks on a dynamic basis as cloud capacities change and reports of specific risks or incidents emerge.

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

The ethical risks for lawyers and law firms from cloud

176. *Id.* (quoting John Pescatore, security analyst at Gartner). Note, however, that the comment that "nothing tremendously bad has happened yet" appears already inaccurate and obsolete, in light of reports of offshore hacking, such as those disclosed in the Operation Shady RAT report. Dmitri Alperovitch, *Revealed: Operation Shady RAT*, MCAFEE 2–3 (Aug. 2, 2011, 9:14 PM), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

177. Palmer, *supra* note 7.

178. *Id.*

179. JOHN N. STEWART, EXECUTIVE PERSPECTIVE: VULNERABILITY DISCLOSURE (2006), *available at* http://www.cisco.com/web/about/security/cspo/docs/article_vulnerability-Disclosure20060701.pdf.

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 insiders (resulting in data shared with unauthorized persons), and risks from state surveillance and interception under the auspices of legal authority.[180] The discussion below focuses on public clouds, as it seems unlikely that law firms will initially set up their own private clouds (such investments are hard to justify during recessions), or will find it impractical 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,[181] 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.[182] The cloud service providers themselves

180. Although we believe that ethical risks from cloud computing will probably arise in connection with inadvertently and inadequately handled security risks, we would point out that the ABA's Commission on Ethics 20/20's Working Group on the Implication of New Technologies clearly distinguished between "best practices" for security and ethically required security measures, and emphasized that there is not only a gap, but that the standard for what is ethically required is below that of "best practices." As the Working Group carefully explained:

> As an initial matter, the Commission recognizes that there may be a gap between technology-related security measures that are ethically required and security measures that are merely consistent with "best practices." For example, it may be consistent with best practices to install sophisticated firewalls and various protections against malware (such as viruses and spyware), but lawyers who fail to do so or who install a more basic level of protection are not necessarily engaged in unethical conduct. Similarly, it might be inadvisable to use a cloud computing provider that does not comply with industry standards regarding encryption, but it is not necessarily unethical if a lawyer decides to do so.

ABA Comm'n. On Ethics 20/20, *Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology* (Sept. 20, 2010), *available at* http://myshingle.com/wp-content/uploads/2010/11/cloudcomputing.pdf.

181. *See* Oxford Analytica, *IT Outsourcing Poses Risks*, FORBES (Oct. 22, 2009, 6:00 AM), http://www.forbes.com/2009/10/21/information-technology-outsourcing-risks-technology-oxford.html.

182. *See* Jon Brodkin, *Gartner: Seven Cloud-Computing Security Risks*, INFOWORLD (July 2, 2008), http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

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."[183] 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 review 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 what appear at present to be 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.

b. Instabilities of Cloud Software

i. Program Instability and Defects

Programs like Google Docs have a relatively short track record or performance history. Thus, their stability—their ability to remain operable without intermittent or prolonged interruption from "crashes" and "outages"—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, e.g., "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."[184]

That level of availability would not meet the requirements set

183. *See* Harauz, Kaufman & Potter, *supra* note 146, at 62.

184. Jon Brodkin, *U.S. Government Launches Cloud Push, Demands Strict Uptime and Service Levels*, NETWORKWORLD (Aug. 5, 2009, 4:06 PM), http://www.networkworld.com/news/2009/080509-federal-government-cloud-computing.html.

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 Site—which will enable Government purchasers to buy . . . service offerings."[185] Presumably to avert such shortcomings, the GSA's RFQ requires the contractor to provide availability based on a monthly calculation as follows: "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%)."[186]

The problem with such specifications for "uptime" is the kind commonly encountered in any computer-based, mission-critical system (such as flight control and military fire-control systems). Unless the specified requirement is simple and straightforward, and can be verified with tests based on facts accessible to the customer or end-user, the requirement becomes incomputable, hopelessly vague, and ultimately unenforceable. For example, a military tactical display (in a fighter aircraft or submarine) must be updated rapidly, at consistently timed intervals, and completely, or else the end-user will lose sight of the tactical environment and be "blind" to changes in the adversary's position and in weapons fired. If the specified response time for such a display is "every 0.5 second,"[187] that must be measurable with data accessible to the end-user. Regrettably, the typical service level agreement of cloud vendors expresses the crucial value of "uptime" in a percentage whose calculation requires facts that only the vendor possess (such as processing time for all requests during a specified interval) or that neither party has access to (such as excluding the "time for transmittal from a customer's system to the cloud vendor's servers). The apparent precision carried out to two places past the decimal point (99.95%) and the apparent high probability of system "uptime" (which looks so close to 100%) are illusory. Since the consumer cannot compute "uptime," the precision is a disguised

185. General Services Administration, U.S. Federal Cloud Computing Initiative, *Request for Quotation, Attachment C, Statement of Work*, § 3.2, at 3 (July 30, 2009), *available at* http://www.scribd.com/doc/17914883/US-Federal-Cloud-Computing-Initiative-RFQ-GSA.

186. *Id.* at 6 tbl.2.

187. *See, e.g.*, COALITION WARRIOR INTEROPERABILITY DEMONSTRATION 2005 FINAL REPORT: COMMON OPERATING PICTURE PRODUCT LINE 1 (2005), *available at* http://123.204.62.144/JL/Image/Web_Research/Web_Research_12.pdf (last visited Oct. 16, 2011) (discussing the COP-Tactical Display System product as "maintaining near real time refresh rates (sub-second)").

inexactitude. Since the vendors also include numerous caveats and exclusions for "downtime" that will not be counted against the promised "uptime" percentage, the seemingly high reliability proves to be something less and indefinite.[188]

Moreover, the service level agreements apply a "red tape" barrier that creates extraordinary hurdles to a customer seeking a credit for a failure of the cloud vendor's system to achieve the specified "uptime." Consider the steps that a leading cloud vendor requires the customer to complete in order to qualify for a credit that it even then might not necessarily receive:

> To receive a Service Credit, you must submit a request by sending an e-mail message to aws-sla-request @ amazon.com. To be eligible, the credit request must . . . (ii) include, in the body of the e-mail, the dates and times of each incident of Region Unavailable that you claim to have experienced including instance ids of the instances [sic] that were running and affected during the time of each incident; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); . . . . If the Annual Uptime Percentage of such request is confirmed by us and is less than 99.95% for the Service Year, then we will issue the Service Credit to you . . . . Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.[189]

The record of outages and the opaque and often delayed explanations the vendors tend to give for the causes suggests that customers are being asked to treat the "uptime" percentages as a sufficiently high reliability to entrust their data and processing to the cloud, but without any effective recourse or remedy in the event of an outage or a denial of access that the vendor can impose in its sole discretion. Amazon, for example, requires the customer to agree that Amazon may take "any of the corrective action regarding Customer Accounts to the extent we deem necessary or appropriate, in our sole discretion,"[190] and that such action may

188. We provide an example of the regressive and ultimately incomputable calculations *infra* note 513.

189. *Amazon EC2 Service Level Agreement*, AMAZON WEB SERVICES (Oct. 23, 2008), http://aws.amazon.com/ec2-sla.

190. *AWS Service Terms*, AMAZON WEB SERVICES, § 7.10, http://aws.amazon.com /serviceterms (last updated Aug. 22, 2011).

include "suspending, canceling or closing of Customer Accounts."[191] Moreover, the agreement further authorizes Amazon to "throttle, suspend or terminate your access to SES (Simple Email Service), or block or decline to send any SES Email,"[192] in Amazon's sole discretion if it determines that certain events have occurred, including alleged customer noncompliance with the agreement. That is extraordinary leverage when the pressure the vendor can apply is denial of access to, and use of, a communications mode that is as fundamental to current business as e-mail.

ii. Operating System Instability and Defects

The same risks of unproven, long term stability arise equally with regard to a cloud vendor's operating systems as with any operating system whose uptime and reliability must be sufficient to avoid a costly and untimely disruption to a customer's business activities. Anyone who used an early Windows-based computer has probably had the experience of adding new applications that conflicted with, or would not operate reliably on top of, the Windows operating system. Similarly, such conflicts would often appear with distressing results when a new version of the operating system was issued or patched. At least, in such instances, the individual user or the business enterprise could decide what applications to add or remove to reduce the frequency and severity of conflicts and disruptions. However, when a customer elects to use a cloud vendor's services, such decisions also are entrusted to the sole discretion of the cloud vendor, which can put customers at risk without them knowing when the vendor is taking the risks by adding or subtracting applications or making so-called "routine" maintenance updates to its operating system, which may result in a sustained outage. As one commentator has observed:

> [With a software-as-a-service cloud system] [y]ou would have no control over what other applications are sharing the same server; each other application provides a potential point of entry for hackers, and poorly written software might have adverse effects on the stability of the operating system . . . . [I]n the event of server instability, the hosting company could easily transfer the site to a different server. You would however be reliant upon them

191. *Id.*
192. *Id.* § 22.2.

> to monitor their systems closely and expedite the move.[193]
>
> . . . .
>
> In addition, there is the issue of loss of control. Providers like Amazon reserve the right to shut off the server without prior notice if it is behaving in a way that leads them to believe it has been compromised by hackers, or if they think we are using it for unethical activities like spamming. This means that if you were to end up on a blacklist by mistake, the consequences would be worse than with a non-cloud server.[194]

iii. Upgrade Instability and Defects

Upgrades often introduce new instabilities or instabilities whose symptoms and recovery times are unfamiliar to the user. Indeed, the chief executive of Hyundai Capital, which is South Korea's largest consumer-finance company, recently observed:

> We need to put a price tag to every IT door and window. Maybe we want to have another website, and we think the development cost is $500,000. But that could also mean there is an additional hacking route. So that adds to the cost and consideration. Before this, we were crazy making apps. Apps are more convenient for us and for the clients. But now, we understand that each application creates a new route for hacking. We are now slowing down the whole organization. How things look and how they work is now secondary. Security is now first.[195]

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.

---

193. Neil Turner, *Cloud Computing: A Brief Summary*, LUCID COMMC'NS LTD., § 2.1 (Sept. 2009), *available at* http://www.lucidcommunications.co.uk /Content/whitePapers/CloudComputing.pdf.

194. *Id.* § 3.1.

195. Evan Ramstad, *Executive Learns from Hack*, WALL ST. J., June 21, 2011, at B6.

This may happen regardless of, whether the customer wants the risks and whether the customers are prepared for those risks and for the accompanying learning curve for using the software.

The risks in cloud computing remain hard to assess. That they are not imaginary or far-fetched has been demonstrated by reported "crashes" and "outages" of cloud computing services,[196] corruption of data in at least one instance,[197] and unauthorized release of customer data.[198] An early example of the types of risks cloud computing may raise occurred on February 24, 2009, when Google's e-mail service, which at the time had over 100 million customers (including both individuals and businesses), suffered a complete world-wide shut down, depriving customers of access to their Gmail accounts for more than two hours.[199] Because it occurred at 1:30 a.m. Pacific Standard Time, most U.S. customers were unaffected.[200]

Users in Europe and Asia had a brief experience of a "worst-case scenario" for users of a public cloud software as a service: an inability to send, receive, or to gain access to their remotely stored e-mail data and attachments.[201] On March 10, 2009, Google's e-mail service went down for an undisclosed reason, but apparently a significant number of users found service restored within a half hour, but others reportedly remained without access to their accounts for several hours.[202] A similar shut down of Gmail occurred in August 2008.[203] A May 14, 2009 "outage at Google"

196. *See* Blodget, *supra* note 100 (noting that Amazon experienced a "massive service outage" that led to gaps in customers' historical data).

197. *Id.*

198. Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426 (stating that about 77 million Sony users had their identities stolen because of a massive breach of Sony's video game network).

199. Chris Nuttal, *Google E-mail Crash Hits Millions and Raises Fears over Web Services*, FIN. TIMES, Feb. 25, 2009, http://www.ft.com/intl/cms/s/0/0950a2b6-02de-11de-b58b-000077b07658.htmlWTO#axzz1YuyDoGKi.

200. *Id.*

201. *See generally Four Hours Without Gmail*, N.Y. TIMES (Feb. 24, 2009, 9:47 AM), http://bits.blogs.nytimes.com/2009/02/24/four-hours-without-gmail/ (noting that millions of users in Europe were without e-mail access during work hours, and those in Asia were without services post-work).

202. Andrew Morse, *Google Mail Hit by Outage, Second in Less than Month*, WALL ST. J., Mar. 11, 2009, at B5.

203. *See* Murad Ahmed, *Google Mail Users Hit by Global Outage*, SUNDAY TIMES (Feb. 24, 2009), http://technology.timesonline.co.uk/tol/news/tech_and_web/article5797157.ece ("The last major Gmail outage was in August 2008, when the service shut down for 'a couple of hours.'").

disabled use of Google's cloud services for many of its customers.[204]

Google has yet to reveal the cause of the August 2008 shut down. Google eventually disclosed the cause of the February 2009 shutdown, 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:[205]

> [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 cent[er] and triggered an overload, causing data to be pushed automatically into a third cent[er].
>
> That in turn led to another overload, eventually triggering a series of failures that toppled Google's data cent[er]s like falling dominoes.[206]

The so-called "rogue code" that caused the shutdown was written by one of Google's in-house programmers.[207]

iv. Potentially Irrevocable Losses of Data or Data Temporarily Inaccessible

As noted in the Introduction to this article, serious data breaches and outages have been reported in 2011 concerning cloud computing services offered or used by several major vendors such as Google, Amazon, and Sony. Although the vendors acknowledge that such incidents are regrettable and try to play down their significance, the consequences from security breaches, to cloud and non-cloud computing systems, appear to be growing in severity, financial cost, and reputational damage.[208] Sony, for

---

204. Steve Hamm, *Cloud Computing's Big Bang for Business*, BUSINESSWEEK, Jun. 15, 2009, at 44.

205. Richard Waters, *Rogue Code Led to Gmail Shutdown,* FIN. TIMES, Mar. 1, 2009, http://www.ft.com/intl/cms/s/2/c5dd4574-06a3-11de-ab0f-000077b07658.html#axzz1QoIjDiB7.

206. *Id.*

207. *Id.*

208. One of the most costly breaches to date involved the March 2011 breach by an advanceMD persistent threat attack of RSA's SecurID two-factor authentication tokens reportedly used by "40 million employees to access sensitive corporate and government networks." Dan Goodin, *RSA Breach Leaks Data for*

example, whose online gaming system is "delivered through the cloud,"[209] reported that its April 2011 security breach, which resulted in the theft of "names, addresses, passwords and possibly credit card details of 77m accounts,"[210] would probably cost it "¥14bn."[211] However, probably the worst adverse consequence for data customers is the potential irrevocable loss of data. Illustrative of such a loss is the one that occurred at Ma.gnolia, a cloud provider of bookmarking services, (i.e., one that enables customers to bookmark web sites and web pages).[212] Ma.gnolia revealed in February 2009 that it "could not recover" customers' work "from a corrupted database." "There was also no recoverable back-up, meaning many users would have lost their carefully cultivated collections."[213] 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.[214]

After Amazon's April 2011 outage, it was reported that "[s]ome

---

Hacking SecurID Tokens, THE REGISTER (Mar. 18, 2011, 00:39 GMT), http://www.theregister.co.uk/2011/03/18/rsa_breach_leaks_securid_data. RSA's parent, EMC, disclosed in July 2011 that to deal with the cyber attack it spent $66 million in second quarter 2011, most of which was devoted to transaction monitoring for its corporate customers who were concerned that their RSA security tokens had been compromised as a result of the attack. Hayley Tsukayama, *Cyber Attack on RSA Cost EMC $66 million*, WASH. POST (July 26, 2011, 4:46 PM), http://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html.

209. *Online Reputations in the Dirt*, THE ECONOMIST, Apr. 30, 2011, at 65.

210. *Id.*

211. Jonathan Soble, *Tax Charge Takes Sony Into $3bn Loss*, FIN. TIMES, May 23, 2011, http://www.ft.com/cms/s/2/bf4fd94a-8506-11e0-871e-00144feabdc0.html#axzz1Z1J8FfJ5.

212. Michael Calore, *Ma.gnolia Suffers Major Data Loss, Site Taken Offline*, WIRED (Jan. 30, 2009, 12:56 PM), http://www.wired.com/epicenter/2009/01/magnolia-suffer.

213. Chris Nuttall, *Global Crashes Spark Crisis of Confidence*, FIN. TIMES, Mar. 12, 2009, http://www.ft.com/cms/s/0/bb4a1fea-0d0d-11de-a555-0000779fd2ac,dwp_uuid=b50bc45e-0d16-11de-a555-0000779fd2ac.html.

214. *Id.*

data seem to have been lost permanently."[215]

Data that becomes temporarily inaccessible can have profound consequences for a lawyer or law firm whose clients need work performed urgently. Delays in getting to 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 or result in waivers of privilege. 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 Google Docs customers, a glitch allowed unauthorized shared access to certain documents stored 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.[216]

v. Ethical Issues

If a lawyer or law firm is considering the use of a public cloud for storage or processing of records that include confidential client information, certain precautions are advisable in order to protect the client's interests and to ensure compliance with the NYRPC and the MRPC. Because 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

215. *Online Reputations in the Dirt*, ECONOMIST, Apr. 30, 2011, at 65.

216. Stephen Shankland, *Google Docs Suffers Privacy Glitch,* CNET (Mar. 9, 2009, 7:05 AM), http://news.cnet.com/google-docs-suffers-privacy-glitch.

the course of the representation . . . ."[217]

The NYRPC does not define "intentionally." However, it gives the following interpretive guidance for the use of the word "knowingly": "A person's knowledge may be inferred from circumstances."[218] 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 evidence 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 NYRPC 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 NYRPC Rule 1.1(c)(2), but also NYRPC Rule 1.3(a) and 1.3(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."[219]

The "competent representation" requirement in the MRPC contains far less detail than NYRPC Rule 1.1. MRPC Rule 1.1 merely states that "a lawyer shall provide competent representation," which "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[220] Thus, as previously discussed, MRPC Rule 1.1 provides no requisite mental limitations for competent representation, perhaps inferring the broader reach of the MRPC.[221] Consequently, a lawyer who fails to take reasonable care to investigate the risks involved with a particular cloud provider

217. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R.1.1 (2011).

218. Black's Law Dictionary defines the word "knowingly" as "with knowledge; consciously; intelligently; willfully; intentionally. An individual acts 'knowingly' when he acts with awareness of the nature of his conduct." BLACK'S LAW DICTIONARY 827 (6th ed. 1991). Courts use a similar definition of the term "knowingly" in civil cases. *See, e.g.*, Baywood Elec. Corp. v. N.Y. State Dep't of Labor, 649 N.Y.S.2d 28, 30 (N.Y. App. Div. 1996) (defining "knowingly" as when the accused "knew or should have known" that he or she was committing a violation).

219. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.3(a)–(b) (2011).

220. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2007).

221. *See supra* Part III.

might similarly have violated MRPC Rule 1.1. As a result, lawyers or firms seeking to utilize cloud providers must review the vendors to ensure that their services are both reliable and secure.

vi. Considerations and Precautions

Lawyers and law firms may need to choose between 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 use of a public cloud should conduct a thorough due diligence review of the cloud service provider. The review might examine the service provider in light of the inherent risks of any public cloud. Such a review also might 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 was outsourcing storage of hard copy to a domestic or overseas warehouse, it would be prudent to question the warehouse operator about its experience with an inability to provide access to documents on short notice. Similarly, a law firm should question a cloud provider about all outages it has experienced, what back-up copies it makes (if any), and 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.[222] The firm also should negotiate terms of service that require the cloud vendor to assist the firm in fulfilling its duties to collect, preserve, and produce a client's electronic records under applicable e-discovery rules.

It may appear unrealistic to expect that major cloud providers such as Google, Microsoft, IBM, and Amazon will cooperate with any request for such a due diligence review and negotiate terms of service based on that review's findings. However, if law firms were to weigh the risks to their clients, their reputations, and their compliance with the NYRPC or the MRPC, the need to conduct a due diligence review could appear compelling. In addition, a cloud vendor's refusal to assist counsel in fulfilling its e-discovery obligations could expose lawyers and clients to sanctions.

---

222. *See, e.g.*, Contract Between the City of Los Angeles and Computer Science Corporation for the SAAS E-Mail and Collaboration Solution (SECS), City of L.A. Inter-Departmental Correspondence (Oct. 2, 2009), *available at* http://www.infolawgroup.com/uploads/file/City%20of%20Los%20Angeles%20and%20CSC-Google%20Contract%281%29.pdf (explaining prudent procedures regarding the implementation of a cloud computing system).

Moreover, the New York State Bar Association's Committee on Professional Ethics (NYSBA 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."[223] Complying with the guidance in the NYSBA's 2008 opinion will now be particularly difficult because Yahoo! and Google use or have used terms of service that allow them to scan the contents of outgoing and incoming e-mails.[224] 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.

Similarly, the ABA has cautioned lawyers to investigate the security of a provider's premises and network before outsourcing any client services.[225] Particularly where confidential information is at stake, a lawyer must "recognize and minimize" the risk that a service provider could reveal client information to unauthorized parties.[226] The ABA opinion suggests that a written confidentiality agreement be drafted to prevent wrongful disclosure—a precaution that might be difficult if utilizing the services of a large cloud provider.[227]

---

223. New York State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 820 (2008), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&Template=/CM/ContentDisplay.cfm&ContentID=40117.

224. *Terms of Service*, YAHOO!, ¶ 6, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last updated Nov. 24, 2008); *Google Terms of Service*, GOOGLE ¶¶ 11.1, 11.2, http://www.google.com/accounts/TOS (last visited Oct. 20, 2011); *Privacy Policy*, GOOGLE, http://www.google.com/privacy/privacy-policy.html (last updated Oct. 3, 2010). For analysis of these types of content licenses and policies, see *Yahoo Amends Ts and Cs to Scan and Analyse Users' Emails*, COMPUTER ACT!IVE (Aug. 7, 2011), http://www.computeractive.co.uk/ca/news/2091488/yahoo-amends-ts-cs-scan-analyse-users-emails; *Google's Scan of User E-mail: Fair or Creepy?*, CROSSCUT.COM (Nov. 18, 2007), http:crosscut.com/2007/11/18/seattle/9222/Google-s-scan-of-user-e-mail:-fair-or-creepy-.

225. ABA Formal Op. 08-451, *supra* note 94.

226. *Id.*

227. *Id.* The ABA Opinion emphasizes that "[w]ritten confidentiality agreements are, therefore, strongly advisable in outsourcing relationships." *Id.* However, the ABA Opinion adds a recommendation that would be difficult for major customer law firms to follow if the same cloud vendor provided services to even a few of the largest United States based law firms: "Likewise, to minimize the risk of potentially wrongful disclosure, the outsourcing lawyer should verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters; in such an instance, the outsourcing lawyer could choose another provider." *Id.* If the ABA continues to hold that view, then it would appear that the reasonable inference to be drawn is that it may well be impracticable for large law firms, if not any law firms, to store client

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 MRPC Rule 1.1 or the NYRPC Rule 1.1(c)(2) to avoid intentionally damaging a client's interests.

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.[228] Selection of a trustworthy e-mail service provider may not have averted such mistakes, but such mistakes are

---

confidential data with a major cloud computing service provider and to follow the ABA Opinion's recommendation.

228. As John Barkett perceptively observed:

> I do not know of a lawyer who has not suffered from Microsoft Outlook's propensity automatically to fill in the e-mail address of a recipient for a sender in a hurry who types a couple of letters of a name and then does not scroll down for the list of potential recipients to identify the intended addressee. This failure to protect a client confidence is usually immediately remedied by the recipient who responds: "I don't think you intended this e-mail for me. I am immediately destroying it." After sending a "thank you" e-mail, the sender will resolve to be more careful: After all, Rule 1.6 is prescriptive unless the lawyer has received the client's informed consent to make the disclosure.

JOHN M. BARKETT, THE ETHICS OF E-DISCOVERY 43 (2009). There are several examples of irreversible mistakes which led to a waiver of privilege because counsel did not verify whether the client had a reasonable expectation of privacy in e-mail communications sent to counsel from the client's place of employment. *See* Stengart v. Loving Care Agency, Inc., No. BER-L-858-08, 2009 WL 798044 (N.J. Super. Ct. Law Div. Feb. 5, 2009) ("[W]hen an employee sends an E-mail to their attorney through an E-mail account issued by their employer over their employer's servers, several courts have found that such correspondence is generally not protected by the attorney client privilege if the employer maintains a policy warning its employees that E-mail correspondence from company issued E-mail accounts are subject to review."); *see also* Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436 (Sup. Ct. 2007) (holding that e-mails between a hospital employee and his personal attorneys were not privileged because employer's policy regarding computer use and e-mail monitoring stated that employees had no reasonable expectation of privacy in e-mails sent over the employer's e-mail server); *In re* Asia Global Crossing, Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005) (holding a party waived any attorney-client privilege they had with respect to e-mail communications between themselves and their attorneys by sending communications to a third party, but requiring additional facts regarding the existence of a policy against personal use of a corporation's e-mail system or the existence of a policy of monitoring employee e-mail before deciding the question of whether the party waived their attorney-client privilege in that regard); Kaufman v. SunGard Invest. Sys., No. 05-cv-1236, 2006 U.S. Dist. LEXIS 28149 (D.N.J. May 9, 2006).

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. Sending an e-mail to the wrong recipient, which almost every e-mail user has done, is an example of this type of error. 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, serious and potentially costly errors, 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 to 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.[229] 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.[230] Because counsel often corresponds by e-mail 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. Because security risks and risks from breaches of confidentiality from use of public clouds could be even greater than those experienced with e-mail, the lessons learned from

229. *See, e.g.*, Joseph R. Chenelly, *Misdirected Email Doomed Convoy*, MILITARY.COM (Apr. 9, 2008), http://www.military.com/news/article/misdirected-email-doomed-convoy.html (explaining how a misdirected e-mail sent an unarmored convoy into a deadly fighting zone, leaving seventeen dead).

230. *See generally* Katherine Eban, *Lilly's $1 Billion E-Mailstrom*, PORTFOLIO.COM (Feb. 5, 2008), http://www.portfolio.com/news-markets/top-5/2008/02/05/Eli-Lilly-E-Mail-to-New-York-Times (providing an illustrative example of a confidential e-mail misdirected to an individual with the same surname as the intended recipient). Indeed, as this article was in its final drafting, one of the authors received a misdirected e-mail from a former employee of an organization on whose board the recipient serves that contained information personal to the employee.

adoption of e-mail technologies should be viewed as useful, but less than the minimum, precautions a law firm should take when deciding whether and when or to what extent 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 Representation" (Opinion 2008-1).[231] 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.[232]

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."[233] 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."[234] But it added an important caution: "From an ethical standpoint, a lawyer should ensure that

231. THE ASS'N OF THE BAR OF THE CITY OF NEW YORK, COMM. ON PROF'L AND JUDICIAL ETHICS, Formal Op. 2008-1 (2008) [hereinafter ABCNY Opinion 2008-1], *available at* http://www.nycbar.org/ethics/ethics-opinions-local/2008-opinions/799-a-lawyers-ethical-obligations-to-retain-and-to-provide-a-client-with-electronic-documents-relating-to-a-representation-.

232. *Id.* pt. 1.

233. *Id.*

234. *Id.* pt. 3.

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."[235]

Because public clouds have been temporarily shut down,[236] and the risks of additional shutdowns will likely persist, and possibly grow, if the occurrences of cyberattacks increase, law firms arguably should not rely incautiously on a public cloud. Law firms already should know not to rely solely on storage of electronic records on 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 fail to take 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.
>
> While we can't give you exact figures, please be assured that we back up data almost as often as you can change it.[237]

---

235. *Id.*

236. *See supra* note 50.

237. *Save Your Documents*, GOOGLE, http://docs.google.com/support/bin/answer.py?hl=en&answer=44665&topic=1360900 (last visited Oct. 20, 2011). Google 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." Google substituted the following: "Your presentation will begin saving within Google Docs almost as soon as you begin entering text." *Create and Save a Presentation*, GOOGLE , http://docs.google.com/support/bin/answer

In light of the potential ethical issues, including the problem noted below, that can arise if a cloud computing service agreement places the responsibility for security of a customer's data on the individual or organization that sent the information to the cloud, 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

.py?hl=en&answer=69074 (last visited Oct. 20, 2011). The authors found no redline of the changes to such descriptions or to Google's Terms of Service. Thus, only by printing and saving the Terms of Service at a moment in time would users be able to trace changes in the master agreement most users have with Google.

> of retention, storage, and retrieval of electronic documents to which a client has a presumptive right of access.[238]

Even stronger cautions appear in the California State Bar Opinion No. 2010-179 (Opinion No. 2010-179) on the need to inform clients when use of technology may result in a heightened risk to their data. The opinion examined an attorney's duties when using technology to transmit or store confidential client information when such technology "may be susceptible to unauthorized access by third parties," describing that "[t]he greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent."[239]

Among the risks to its data that should be reviewed with a client is that of an inadvertent disclosure of privileged or confidential information or work product that might result in a court deciding that such disclosure waived the applicable attorney-client or attorney work product privilege. Moreover, as Opinion No. 2010-179 noted, even the mere use of an insufficiently secure technology without a disclosure could be deemed to have waived the privilege:

> [I]t is possible that, if a particular technology lacks essential security features, use of such a technology could be deemed to have waived these protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining waiver. Further, the analysis differs with regard to an attorney's duty of confidentiality. Harm from waiver of attorney-client privilege is possible depending on if and how the

238. ABCNY Opinion 2008-1, *supra* note 231, pt. 6 (emphasis added). The Opinion concludes: "In New York, a client has a presumptive right to the lawyer's entire file in connection with a representation, subject to narrow exceptions." *Id.*

239. To clarify what it meant by "informed consent," California State Bar Opinion No. 2010-179 explained in a footnote that:

> For the client's consent to be informed, the attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal), and any other facts that may be important to the client's decision . . . . It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.

California Formal Op. 2010–179, *supra* note 130, at 5 n.15.

> information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed.[240]

Prior to 2010, although some state bar associations had issued ethics opinions on issues related to a lawyer's storage of client data in a cloud computing platform,[241] no New York ethics opinion had issued guidance on the ethics of storing client confidential information online, which includes storing information in a cloud computing vendor's off-site servers where it would be accessible wirelessly. Lawyers and law firms subject to the NYRPC will find instructive the New York State Bar Association (NYSBA) Committee on Professional Ethics' Opinion 842 (Opinion 842), issued on September 10, 2010. The opinion addresses whether a lawyer may "use an online system to store a client's confidential information without violating the duty of confidentiality or any other duty," and if so, what steps the lawyer should take to "ensure that the information is sufficiently secure."[242] Opinion 842 concluded that a lawyer "may use an online 'cloud' computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the [cloud vendor's] system is secure and that client confidentiality will be maintained."[243]

Although that conclusion, as stated, may appear to require that "reasonable care" under NYRPC Rule 1.6 must guarantee "that client confidentiality will be maintained[,]" that was not the Committee's intended guidance as reflected in its explanation that "exercising 'reasonable care' under Rule 1.6 does not mean that the lawyer guarantees that the information is secure from *any* unauthorized access."[244] Of particular value is the Committee's identification of the steps that a lawyer may take to protect client confidential information against unauthorized disclosure, including:

---

240. *Id.* at 6 (footnotes omitted).

241. Such ethics opinions include the following: Alabama State Bar Ass'n, Formal Op. 2010–02, *supra* note 138; California Formal Op. 2010–179, *supra* note 130; Nevada State Bar Ass'n Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references /ABA10a/PDfs/3_12.pdf (last visited Oct. 20, 2011).

242. New York Op. 842, *supra* note 94.

243. *Id.* ¶ 9.

244. *Id.* ¶ 5.

- Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security . . . .;
- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored[.][245]

Lawyers, however, will probably in the near future find it a significant challenge to follow the Committee's recommendation that the data storage provider have "an enforceable obligation to preserve confidentiality and security."

There are *at least three significant obstacles to overcome* in order to fulfill that obligation in negotiation of a cloud computing service level agreement with a major vendor. The *first obstacle is identification and understanding of the vulnerability points in a cloud platform's structure and processes*; such vulnerability points may be in the cloud vendor's servers, the data customer's computers and networks, or in the communication between those two systems.

The *second obstacle is determining whether the cloud computing service vendor or the data customer is ultimately responsible for security under the terms of their service level agreement.* Although marketing language on a vendor's website will usually offer assurances concerning the security of data stored on its cloud servers, a careful examination of the vendor's standard service level agreement usually reveals that the vendor disclaims responsibility and declares it the data customer's responsibility. For example, Amazon offers the following assurance concerning security of its EC2 cloud service: "Secure – Amazon EC2 provides numerous mechanisms for securing your computer resources"[246] and Amazon supports that assurance with a referral to a link to its security white paper, entitled *Amazon Web Services: Overview of Security Process.*[247] However, those assurances are undercut and the responsibility for security is firmly placed on the data customer by the standard Amazon Web Services Customer Agreement, which asserts that while Amazon "will implement reasonable and appropriate measures designed to *help you secure Your Content against accidental or unlawful loss, access or*

245. *Id.* ¶ 9.
246. *Amazon Elastic Computer Cloud (Amazon EC2)*, *supra* note 155.
247. *Id.*

disclosure,"[248] the ultimate responsibility for security rests with you—the data customer:

> **4. Your Responsibilities**
>
> . . . .
>
> **4.2 Other Security and Backup.** You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content.[249]

Amazon is not unique among cloud computing vendors in its insistence that the data customer accept responsibility for security of its data stored on Amazon's cloud servers that Amazon has exclusive custody of and over which Amazon exercises exclusive control. Although it may seem paradoxical that cloud service vendors offer to be bailees of a data customer's digital assets and yet refuse to be responsible for the security of such data while in their servers, on their premises, and under their control, that appears to be the emerging standard (at least for data customers who lack the leverage to negotiate a different allocation of responsibilities for data security). One of the major criticisms directed at cloud vendors in the aftermath of the data security incidents in the second quarter of 2011 is the insufficiency of security provided by the cloud vendors for the customer's data:

> The biggest complaint in the wake of recent data breaches, whether it's Sony or Epsilon, has centered on the lack of security controls in place to protect customer data. A recent Ponemon Institute report found that cloud providers don't think that's their job.
>
> A shocking 73 percent of U.S. service providers and 75 percent of their European counterparts said their cloud services did not substantially protect and secure their customers' confidential or sensitive information, according to the recent Security of Cloud Computing Providers report from the Ponemon Institute. Nearly 62 percent of U.S. providers and 63 percent of European providers were not confident that their cloud applications and resources were secure.

---

248. *Amazon Web Services Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement (last updated Aug. 23, 2011) (emphasis added) [hereinafter *August 2011 AWS Customer Agreement*].

249. *Id.* § 4.2.

> . . . .
>
> A majority of the surveyed [cloud] vendors don't even have dedicated security personnel to oversee the security of their applications, infrastructure or platform, the report found. On average, providers allocated 10 percent or less of their resources to address security.[250]

Such findings suggest that obtaining an enforceable agreement from a cloud service vendor to be responsible for the security of a customer's data could prove a formidable challenge.

The *third obstacle is that cloud computing vendors tend to include in their service level agreements the right to suspend a customer's access to its data as a remedy triggered by the vendor's sole determination that the data customer is the source of a security risk.*[251] Although suspending a customer's access to its data does not constitute a direct violation of the confidentiality and security of such data, it renders both concepts rather hollow since the same agreement both makes the customer responsible for security of its data in the cloud computing vendor's servers and gives the vendor the right to suspend customer access to such data, making it impossible thereafter for the customer to monitor or otherwise protect such data. An example of such a provision, in the August 2011 Amazon Web Services Agreement, states:

> We may suspend your or any End User's right to access or use any portion or all of the Service Offerings immediately upon notice to you if we determine: (a) your or an End User's use of the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) may adversely impact the Service Offerings or the systems or Content of any other AWS customer, or (iii) may subject us, our affiliates, or any third party to liability . . . .[252]

A noteworthy omission from such agreements further compounds the problem: there is no undertaking by the cloud computing vendor that it will provide the data customer with any notice of a security breach that might have affected the customer's

250. Fahmida Y. Rashid, *Cloud Service Providers Say Data Security 'Not My Job': Study*, EWEEK (May 7, 2011), http://www.eweek.com/c/a/Security/Cloud-Service-Providers-Say-Data-Security-Not-My-Job-Study-381728 (noting that cloud providers are in the business of giving their customers what they want).

251. *See, e.g.*, *Legal Cloud Services Agreement*, LOGICWORKS, § 4, http://www.logicworks.net/legal/cloud-services-agreement (last visited Oct. 20, 2011) (giving the vendor the right to suspend the customer's access to his or her own data).

252. *August 2011 AWS Customer Agreement*, *supra* note 248, § 6.1(a).

data.[253] As a result, there is also no requirement that the vendor alert the customer to the need to take precautions to protect its data or its enterprise from unauthorized use of its data or that the vendor give the customer any information of the kind of attack, the vulnerability it exploited, or other information that would be crucial to a customer. The precautions are not only for the data protection, but in order to ensure that it complies with applicable laws and regulations that might require it to give notice to third parties that their data too may have been affected by the security breach.[254] Also omitted from cloud service agreements are any grants of rights to the data customer to audit the vendor's maintenance of security or to gain access to the vendor's premises and to interview its staff in order to investigate a security breach.

If such serious omissions are not corrected in the negotiated definitive service agreement between a cloud computing vendor and a lawyer or law firm, then counsel may find it difficult, if not impossible, to fulfill other important obligations required by Opinion 842 which cautions:

> [T]he lawyer should periodically reconfirm that the [cloud] provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.[255]

In that passage, the standards set for a New York lawyer or law firm would appear to be significantly higher than those described in the ethics opinions on cloud computing by other states' bar associations, the ABA, and the ABA Commission on Ethics 20/20.[256]

---

253. *See, e.g.*, *id.* (illustrating that the vendor does not have to inform its customer of a security breach).

254. *Cf.* Peter Fretty, *Turbulence in the Clouds*, PETERFRETTY.COM (Feb. 25, 2011), http://www.peterfretty.com/2011/02/25/turbulence-in-the-clouds (explaining precautions taken by cloud computing vendors and the purpose of these precautions).

255. New York Op. 842, *supra* note 94, ¶ 10.

256. *See Cloud Computing Among Issues of Ethics 20/20 Hearing in Atlanta*, ABA (Feb. 12, 2011), http://www.abanow.org/2011/02/cloud-computing-among-

The obligations to ensure that counsel receive prompt notice of a security breach, that counsel can effectively investigate such breach, and that counsel "discontinue use of the service" if the vendor fails to provide assurances that "any security issues have been sufficiently remediated" arguably create a potential Armageddon scenario if counsel have not negotiated a cloud computing service agreement that contains provisions that would avert such an outcome.[257] Moreover, the considerable disruption of work and the resulting financial and reputational costs that would ensue from counsel having to discontinue use of cloud computing services (and notifying any affected clients) after having become dependent upon such services would appear to set a very high entry barrier for New York lawyers and law firms that might be considering moving client confidential data from onsite computers to a cloud computing server. We doubt whether fulfillment of Ethics Opinion 842 obligations would be possible under the customer service agreements that cloud computing service vendors currently have posted on their web sites as their standard terms and conditions. Therefore, if a lawyer or law firm does not negotiate appropriate modifications of such agreements to ensure that they have the means to achieve such compliance, they would appear to be putting themselves in potential conflict with their ethical obligations under the NYRPC rules as interpreted by Ethics Opinion 842.[258] However, it should also be noted that Ethics Opinion 842 might also provide a lawyer or law firm with leverage in negotiations with a cloud computing vendor, since such opinion could be cited as an applicable standard that a vendor would need to ensure that a data customer lawyer or law firm could fulfill under any definitive cloud computing service level agreement.

Continued occurrences of data breaches that affect cloud computing services would probably also further raise the ethical entry barrier for New York lawyers and law firms—and for counsel practicing in other jurisdictions that decide to follow or incorporate the obligations set forth in Ethics Opinion 842. Moreover, Ethics Opinion 842 does not address, and thus leaves unclear, whether the ethical obligations it identifies apply also to in-house counsel of government agencies, companies, and financial institutions (such as the New York Federal Reserve Bank) whose

issues-of-ethics-2020-hearing-in-atlanta.

257. *See* Rebecca S. Eisner, *Clear Skies or Stormy Weather for Cloud Computing: Key Issues in Contracting for Cloud Computing Services*, 1060 PLI/Pat 393 (2011).

258. *See, e.g.*, N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.2 (2011).

offices are located within New York state.[259] To what extent are such counsels subject to, or relieved of, obligations identified by Ethics Opinion 842 if their employers decide, without consulting them, to move the enterprise's confidential data to a cloud computing vendor's servers? Clarification of such issues in a future NYSBA Ethics Opinion would help avert confusion at a time when many enterprises are attempting to decide when, and to what extent, to move data of varying sensitivities to the cloud.

c. 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.[260] The law firm's partners can require their IT staff to report fully and promptly any problems they have found, but depending on the cloud service agreement such reports may not be available on demand, or contain complete or sufficiently 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 important to trace to its cause as such losses occur briefly but repeatedly.[261]

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 make the cloud increasingly likely to have vulnerabilities and the rich store of sensitive data in the cloud is a highly attractive target for cyber-exploitation.[262] John Harauz explains the cloud architecture vulnerabilities as follows:

Clouds can comprise multiple entities, and in such a

259. *See* New York Op. 842, *supra* note 94.

260. *See* Matthew A. Verga, *Cloudburst: What Does Cloud Computing Mean to Lawyers*, 5 J. LEGAL TECH. RISK MGMT. 41, 46 (2010) ("Depending on the service provider chosen and the configuration of its facilities, the data could be in one facility or several, and the facilities could be almost anywhere in the world. Where the data is located will dictate the laws to which it is subject.").

261. *See, e.g.*, Jack Newton, *Putting Your Practice in the Cloud a Pre-Flight Checklist*, 73 TEX. B.J. 632 (2010).

262. *See, e.g.*, Harauz, Kaufman & Potter, *supra* note 146, at 63 (discussing that if a cybercriminal finds out the identity of a vulnerable cloud computing provider, then it becomes an easy target).

> 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.[263]

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 multiply 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.[264]

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 . . . ."):[265]

---

263. *See id.*

264. COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 157–58 (William A. Owens et al. eds., 2009), *available at* http://books.nap.edu/openbook.php?record_id=12651&page=R1.

265. *Id.* at IX. The report explains:

> Cyberexploitations do not seek to disturb 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

> 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 activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year.[266]

i. 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 adverse consequences and to avert reoccurrences. The diminished ability to mitigate and avert consequences and reoccurrences may implicate a law firm's ability to provide competent representation.[267]

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. For example, the 2009 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

---

compromise.

Id. at 11, 151.

266. DENNIS C. BLAIR, ANNUAL THREAT ASSESSMENT OF THE INTELLIGENCE COMMITTEE FOR THE SENATE SELECT COMMITTEE ON INTELLIGENCE, 39 (Feb. 12, 2009), *available at* http://intelligence.senate.gov/090212/blair.pdf.

267. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2007).

> YOU AS PART OF THE SERVICES WILL BE CORRECTED.[268]

The 2011 text of the same section 14.3 replicates the warranties from 2009.[269]

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.[270] 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 Google to attempt to correct faults or defects or any right to require Google to attempt to mitigate the damage to the law firm customer.[271] 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"[272] and Rule 1.1(c) to "not intentionally . . . prejudice or damage the client during the course of the representation,"[273] 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.

MRPC Rule 1.1's competency requirement provides an obligation analogous to that in NYRPC Rule 1.1(a).[274] Providing competent representation appears to require a law firm to ensure

---

268. *Google Terms of Service*, GOOGLE, § 14.3(c)–(d) (Apr. 16, 2007), http://www.google.com/accounts/TOS [hereinafter *2011 Google Terms of Service*].

269. *See supra* text accompanying note 237.

270. *See supra* text accompanying note 237; *Google Terms of Service*, GOOGLE, § 14 (Feb. 24, 2009), http://www.tosback.org/version.php?vid=134 [hereinafter *2009 Google Terms of Service*].

271. *2011 Google Terms of Service*, *supra* note 268.

272. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.1(a) (2011).

273. *Id.* R. 1.1(c).

274. *Id.* R. 1.1(a).

that the technologies it utilizes do not hinder a client's objectives through technological faults. The inability to correct functional flaws in a cloud system, particularly those that are recurring, arguably detracts from the lawyer's effectiveness and ultimately could harm the client's fiduciary interests by imposing additional costs or by delaying action necessary to the advancement of the case.

Similarly, NYRPC Rule 1.1(c) may find an analogue in MRPC Rule 1.3's diligence requirement. MRPC Rule 1.3 requires a lawyer to act with "reasonable diligence" in representing a client.[275] Diligence requires a lawyer to pursue a client's interests despite any obstacles that may arise.[276] The essence of MRPC Rule 1.3 is that lawyers take "whatever lawful and ethical measures are required" to ensure that the client's objectives are achieved and to ensure that the client is not prejudiced through the lawyer's dilatory actions. Arguably, an inability to control the technology through which client information is processed could be construed as a failure to pursue the client's interests through the lawful means available to the lawyer.

ii. 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 also might 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, and without notice to the customer*. Some terms of use or terms of service, such as those for Google Docs, not only claim the right to vary the terms unilaterally, but also to treat the continued use of the service after such changes as acceptance of those changes even though a customer may not have been aware of the change because posting of such changes is not accompanied by any e-mail notice to the users.[277] A law firm

275. MODEL RULES OF PROF'L CONDUCT R. 1.3 (2007).
276. *See id.* R. 1.3 cmt. 1.
277. *2011 Google Terms of Service*, *supra* note 268, § 19.2.

entering into standard Terms of Use for a public cloud software service that gave such rights to the cloud provider might 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).

The Terms of Service for Google Docs 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.*"[278]

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, law firms should infer from the quoted provisions a near certainty 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 terms of service, much more compelling.

In addition, lawyers and firms should negotiate specifically with the cloud provider over rights upon termination of their relationship. Will the lawyer or firm be assured that all electronic

278. *2011 Google Terms of Service*, *supra* note 268, §§ 4.2–4.4 (emphasis added). These terms are identical in text and formatting to the 2009 version. *2009 Google Terms of Service*, *supra* note 270, §§ 4.2–4.4.

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 [a] 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.[279]

Without special provisions, there is no assurance of retrieval of documents stored in Google Docs at the time of termination, or any assurance regarding Google's responsibility concerning the purge of records after termination.

The City of Los Angeles negotiated a cloud service contract with Google. An October 7, 2009 final draft is available. The draft covers some of the contingencies discussed and negotiations suggested in this article.[280] Thus, we conclude that, with the negotiating resources of a major city and possibly of other large enterprises, Google may make more favorable terms available to customers.

Another cloud provider, Amazon, has made numerous changes to its terms of service on the subjects of post-termination services and the retrieval of electronic records in its "Amazon Web Services™ Customer Agreement" (Amazon Agreement) that governs its "Amazon Elastic Compute Cloud" (Amazon EC 2).[281]

---

279. *2011 Google Terms of Service*, *supra* note 268, §13.3.

280. Memorandum from Miguel A. Santana, City Admin. Officer, City of Los Angeles, to Chair, Budget and Fin. Comm. 9 (Oct. 2, 2009), *available at* http://www.infolawgroup.com/uploads/file/City%20of%20Los%20Angeles%20and%20CSC-Google%20Contract%281%29.pdf.

281. *Compare AWS Customer Agreement*, AMAZON WEB SERVICES, §§ 6.2(d), 7.3(b), http://web.archive.org/web/20110703131958/http://aws.amazon.com/agreement (last updated May 23, 2011) [hereinafter *May 2011 AWS Customer Agreement*] (stating that in the event of suspension, Amazon will "not erase any of Your Content . . . except as specified elsewhere in this Agreement"; and in the event of termination other than for cause, Amazon will not "erase any of Your Content" during the thirty days following termination, and undertakes to allow retrieval of

However, the Amazon Agreement only provides for preservation of data stored on Amazon EC 2 if the suspension or termination is "other than for cause."[282] The October 2010 Amazon Agreement provided, to those terminated other than for cause, 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.[283]

In the October 2010 version of the Amazon Agreement, customers suspended or terminated for cause could read a starker warning in section 3.7.3 that Amazon would "have no obligation to continue to store your data during any period of suspension or termination or to permit you to retrieve the same." That warning is omitted from the August 2011 version of the Agreement, which merely states: "[A]ll your rights under this Agreement immediately terminate."[284]

From the provisions of the October 2010 and later versions of the Amazon Agreement cited immediately above, the authors infer all of the following:

- Amazon has changed its commitment from one promising that it will not "intentionally erase" a customer's data after an other-than-for-cause termination, to one that more forcefully promises not to erase data. In neither the October 2010 nor August 2011 versions of the Agreement does Amazon give assurance that it will take precautions to *protect* such data or to ensure that post-termination protection will be equal or in any way comparable to pre-termination protection.
- Post-termination "retrieval of data stored" in the cloud is not

---

content only on payment of charges for post-termination use and other amounts due and to provide "the same post termination data retrieval assistance that we generally make available to all customers"), *with August 2011 AWS Customer Agreement*, *supra* note 248, §§ 6.2(d), 7.3(b). Implicit in the preamble to section 7.3(a) and (b), respectively, is the fact that termination can be "immediately upon notice to you [the customer]." *May 2011 AWS Customer Agreement*, *supra*.

282. *AWS Customer Agreement*, AMAZON WEB SERVICES § 3.7.2, http://web.archive.org/web/20101029051446/http:/aws.amazon.com/agreement (last updated Oct. 21, 2010) [hereinafter *October 2010 AWS Customer Agreement*]; *August 2011 AWS Customer Agreement*, *supra* note 248, § 7.3(b).

283. *October 2010 AWS Customer Agreement*, *supra* note 282, § 3.7.2.

284. *August 2011 AWS Customer Agreement*, *supra* note 248, § 7.3(a)(i).

unconditional even in terminations other than for cause. It is conceivable in the October 2010 and August 2011 versions of the Agreement on payment of Service, data storage charges post-termination, 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.[285]

- If Amazon elects to terminate the service, it makes no commitments to keeping stored data whatsoever or to allow any retrieval of data. Customers might lose data while they attempt to cure the causes that led to the termination.
- If a law firm customer urgently needed to retrieve client-related data shortly following termination of the cloud service, even if the law firm was 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).[286] A law firm should consider carefully whether it is a reasonable, and reasonably defensible, risk to entrust a 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.

These are not speculative concerns even in the absence of intentional suspension or termination. As revealed by the 2011 interruption of service that Amazon suffered, some cloud customers were unable to access their data and others suffered a permanent loss of data.[287] Moreover, whether a client's data should be stored where the bailee could hold it a virtual hostage or imperil its recovery is a troubling proposition. Lawyers and law firms may want to address these potential risks in order to avert the possibility of an ethical issue arising under the NYRPC requirements for

285. *E.g.*, *id.* § 7.3(a)(ii); *October 2010 AWS Customer Agreement*, *supra* note 282, § 3.7.2.

286. *October 2010 AWS Customer Agreement*, *supra* note 282, §3.7.2.

287. Blodget, *supra* note 100 (describing how data loss resulting from reliance on cloud service providers is catastrophic for small firms).

competent representation and avoidance of damage to a client. Thus, some lawyers or law firms might find the failure to reach an agreement on the handling of such issues a deal breaker with the cloud vendor. Furthermore, if a law firm accepts a cloud vendor's standard service agreement, the firm needs to address the risk that vendors typically reserve the right to change the terms of their service agreements at any time without prior notice to the customer, which could leave a law firm dissatisfied with the protections as to its clients' confidential data.[288]

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 imperil a contractually compliant law firm if *its client's* data become indefinitely inaccessible: "In the Event of [a termination for cause, 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."[289]

The Amazon Agreement uses control over the continued storage and retrieval of data as collateral to protect its interests without limitation.[290] A law firm may endeavor to renegotiate such terms and should give consideration to disclosing the resulting arrangement with its clients so that the clients may 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 client documents on its premises in its own computers or digital storage media, the ethical risks relating to competent representation would diminish substantially.

On-premises backups do not address the other ethical issues inherent in the arrangement proposed by the Amazon Agreement. The agreement does not mention in the termination clauses any post-termination obligation to either prevent unauthorized access to data stored on its cloud by a terminated customer, or to purge all copies of such data if a customer requests it (for example, where destruction of previously disclosed litigation material is required by

288. *See, e.g.*, *August 2011 AWS Customer Agreement*, *supra* note 248, §§ 2.1–2.3, 12.

289. *October 2010 AWS Customer Agreement*, *supra* note 282, § 3.7.3. The companion provision in the 2009 version was section 3.7.3. *See AWS Customer Agreement*, AMAZON WEB SERVICES, http://web.archive.org/web/ 20090804041357 /http://aws.amazon.com/agreement (last updated July 9, 2009).

290. *October 2010 AWS Customer Agreement*, *supra* note 282, § 3.7.

settlement agreement).[291]

iii. Risks of Noncompliance with E-Discovery Obligations

Damage to or loss of client data and documents stored in a public cloud can pose an additional ethical risk where the client and his or her counsel reasonably anticipate that the client may be the subject of a federal government investigation or a party to litigation in federal courts, thereby possibly incurring a duty under the Federal Rules of Civil Procedure 26 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.[292] 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 imposes sanctions for spoliation, serious damage to the client's interests as well as those of the firm can result.

To understand the risks involved, suppose an adversary raises a spoliation claim as to documents, stored in a public cloud, 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 the court ordered the client to permit an adversary, an adversary's expert, or a government agent to make a "mirror image" of hard drives containing the potentially relevant data and documents, and 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 Federal Rules of Civil Procedure Rule 37 (Failure to Make Disclosures or to Cooperate in Discovery; Sanctions), 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

291. *Id.* § 3.

292. F. Brenden Coller, *I'm Responsible to Do what? Counsel's Affirmative Duty to Ensure Compliance with Litigation Holds*, E-DISCOVERY L. REV. (Aug. 18, 2011), http://www.ediscoverylawreview.com/2011/08/articles/im-responsible-to-do-what-counsels-affirmative-duty-to-ensure-compliance-with-litigation-holds ("[C]ourts all over the country have emphasized the duty placed on counsel—both in-house and outside—to ensure that clients comply with their discovery obligations.").

potentially accessible to third parties and government agents?

There appears to be a reasonable possibility of other serious logistical problems—for counsel and their clients—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.[293] 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 court orders that a party deliver a "mirror image" of records stored at a specific location, would the 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, during the first nine months of 2011, Soonr's Terms of Service and End User License Agreement provision on termination arguably intensified these risks. The relevant Soonr contract provisions stated:

> 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.[294]

Law firms might find it useful to consider such scenarios and

293. EUROPEAN NETWORK AND INFO. SEC. AGENCY, CLOUD COMPUTING: BENEFITS, RISKS, AND RECOMMENDATIONS FOR INFORMATION SECURITY, 9–11 (Nov. 2009), *available at* http://www.enisa.europa.eu/act/rm/files/ deliverables/cloud-computing-risk-assessment/at_download/fullReport. For an excellent analysis of these issues and related e-discovery decisions, see John M. Barkett, *Zubulake Revisited:* Pension Committee *and the Duty to Preserve* (2010), http://apps.americanbar.org/litigation/litigationnews/trial_skills/docs/pension-committee-zubulake.pdf.

294. *Soonr Terms of Service and End User License Agreement*, SOONR, § 10.3, http://www.soonr.com/security/eula.html (last visited Aug. 24, 2011). The terms of Soonr's Terms of Service and End User License Agreement, as well as its privacy policy, all changed in August 2011, during the editing of this article.

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.[295] A lawyer or law firm also might 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."[296]

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:

> YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE . . . SHALL NOT BE LIABLE TO YOU FOR . . . ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF . . . THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER COMMUNICATIONS DATA MAINTAINED OR TRANSMITTED BY OR THROUGH YOUR USE OF THE SERVICES.[297]

The Amazon Agreement provides:

> 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 . . . . We strongly encourage you, where available and appropriate, to . . . use encryption technology to protect Your Content from unauthorized access [and] routinely archive Your Content . . . . We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content.[298]

---

295. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.1(c)(2) (2011).
296. *Id.*, § 1200 R. 1.4(a)(2).
297. *2011 Google Terms of Service*, *supra* note 268, § 15.1(B)(III).
298. *October 2010 AWS Customer Agreement*, *supra* note 282, § 7.2.

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 on a public cloud, the "litigation hold" preparations and discussions may be aided by considering the issues that could arise from efforts to preserve and to produce records on the public cloud. Such ethical issues may persist, and we return to them later in the discussion of other security risks.

d. 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 (1) such code will be installed, (2) certain problems are known to be likely to occur with certain existing programs, or (3) after installation certain problems have been found to have resulted. Indeed, cloud providers and their supporters 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.[299] However, the service level agreements of the major

299. *Top Ten Advantages of Google's Cloud*, GOOGLE, http://www.google.com /apps/intl/en/business/cloud.html (last visited Oct. 20, 2011). Microsoft, for example, touts as a benefit of its Azure cloud platform that "[c]ustomers and partners can focus on delivering services and value to their customers—and not on managing technology infrastructure," which includes, by necessity, patching. *Windows Azure Platform FAQs,* WINDOWS AZURE, http://www.microsoft.com

cloud vendors do not, at present, promise that all customers will receive each security patch simultaneously, and in the absence of such promise a vendor could issue patches gradually or incompletely in so-called "roving patches."[300] 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, the patch can introduce a glitch into a law firm's networks or cause a cascading response of adverse consequences that reach beyond the cloud and 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 required downloads from the cloud:

> 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.[301]

i. 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's customer and threaten the data stored on its Internet-linked computers and digital storage devices.[302] 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

/windowsazure/faq (last visited Oct. 20, 2011) (expand "What are the key benefits of the Windows Azure platform?" hyperlink). However, in Amazon's web services, the vendor is only responsible for "patching systems supporting delivery of service to customers," but the customer is responsible for patching their own "guest operating systems, software and applications." AMAZON WEB SERVICES: RISK AND COMPLIANCE 10 (May 2011), *available at* http://d36cz9buwru1tt.cloudfront.net /pdf/aws-risk-and-compliance-whitepaper.pdf.

300. Woody Leonhard, *The Perils of Patching in the Cloud*, INFOWORLD (Aug. 13, 2010), http://www.infoworld.com/t/software-service/the-perils-patching-in-the -cloud-872?page=0,1.

301. *2011 Google Terms of Service*, *supra* note 268, § 14.4. The 2009 Terms of Service were similar. *2009 Google Terms of Service*, *supra* note 270, § 14.4.

302. *See* EUROPEAN NETWORK AND INFO. SEC. AGENCY, *supra* note 293.

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 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 accounts."[303] However, as Opinion 2008-1 observed (with respect to the 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 relationship . . . ."
>
> . . . .
>
> 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.[304]

The MRPC do not contain a bookkeeping requirement similar to that contained in the NYRPC. However, in Informal Opinion 1384, the ABA Committee on Ethics and Professional Responsibility stated that while "[a] lawyer does not have a general duty to preserve all of his files permanently," clients have a reasonable expectation that valuable information from the lawyer's files "will not be prematurely and carelessly destroyed, to the clients' detriment."[305] Consequently, if a lawyer allows a client's files to be lost or destroyed due to the installation of new code, the lawyer or law firm could be at risk of breaching MRPC Rule 1.1 or MRPC Rule 1.3. By failing to account for the possibility of lost files,

303. ABCNY Opinion 2008-1, *supra* note 231, pt. 2 (discussing a lawyer's ethical obligations to retain and to provide a client with electronic documents relating to representation). All such documents are required to be retained for a period of "seven years after the events that they record." N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.15(d)(1) (2011).

304. ABCNY Opinion 2008-1, *supra* note 231, pt. 2.

305. ABA Comm. on Ethics & Prof'l Responsibility, Informal Op. 1384 (1977).

the law firm has arguably demonstrated a lack of competence by not educating itself on the risks that its choice of technology poses to client files. Additionally, in allowing client files to be lost or destroyed, the lawyer is subjecting the client to harm, which could arguably implicate MRPC Rule 1.3's diligence standard.[306]

ii. Considerations and Precautions

A lawyer and law firm's chief concern should 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."[307] 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.

e. 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 probably will be substantially diminished. Moreover, unless the cloud service agreement requires it, the law firm may be at risk of not receiving *any* timely reports of a breach in the defenses. Furthermore, a firm may misunderstand the

306. *See supra* note 87 and accompanying text; *see also, e.g.*, Alabama State Bar, Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf (discussing "Retention, Storage, Ownership, Production and Destruction of Client Files"); State Bar of Arizona, Ethics Op. 09-04 (2009), *available at* http://www.myazbar.org/ethics/opinionview.cfm?id=704 (discussing "Confidentiality; Maintaining Client Files; Electronic Storage; Internet"); Prof'l Ethics of the Florida Bar, Op. 06-1 (2006), *available at* http://www.floridabar.org/tfb/tfbetopin.nsf/43859e278a5ce05185256b51000b736b/9d8c4cf77b6a54278525718f005ab400?OpenDocument (discussing electronic storage of client records); New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 680 (1996), *available at* http://www.nysba.org/AM/Template.cfm?Section=Home&ContentID=49409&Template=/CM/ContentDisplay.cfm (discussing electronic storage of client records).

307. ABCNY Opinion 2008-1, *supra* note 231, pt. 2.

defenses that exist in the cloud. As Forrester analyst Chenxi Want noted, "'[c]loud computing is optimized for performance, optimized for resource consumption, and optimized for scalability'. . . . 'It's not really optimized for security.'"[308]

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."[309]
- "[A] request for encryption of stored data goes beyond the [cloud service provider] industry standard and may, because of technological constraints, degrade the service."[310]
- "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."[311]
- There is a fundamental problem with cloud computing that uses "virtualization software to partition servers into 'images' . . . . Although packing those virtual machines into cloud providers' data centers provides a more flexible and efficient setup[,] . . . virtual machines suffer from a rarely discussed flaw: They don't always have enough access to the random numbers needed to properly encrypt data."[312]

i. 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

308. Neil Roiter, *How to Secure Cloud Computing*, SEARCHSECURITY.COM (Mar. 2009), http://searchsecurity.techtarget.com/magazineContent/How-to-Secure-Cloud-Computing (quoting Forrester analyst Chenxi Want).

309. *Id.*

310. Barry Reingold & Ryan Mrazik, *Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy (Part I)*, 14 No. 5 CYBERSPACE L. 1, 2 (June 2009).

311. *See* Roiter, *supra* note 308.

312. Andy Greenberg, *Why Cloud Computing Needs More Chaos*, FORBES.COM (July 30, 2009, 7:00 PM EDT), http://www.forbes.com/2009/07/30/cloud-computing-security-technology-cio-network-cloud-computing.html.

firm's network defenses are much the same as those discussed in the earlier sections of this essay concerning the risks of inadvertent disclosure of client confidential information through the use of new technologies[313]—troublesome 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 states a "lawyer shall not knowingly reveal confidential information."[314] 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. 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's confidential information?

Breaches in a law firm's network defenses raise similar ethical issues under MRPC Rule 1.6(a), which states that lawyers are not permitted to reveal client information unless the client either gives informed consent or the disclosure is "impliedly authorized" to carry out the representation.[315] Outsourcing data control is not "impliedly authorized" within the meaning of Rule 1.6(a).[316] Even sophisticated clients are unlikely to understand the network defenses that a law firm has in place to protect its information. For this reason, it is possible that law firms have an obligation to disclose to a client any proposed use of cloud services and to obtain the client's informed consent due to the potential for security breaches in cloud defenses. The ABA's 2008 opinion on outsourcing services seems to support this assertion. The opinion notes that particularly where the relationship between the firm and the service provider is "attenuated," no information that is otherwise protected under MRPC Rule 1.6 can be revealed without the client's informed consent.[317]

313. *See supra* Part III.B.
314. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(a) (2011).
315. MODEL RULES OF PROF'L CONDUCT R. 1.6(a)(2) (2007).
316. ABA Formal Op. 08-451, *supra* note 94, at 5 (stating that the implied authorization of Rule 1.6(a) and Comment 5 do not extend to outside entities over whom the firm lacks effective supervision and control).
317. *Id.*

Ultimately, lawyers are prohibited from *actually revealing* information relating to the representation of a client and they must prevent disclosures that *could* lead to the discovery of confidential information. If relinquishing control over network defenses might heighten the probability of unauthorized access to client information, the decision to transfer control to a cloud service provider would seemingly fall within the scope of MRPC Rule 1.6. As a result, lawyers have an affirmative obligation to attempt to minimize the risks that the cybersecurity defenses maintained by outside service providers will not keep pace with rapidly evolving threats. In that event, counsel might be at risk of failing to take or ensuring that third parties take reasonable precautions to present disclosure of client confidential information.

ii. Considerations and Precautions

The answer to the question above probably would depend on the other precautions taken by counsel, the sensitivity of the client's information, whether safeguards would have averted the breach, and 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 also would 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 arguably would improve the chances that the counsel will become aware of security flaws that they may want to address before outsourcing storage of client data to a public cloud.

By increasing the probable protection of client confidential information, counsel will, in most instances, be increasing their own protection against the risks of an ethical breach. If a breach occurs despite reasonable precautions, those precautions may provide important evidence with which to defend counsel from allegations of a violation of the counsel's ethical obligations under the NYRPC.

f. 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 cybersecurity, 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. For example, the authors have yet to find a cloud service agreement that promises to alert the customer when the provider learns of a security breach. Regardless of the precise origins of the breach, counsel need to know and to inform their clients of the breach and to help them recover from it. If the cloud service provider is located in one of the few jurisdictions that has not enacted a data breach reporting law,[318] the cloud service provider might decide it is entitled to issue *no* report on the incident or on the data affected by the breach.

i. Ethical Issues

A data breach involving the potential release of or access to client confidential information implicates a lawyer and law firm's ethical obligation under NYRPC Rule 1.6(a) to "not knowingly reveal confidential information."[319] If a cloud provider's policy is not to report data breaches to its customers, those customers cannot assess on an ongoing 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 *others whose services are utilized by the lawyer* from disclosing or using confidential information of a client . . . ."[320]

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

318. *See supra* Part III. As of October 12, 2010, only four states did not have data security breach notification laws. Those states were Alabama, Kentucky, New Mexico, and South Dakota. *State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13489 (last updated Oct. 12, 2011). For a listing of the data security breach laws, see *id.*

319. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(a) (2011).

320. *Id.* § 1200 R. 1.6(c) (emphasis added).

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).

The prospect of successive service interruptions and data breaches looms larger after occurrences of both safeguards and uncorrected vulnerabilities in 2011. Sony,[321] Amazon,[322] and Google[323] all have suffered from these types of events in recent years. For example, public concerns about Sony's vulnerabilities rose after Sony reported its second 2011 episode.[324]

The proposed changes to Model Rule 1.6 build upon the New York provision and support the assertion that public cloud providers would fall within the category of persons "whose services are utilized" by the lawyer or law firm. The ABA Commission notes that there is currently an implicit duty to prevent inadvertent disclosure in MRPC Rule 1.6.[325] However, the proposed MRPC Rule 1.6(c) states, "[a] lawyer shall make reasonable efforts to prevent the inadvertent disclosure of or unauthorized access to, information relating to the representation of a client,"[326] which includes unauthorized access by third parties whose services the lawyer utilizes. Although the Commission did not propose any specific security procedures due to the rate at which technology changes, it was the Commission's belief that "lawyers should have an obligation to act reasonably when using technology" and that the rule should clearly state the obligation to do so.[327]

321. Matt Peckham, *PlayStation Network Outage a Disaster for Sony*, TIME (Apr. 21, 2011), http://techland.time.com/2011/04/21/playstation-network-outage-a-disaster-for-sony.

322. Blodget, *supra* note 100.

323. Claudine Beaumont, *Google Gmail Crash Which Hit Millions Now 'Fixed,'* THE TELEGRAPH (Feb. 24, 2009, 6:47 PM), http://www.telegraph.co.uk/technology/google/4799758/Google-Gmail-crash-which-hit-millions-now-fixed.html.

324. *See* Jared Newman, *Playstation Network Breach: It's Really, Really Bad*, TECHNOLOGIZER (Apr. 26, 2011, 2:17 PM), http://technologizer.com/2011/04/26/playstation-network-breach-data-stolen.

325. ABA Comm'n on Ethics 20/20, *supra* note 62, at 9.

326. *Id.* at 6.

327. *Id.* at 4.

It is, therefore, questionable whether a lawyer or law firm who relinquishes control over the storage of its data would be acting reasonably when it has little to no control over security breaches. The Commission provides some guidance on the meaning of "reasonableness" in Comment 16 to proposed MRPC Rule 1.6(c). The Commission identifies several factors that lawyers should consider in determining whether their efforts to protect a client's confidential information are reasonable. These factors include considering the "sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards."[328] Based on these factors, it is possible that the "reasonableness" of a lawyer's action will vary based on the circumstances. However, where the lawyer or the law firm are aware that breaches have already occurred, it is arguably *unreasonable*, based on these factors, to fail to implement additional safeguards as the likelihood of disclosure would now be apparent.

ii. 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 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."[329]

The same duty to "assess the risks attendant to 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 an 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

328. *Id.*

329. New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, 2 (Dec. 8, 2004), http://www.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions751825/Opn782.pdf.

storage and of transmission can be affected by such threats and may therefore deserve continual reassessment. As the NYSBA Ethics Committee has observed (in the context of transmittals by e-mail), "[r]easonable 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."[330]

The ABA made a similar assessment in its opinion on the use of unencrypted e-mail. Its opinion compared various forms of communication from "direct" e-mail to services provided by third parties. Although the ABA ultimately concluded that lawyers have a reasonable expectation of privacy when using e-mail to transmit information, it noted that "[t]he reasonableness of a lawyer's use of any medium to communicate with or about clients depends both on the objective level of security it affords and the existence of laws intended to protect the privacy of the information communicated."[331] The ABA evaluated four different e-mail systems before reaching its conclusion, thereby reflecting the view that the "reasonableness" of an expectation of privacy depends, at least in part, on the particular third-party provider's security measures for ensuring the confidentiality of user e-mail.[332] Furthermore, "when the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted, the lawyer should consult" with the client as to what method is appropriate for the transmission of that information.[333]

The digital era ultimately 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 that same confidential information. The growing recognition that security breaches are frequent occurrences approaching 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 and in the August 30, 2011 changes to its policy as shown in the version below:

No method of transmission over the Internet, or method

330. *Id.* at 2–3.
331. ABA Formal Op. 99-413, *supra* note 133.
332. *Id.*
333. *Id.*

> of electronic storage, is 100% secure, however. Therefore, we cannot guarantee its absolute security.
>
> Sharing access to your files may create additional risks to privacy and to the confidentiality of the information within your files. We provide certain safeguards from our end, for example, the ability for you to view who has accessed the files you've decided to share. But some of the responsibility to prevent unauthorized access remains with you.[334]

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. For example, 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, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal data.[335]

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

---

334. *Privacy*, SOONR, http://www.soonr.com/security/privacy.php (last updated Aug. 30, 2011).

335. *Privacy Policy*, GOOGLE, http://www.google.com/privacypolicy.html (last modified Oct. 3, 2010).

g. 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 license that had been offered by Soonr until late August, 2011, a cloud service provider either claims the right to move, store, and process a customer's data in any location at the provider's sole discretion, or expresses no position on the issue and thereby makes no promise to limit the data's storage to locations identified to the customer or subject to the customer's approval.[336] The agreement gives the

336. *Soonr Terms of Service and End User License Agreement*, *supra* note 294, § 9.2. On occasion a customer has sufficient leverage to negotiate location limitations, as can be seen in the City of Los Angeles' Google Apps contract which contains the following provision:

> 1.7 Data Transfer. Google agrees to store and process Customer's email and Google Message Discovery (GMD) data only in the continental United States. As soon as it shall become commercially feasible, Google shall store and process all other Customer Data, from any other Google Apps applications, only in the continental United States.

Information Technology Agency, *Professional Services Contract*, CITY OF L.A., 75 (Nov. 20, 2009), http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf. Thomas Trappler identifies additional issues relating to the location (and change in location) of a customer's data stored in a cloud vendor's servers:

> A variety of legal issues can arise if an institution's data resides in a cloud computing provider's data center in another country. Different countries, and in some cases even different states, have different laws pertaining to data. One of the key questions with cloud computing is, which law applies to my institution's data, the law where I'm located, or the law where my data's located? Additionally, there are questions about export control: Does saving controlled data on a cloud computing service with a data center located outside the United States constitute a violation of export control laws? For these reasons, it can be important for the contract to identify the geographic region within which the data center hosting your institution's data may be located.

Thomas J. Trappler, *If it's in the Cloud, Get it on Paper: Cloud Computing Contract Issues*, EDUCAUSE Q. (2010), http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532. In addition, there are environmental risks that may be elevated by entrusting data to a cloud computing provider that may elect to store the data in a vulnerable offshore location, as highlighted in a recent U.K. Government study:

> The Foresight Programme from the UK's Government Office for Science produces in-depth studies looking at major issues 20–80 years in the future. It recently published a report on the International Dimensions of Climate Change that identifies a significant vulnerability from cloud computing. As more data centres are needed, and with the UK a relatively expensive location, more will be going offshore, but that makes them potentially more vulnerable to climate change impacts.
>
> The report points out that data storage facilities have already suffered from flooding and cites the Vodafone data centre in Ikitelli, Turkey, which was affected by flash flooding in 2009, putting a quarter of

customer no right to receive reports on the exact locations where their data are stored or the number of "copies" made of such data that may exist. 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 data protection laws and regulations of the E.U. or its member states.[337] Such appeared to be the case for transfers covered by the Soonr Terms of Service and End User License Agreement, which prior to an August 2011 change to Soonr's privacy policy made no promise to store U.S. persons' data on U.S.-located servers:

> 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.[338]

Some cloud service providers offer features that promise advantages to the user with an undisclosed reduction in security. For example, Gmail and Google Docs provide an automatic draft saving feature by which the service periodically "saves" and uploads the contents of e-mail or documents to Google's servers where they are saved as "drafts".[339] However, researchers report that the same

---

> the local network at risk. Similarly, in August 2009 the rainfall from Typhoon Morakot caused rivers to flood in Taiwan flushing large volumes of sediment into the ocean. This led to several submarine landslides which broke at least nine communications cables 4000m down. It disrupted the Internet and telecommunications between Taiwan, China, Hong Kong and other parts of Southeast Asia.
>
> The study also makes the point that over 95% of global communications traffic is handled by just one million kilometres of undersea fibre-optic cable. Rising sea levels increase the risk of flooding of coastal cable facilities and may also affect the stability of the seabed, making cables more vulnerable.

Pete Foster, *Cloud Computing—A Green Opportunity or Climate Change Risk?*, THE GUARDIAN (Aug. 18, 2011), http://www.guardian.co.uk/sustainable-business/cloud-computing-climate-change.

337. *See, e.g.*, *Directive 95/46/EC of the European Parliament and of the Council*, EUR-LEX, 31 (Oct. 24, 1995), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT.

338. *Soonr Terms of Service and End User License Agreement*, *supra* note 294, § 9.2.

339. *See* Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy & Henry M. Levy, *Vanish: Increasing Data Privacy with Self-Destructing Data*, UNIV. OF WASH., http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.pdf (last visited

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.[340] Moreover, to the extent that Google retains these early drafts in its system, the drafts qualify as electronic records that must be preserved and produced in e-discovery. Thus, the drafts feature seems to impose new challenges for lawyers and law firms.

i. 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 (EAR)[341] and the International Traffic in Arms Regulations (ITAR)[342] require a license for certain kinds of data to be exported from the United States and make it impermissible to export or re-export certain kinds of data to prohibited destinations.[343] If a client places such data in records they entrust 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 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

Oct. 11, 2011) [hereinafter Geambasu et al.].

340. *Id.*

341. As the Commerce Department's Bureau of Industry and Security explains on its website: "Per Part 772 of the Export Administration Regulations (EAR), 'technology' is specific information necessary for the 'development,' 'production,' or 'use' of a product. . . . The 'export of technology' is controlled according to the provisions of each Category'. . . . Controlled technology is that which is listed on the Commerce Control List." U.S. Dep't of Commerce, *"Deemed Exports" FAQs*, U.S. BUREAU OF INDUS. & SEC., http://www.bis.doc.gov/deemedexports/deemedexportsfaqs.html#2 (last visited Oct. 20, 2011).

342. 22 C.F.R. § 125 (2010).

343. Embargoes and Other Special Controls, 15 C.F.R. § 746 (2011) (setting forth the embargoed destinations identified by EAR in Part 746). For a non-exhaustive list of embargoed destinations identified by the ITAR, see U.S. Dep't of State, *Country Policies and Embargoes*, DIRECTORATE OF DEF. TRADE CONTROL, http://www.pmddtc.state.gov/embargoed_countries/index.html (last updated Sept. 23, 2011) (listing the Federal Register publications that contain the applicable regulations for each such targeted country).

agreement. Although a review of such issues is beyond the scope of this article, 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.[344] 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 NYRPC or MRPC Rule 1.4(a)(2) to "reasonably consult with the client about the means by which the client's objectives are to be accomplished"[345] and under the NYRPC or MRPC Rule 1.3 requirements to "act with reasonable diligence and promptness in representing a client."[346]

ii. 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:

---

344. *See* COMPUTER SEC. DIV., U.S. DEP'T OF COMMERCE, FIPS PUB. 200, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS, at 3 (Mar. 2006), *available* at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf; BURKE T. WARD & JANICE SIPIOR, THE INTERNET JURISDICTION RISK OF CLOUD COMPUTING, 27 INFO. SYS. MGMT. 334, 334–37 (2010).

345. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(2) (2007).

346. MODEL RULES OF PROF'L CONDUCT R. 1.3 (2007).

> [T]he 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.[347]

Such concerns suggest that a law firm give serious consideration to enhanced 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

347. New Jersey Advisory Comm. on Prof. Ethics, Op. 701 (2006), *available at* http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html.

relating to the representation of a client . . . ."[348] In addition to client-specific checks, it is possible that in ensuring compliance with NYRPC and Model Rule 1.4(a)(1), "reasonable care" would include informing the client of the circumstances surrounding the use of the cloud service provider. Both rules provide that a lawyer shall "promptly inform the client of any decision or circumstance with respect to which the client's informed consent . . . is required by these Rules . . . ."[349] Only by informing the client of the proposed course of conduct and use of the cloud service can the client provide any specialized instruction regarding additional security measures.

Also, it would 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 both the NYRPC and the MRPC Rule 1.4(a)(3) requirement to "keep the client reasonably informed about the status of the matter."[350] Moreover, if there is a reasonable possibility that such a breach could result in damage to the client, which the client could 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 . . . ."[351]

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 offsite third-party vendor. The ISBA noted that in looking at the same scenario, the ABA 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.[352] Such disclosure may be required under MRPC

348. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007); *see also* N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(a) (2011).

349. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) (2007); N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.4(a)(1) (2011).

350. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(3) (2007); N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.4(a)(3) (2011).

351. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.1(c)(2) (2011).

352. ISBA Advisory Op. on Prof'l Conduct, Formal Op. 10-01 (2009), *available at* http://www.isba.org/sites/default/files/ethicsopinions/10-01.pdf.

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."[353]

An additional concern is the type of warranties or indemnification that a cloud provider may offer to the lawyers and law firms with which it contracts. Lawyers and law firms may wish to consider the availability of indemnification for damages sustained by outages and data security breaches. In the event that lawyers or firms find the warranty or indemnification provisions lacking in any respect, they may wish to procure separate coverage for actual, incidental, and consequential damages that outages or breaches may cause them directly, and clients indirectly.

h. Diminished Ability to Protect Data from Government Surveillance or Seizure

Data transmitted wirelessly can be intercepted more easily than data sent through telephone wires.[354] Encryption may reduce the potential number of persons who can intercept transmitted data, unless they are government agents or government-sponsored entities.[355] Moreover, the amount of data that can be intercepted

353. *Id.* at 3 (quoting ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995)).

354. A 2010 Government Accountability Office (GOA) Report highlighted the increased risks of wireless communications, noting: "Wireless technologies use radio waves instead of direct physical connections to transmit data between networks and devices. As a result, without proper security precautions, these data can be more easily intercepted and altered than if being transmitted through physical connections." The GAO further observed that:

> Wireless networks also face challenges that are unique to their environment. A significant difference between wireless and wired networks is the relative ease of intercepting WLAN transmissions. For WLANs, attackers only need to be in range of wireless transmissions and do not have to gain physical access to the network or remotely compromise systems on the network.

U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-43, INFORMATION SECURITY: FEDERAL AGENCIES HAVE TAKEN STEPS TO SECURE WIRELESS NETWORKS, BUT FURTHER ACTIONS CAN MITIGATE RISKS 1, 8 (2010), *available at* http://www.gao.gov/new.items/d1143.pdf.

355. PARLIMENTARY OFFICE OF SCI. & TECH., POSTNOTE 270: DATA ENCRYPTION (2006) (U.K.), *available at* http://www.parliament.uk/documents/post/postpn270.pdf. If Congress passes certain legislation requested by the Administration, Government agencies would have access to such encrypted communications. As reported in The New York Times:

> Essentially, officials want Congress to require all services that enable communications—including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct "peer to peer" messaging like Skype—to be technically

will usually be less than the data that can be seized if government agents gain access to the cloud provider's servers.[356]

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,[357] the authors expect that law firms likely will put up far more resolute and vigorous defenses of client confidential information than will cloud providers. 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 confidential information has been requested by, or surrendered to, federal agents.[358]

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 e-mails from the entire domain because the Internet service provider improperly set filtering controls and collected data on the domain instead of the single e-

---

> capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.

Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=1&_r=1&hp.

356. THE HARVARD LAW NATIONAL SEC. GRP., CLOUD COMPUTING & NATIONAL SECURITY LAW 21 (2010), *available at* http://www.law.harvard.edu/students/orgs/nsrc/Cloud.pdf.

357. 12 U.S.C. § 3414(a)(3)(A) (2006); 15 U.S.C. §§ 1681u(d)(1), 1681v(c)(1) (2006); 18 U.S.C. § 2709(c)(1) (2006); 50 U.S.C. §436(b)(1) (2006). For more discussion of the nondisclosure requirements of these national security letter statutes, see DAVID P. FIDLER & SARAH JANE HUGHES, RESPONDING TO NATIONAL SECURITY LETTERS–A PRACTITIONERS' GUIDE, ch. 3 (2011) and text accompanying notes 15–23, *supra*.

358. *See, e.g.*, J. Nicholas Hoover, *LulzSec, Anonymous: Feds Most Wanted*, TECHWEB (June 21, 2011, 1:06 PM), http://www.techweb.com/news/231000131/lulzsec-anonymous-feds-most-wanted.html ("[F]ederal investigators routinely seek access to the server logs of ISPs as part of their investigations. 'Most U.S.-based ISPs these days don't even report law enforcement requests to the public[.]'" (quoting Chester Wisniewiski, senior security advisor at Sophos)); Mike Masnick, *So the FBI Can just Take a Copy of All Instapaper User Data with No Recourse?*, TECHDIRT (June 24, 2011, 6:39 PM), http://www.techdirt.com/articles/20110624/15282814850/so-fbi-can-just-take-copy-all-instapaper-user-data-with-no-recourse.shtml (describing FBI seizure of backup server for popular service known as Instapaper, which individuals use to save web pages and other information).

mail address.[359] While it is troubling that these types of errors can occur, the greater concern for law firms and lawyers intent on protecting a client's confidential information should be that these occurrences are not rare. 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.[360]

Providers of web-based e-mail 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 e-mail 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."[361] However, as the result of a mutual legal assistance treaty between Canada and the United States, Hush released to U.S. Drug Enforcement Agents three CDs containing e-mails from three Hushmail accounts.[362]

Although supposedly Hushmail could release only encrypted e-mails that 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.[363] The court order required Hushmail to use such stored passphrases to decrypt the e-mails

359. Eric Lichtblau, *F.B.I. Gained Unauthorized Access to E-Mail*, N.Y. TIMES, Feb. 17, 2008, at A1, A20, *available at* http://www.nytimes.com/2008/02/17/washington/17fisa.html.

360. *Id.* at A1.

361. Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED.COM (Nov. 7, 2007, 3:39 PM), http://www.wired.com/threatlevel/2007/11/encrypted-e-mai.

362. Criminal Complaint, Statement of Probable Cause at 4, United States v. Stumbo, No. 5:07-mj-00034-TAG (E.D. Cal. Sept. 17, 2007), *available at* http://www.wired.com/images_blogs/threatlevel/files/steroids.source.prod_affiliate.25.pdf.

363. Singel, *supra* note 361.

before releasing them to government agents.[364]

i. Ethical Issues

National security letters (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. NSLs also implicate the implicit duty under MRPC Rule 1.6(a) to prevent the unauthorized disclosure of client information. If 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 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 provider is a major enterprise that has received many NSLs already and has a pre-established protocol for responding to NSLs. 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: A Practitioner's Guide*, 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 [hard copy] 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,

364. *Id.*

> 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.[365]

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's or its client's awareness. Such risks may be significantly greater for some clients because of their nature of their businesses

ii. Considerations and Precautions

Law firm customers of a public cloud provider should not expect notice from the provider that it has received an NSL that would cover data and documents of the law firm or its clients. Notice would violate the gag order provisions of national security letter laws. Indeed, the recipient of the NSL may not decide to notify its own lawyers of receipt unless the lawyers' involvement is necessary to the recipient's response to the NSL or the recipient has a question about its duties under the NSL. Thus, counsels' decision of whether to store in a public cloud the documents and data of clients whose businesses make them more likely to receive NSLs may require additional careful consideration in order to comply with both the NYRPC and MRPC requirements to avoid damaging a client and to exercise reasonable care to prevent the cloud provider from disclosing client confidential information. Such considerations also may deserve to be discussed with the client to ensure compliance with the NYRPC and MRPC requirement to reasonably consult with the client about the means by which the client's objectives are to be accomplished.[366]

365. FIDLER & HUGHES, *supra* note 357, at 42, 44.

366. MODEL RULES OF PROF'L CONDUCT R. 1.2 (2007); N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.2 (2011).

i. Diminished Ability to Monitor and Ensure Secure Purging of Archived Records

Sometimes the concern regarding client confidential information centers not on preservation, access, or production of data but on the need to ensure its destruction, as when a protective order or settlement agreement requires the destruction of confidential materials after 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.

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. For example, 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."[367] 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. As one report observed:

> 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.[368]

In 1985, the Department of Defense (DoD) established its standard for eradicating digital data. Document DoD 5220

---

367. RICHARD KISSEL, ET AL., DEP'T OF COMMERCE, NAT'L INST. OF SCI. AND TECH., SPECIAL PUB. 800-88, GUIDELINES FOR MEDIA SANITIZATION 7 (2006) [hereinafter NIST 800-88], *available at* http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

368. Gordon F. Hughes, Daniel M. Cummins & Tom Coughlin, *Disposal of Disk and Tape Data by Secure Sanitization*, IEEE SECURITY & PRIVACY, Jul.-Aug. 2009, at 29, *available at* http://66.14.166.45/whitepapers/compforensics/datarecovery/scrubbing-sanitization/Disposal%20of%20Disk%20and%20Tape%20Data%20by%20Secure%20Sanitization.pdf.

required "two fixed-character overwrites and one random-character overwrite, followed by a verify read."[369] This standard eventually ceased to be 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 overwrite utilities have an authorized DoD laboratory evaluate them for proper functionality. NIST 800-88 replaces DoD 5220 for disk sanitization.[370]

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.[371]

The federal government has cited NIST 800-88 as the applicable standard in regulations concerning data security. For example, in the HITECH Act: "Organizations should label these media with their internal operating classifications and associate a type of sanitization described in this publication."[372]

If the files stored include personally identifiable information about consumers, whether direct customers of the firm or customers of the firm's client, additional "safe disposal" regulations implementing the Fair and Accurate Credit Transactions Act of 2003[373] may be required. Even if not required, the Act and federal regulations implementing it,[374] may suggest suitable means for the firm to implement.

The Ethics Essays concluded that many law firms or lawyers were not familiar with NIST 800-88 and its standards.[375] They also questioned whether law firms and lawyers or their clients had their confidential information so well organized that it is stored on media labeled by the level of confidentiality as recommended by

---

369. *Id.* at 30.
370. *Id.* (footnotes omitted).
371. NIST 800-88, *supra* note 367, at 7.
372. *Id.*
373. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 216, 117 Stat. 1952 (2003) (codified at 15 U.S.C. §§ 1681–1681x (2006)).
374. *E.g.*, Disposal of Consumer Report Information and Records, 69 Fed. Reg. 68690 (Nov. 24, 2004) (codified at 16 C.F.R. pt. 682).
375. *See* sources cited *supra* note 53.

NIST 800-88.[376]

NIST 800-88 encourages that plans for data sanitization be made based on the media and the level of risk to confidentiality. It explains that the planning process should "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."[377] 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, plans 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.[378] 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.[379] 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.[380]

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.[381] There is no

376. *Id.*

377. NIST 800-88, *supra* note 367, at 7.

378. *Compare 2011 Google Terms of Service*, *supra* note 268, *with 2009 Google Terms of Service*, *supra* note 270.

379. *See, e.g.*, *2011 Google Terms of Service*, *supra* note 268.

380. *October 2010 AWS Customer Agreement*, *supra* note 282, §§ 3.7–.8.

381. NIST 800-88, *supra* note 367, at 7–9. Note that NIST identifies a fourth method of sanitization, "disposal," but that does not involve eradication of the data, and would incur risks of unauthorized access in an era where "dumpster

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 and state standards that can be used as guidance that would help a lawyer or law firm document and demonstrate that reasonable measures had been taken to protect the confidentiality of such information.[382] For example, the HITECH Act defines "unsecured PHR identifiable 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).[383]

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.[384]

---

diving" is not an uncommon practice. *Id.* at 5.

382. Examples of federal data sanitization standards include the HITECH Act and the Safeguards Rule of the Gramm-Leach-Bliley Act. Note that the FTC recommends that financial institutions, to achieve compliance with the Safeguard Rule, should consider disposing of "customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule." BUREAU OF CONSUMER PROT. BUS. CTR., FED. TRADE COMMISSION, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE (Apr. 2006), *available at* http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule; *see* 16 C.F.R. § 682.3 (2005); *Disposal of Consumer Report Information Records*, FED. TRADE COMMISSION, http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf (last visited Oct. 20, 2011). According to one report, "at least 10 states have enacted laws that require destruction of 'personal information' that is no longer needed for business." *Guidelines for Data Sanitization and Disposal*, CARNEGIE MELLON, 3 (Jan. 21, 2010), http://www.cmu.edu/iso/governance/guidelines/docs/DataSanitizationDisposalGuidelines_FINALv1.2.pdf.

383. Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 17937(f)(3) (2010). HITECH further specifies that the Secretary is required to issue guidance in a timely manner. *Id.* § 17932(h)(2).

384. *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusuable, Unreadable or Indecipherable to Unauthorized Individuals 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*, DEP'T HEALTH & HUMAN SERVICES (Apr. 27, 2009), http://www.hhs.gov/ocr/privacy/hipaa/understanding/ coveredentities/federalregisterbreachrfi.pdf; *see also* Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Records, 75 FED. REG. 2014 (Jan. 13, 2010).

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

i. 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. Moreover, information that can be reconstructed into an incomplete and partially identifiable record is 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. In some situations, the lawyer or firm could only defend against the publication of such mangled fragments by a *further disclosure* of client confidential information.

With such data located offsite on a third party's digital media, we suggest that some of the following types of data sanitization issues may arise:

- *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, either 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 E-Discovery Records.* When a firm produces client electronic records in fulfillment of e-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 are not thereby put at heightened risk of 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. If clients believe that their data will be put at such heightened risks, counsel may find it increasingly difficult to persuade clients to fulfill their e-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 it. 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 a 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 a 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 every copy of client confidential information from each of the media on which the copies exist, have been recorded, or have been stored in the cloud vendor's servers and back-up servers raises 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 . . . ."[385]

As discussed previously, the requirement that counsel monitor "other persons" involved in the representation is currently embodied in Comment 16 to MRPC Rule 1.6.[386] Although straying from the MRPC comments would not itself indicate a violation of the MRPC *per se*, Comment 16 nevertheless provides guidance on a lawyer's responsibility to prevent unauthorized disclosure of confidential information.[387] Furthermore, the ABA Commission's proposed amendments to MRPC Rule 1.6 indicate the ABA Commission's attempt to heighten a lawyer's confidentiality obligations under the Rule; thus, a failure to protect client

385. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(c) (2011) (emphasis added).

386. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2007).

387. *Id.*

information after the termination of representation could ultimately still put the lawyer at odds with MRPC Rule 1.6.[388]

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.[389]

MRPC Rule 1.9(c)(2) imposes a similar requirement, but it omits the use of the word "confidential" with reference to revealing the former client's information. The MRPC rule, therefore, appears to have a broader reach than does the NYRPC, although the comments to the MRPC rule indicate that a lawyer may nevertheless use "generally known information" about a client when necessary for representing another client.[390]

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 either NYRPC Rule 1.9(c)(2)[391] or MRPC Rule 1.9(c)(2)[392] regarding a former client's confidential information. Perhaps the MRPC'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 either the NYRPC or the MRPC.

In this connection, the scope of client confidential information of concern includes all such information that a lawyer or law firm is not otherwise required to retain for seven years under NYRPC Rule 1.15(d), such as "copies of all retainer and

388. *See* ABA Comm'n on Ethics 20/20, *supra* note 62, at 5–10.
389. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.9(c) (2011).
390. MODEL RULES OF PROF'L CONDUCT R. 1.9 cmt. 8 (2007).
391. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.9(c)(2) (2011).
392. MODEL RULES OF PROF'L CONDUCT R. 1.9 (C)(2) (2007).

compensation agreements with clients,"[393] "copies of all bills rendered to clients,"[394] 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."[395]

Client confidential information not covered by the seven-year retention rule is put at risk when a lawyer or firm entrusts compliance with the retention rule 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. There is no analogous seven-year retention provision in the MRPC. But under either the MRPC or the NYRPC, 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 copies of all such information to be transferred to the client's new counsel? Surprisingly, this issue is not addressed in either the NYRPC or the MRPC, although the former came into effect in April 2009.[396]

Lawyers and law firms should not rely on cloud service providers to eradicate residual confidential data entrusted to them. As a result, they must deal with the significantly high risk that confidential data of a lawyer 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 as the data increasingly become 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 terminates. The client may instruct counsel to transfer the electronic records to a new counsel. However, copies of the client's confidential data may 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 have lost effective control of the client's

393. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.15(d)(1)(iii) (2011).
394. *Id.* R. 1.15(d)(1)(v).
395. *Id.* R. 1.15(d)(1)(vi) (emphasis added). Here, the seven-year record retention rule would appear to apply to the "payments" to the cloud service provider as well as to the lawyer or law firm. *See id.*
396. *See* N.Y. COMP. CODES R. & REGS. tit. 22, § 1200 (2011).

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 also may 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 (including 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.[397] 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.[398]

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.[399] NIST 800-88 explains, "[a] representative sampling of media should be tested

397. NIST 800-88, *supra* note 367, at 7.
398. *See id.* at 14.
399. *Id.* at 8.

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."[400]

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

Until that gap is corrected by amendment of the NYRPC, we recommend that counsel interpret MRPC Rule 1.9(c)(2) and 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. Counsel also should 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, in the explicit requirement of NYRPC Rule 1.6(c) and in the implicit requirement of MRPC Rule 1.6, a lawyer or law firm must exercise reasonable care to ensure that *others whose services are utilized by the lawyer* will not disclose the client's confidential information.[401] Therefore, one could construe entrusting such information to a cloud service provider's digital media as nullifying an underlying assumption of Rule 1.6, namely that the client's confidential information will only be at risk from counsel's service providers during the representation.[402] In the pre-digital era, that assumption was fundamentally sound: when the attorney-client relationship terminated, the attorney would usually

400. *Id.* at 15.

401. MODEL RULES OF PROF'L CONDUCT R. 1.6; N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 1.6(c) (2011).

402. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6; N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R 1.6(c) (2011).

return or arrange for secure destruction of the hard copies containing client confidential information. If counsel retained such information in a warehouse, counsel 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 NYRPC Rule 1.6(c) and MRPC Rule 1.6 that if counsel entrusts client confidential information to a cloud service provider and its digital media, counsel appears to have 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 NYRPC, and would risk damage to counsel's relationship with clients and its reputation.

ii. Considerations and Precautions

If counsel discusses with a client the cybersecurity issues that may arise from entrusting the client's confidential information to a cloud service provider and its digital media, it also would seem prudent for counsel to discuss carefully with the client the cybersecurity 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. It would be prudent for counsel also to review with the client the risks that data stored on the cloud, and not frequently accessed by the client, might eventually cease to be readable by a client's equipment.[403]

Before discussing such issues with a client, counsel will need to consider carefully whether its agreement with the cloud service provider covers the full range of risks of confidential data remaining on digital storage media and requires the

403. *See* Robert Plant, *To Cloud, or Not to Cloud*, WALL ST. J., Apr. 25, 2011, at R9 ("[C]ompanies can't just hand over data [to a cloud service provider] and forget about it. They need to check it regularly to make sure the formats are still compatible with their current systems—think of all those eight-tracks in the attic—and the tapes haven't started to degrade.").

implementation of safeguards commensurate with such risks. Counsel should anticipate that cloud service providers may 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 providers are not attending to this issue. Counsel cannot safely ignore or postpone addressing such issues. Once the lawyer or law firm entrusts a client's confidential data to a cloud service provider, the problem of such data's eventual eradication is inevitable. 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, lawyers and law firms should 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 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.[404]

Counsel's ethical obligations cannot be fulfilled by accepting a vendor's position that the required precautions are too burdensome, are too 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 is essential for a client to trust its counsel. The promised benefits of cloud computing appear to be significant, but so far they also appear to have 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 onto 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 data were supposedly "deleted," transferred, or backed up. The proliferation of storage sites multiplies the risks that such data may be disclosed to or accessed by unauthorized persons. Because counsel appear to remain obligated to protect such data, even when the data relate to matters

404. NIST 800-88, *supra* note 367, at 7–8.

of a former client, the increase in the risks to the data would appear to also increase the ethical risks for counsel.

j. Increased Risk of Inadvertent Grant of Licenses to Client's Intellectual Property

It probably would appear farfetched to many clients and their counsel that the storage of data on a cloud vendor's servers, or the use of the cloud vendor's services and software, could result in the grant of any license to the client's intellectual property rights in its data. However, certain cloud computing vendors require such grants in their standard customer service agreements. If a law firm, for example, is considering authorizing its lawyers to use Google Docs, as a cloud-based substitute for perhaps Microsoft Word, or fails to prohibit its lawyers from using such an application, the law firm would probably find it objectionable that Google's Terms of Use for Google Docs include a grant to Google, by the data customer, of a so-called "content license" that states, in pertinent part:

> **11. Content license from you.** 11.1 [B]y submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the [Google Docs] Services . . . . 11.3 You understand that Google, in performing the required technical steps to provide the Services to our users, may (a) transmit or distribute your Content over various public networks . . . and (b) make such changes to your Content as are necessary to conform and adapt that Content to the technical requirements of connecting networks, devices, services or media. You agree that this license shall permit Google to take these actions."[405]

Google's response, however, addresses issues only that arise under its Terms of Service, Section 11.1, and thus ignores those that arise under Section 11.2 and 11.3. Moreover, the "content license" is far broader than what Google's response describes it to be. If it were not, it would contain only the language set forth in the response, and not the far more extensive reach attained by the operative words "license to reproduce, adapt, modify, translate,

405. *Google Terms of Service*, GOOGLE (Apr. 16, 2007), http://www.google.com/accounts/TOS?hl=en.

publish, publicly perform, publicly display and distribute any Content which you submit, post or display." If all Google needs to do is have a license to ensure it has "permission to display," it would not need to include in the "content license" an express grant of rights to "publicly perform," "modify," "translate," and "adapt," which arguably also grants Google by implication a right to create derivative works.

To say the license is one thing, when it clearly says the opposite and reaches far beyond the explained scope is fundamentally misleading, as is the suggestion that ownership is the only issue and that only those "not familiar with legal agreements" would find the scope of the "content license" deeply troubling. When one looks again at Sections 11.2 and 11.3, it becomes evident that those sections contradict the position taken in Google's response. A need to ensure "permission to display" is not required by, and is inconsistent with, a statement that the grant of a "content license" includes "a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services." In short, Google's response is lamentable and could mislead unwary readers into overlooking what they are really granting Google the rights to do with their content. For that reason, Google's requirement that users grant it a "content license" raises serious ethical risks for a law firm or lawyers that use, or allow their staff to use, Google Docs when generating or revising documents that contain client confidential data and content in which the client has intellectual property rights.

i. Ethical Issues

There are probably few, if any, clients that would be willing to agree to grant a cloud vendor a right to any content that the client may generate or that its attorneys may generate through the use of a cloud-based, word-processing program such as Google Docs. A lawyer or law firm would certainly also be unwilling to agree to grant such a license. There is, however, an ethical risk that could be inadvertently overlooked by a law firm's failure to ensure that its lawyers, and the personnel that they are responsible for supervising, decide on their own to use a cloud-based service whose terms of use included a "content license" similar to that required for use of Google Docs. The detrimental effects that the grant of such a license could have to a client's copyrights and trade secrets would severely damage a law firm's relationship with its client and

could put the firm at risk of having acted in violation of the NYRPC and MRPC, including Rules 1.1 (to provide "competent representation") and 1.6(a) (to protect "confidentiality" of client information).

ii. Considerations and Precautions

The primary precaution to avert the risk of inadvertent grants of licenses to cloud vendors is for law firms to ensure that, as part of their ongoing efforts to keep abreast of new technologies, they extend such efforts to include a review of a representative sample of vendors' standard terms and conditions. To the extent that such review identifies risks, such as the express grant of "content licenses" or other unacceptable terms, the firm will probably find it prudent to modify their policies for employees and third-party contractors to highlight such risks and to consider prohibiting such personnel from letting any client confidential information become subject to any third-party vendors' services agreement without express authorization by the firm. The attraction that new communications technologies tend to exert, however, over personnel makes such prohibitions unpopular and difficult to enforce consistently throughout an enterprise. Partners, associates, and other personnel are each, for different reasons, probably going to find circumstances where they believe that an exception to such prohibitions is warranted in order to achieve a desired convenience, or to meet an urgent deadline, or to obtain access to data when other means have become inefficient or unavailable. As with any data security policy, it is such discretionary actions that can create vulnerabilities in a system, or in this context, result in an inadvertent and potentially costly grant of a "content license."

k. Increased Risk of Noncompliance with New or Amended Laws and Regulations

When lawyers and law firms remain in control of the client confidential information entrusted to them, they also remain in a position to be able to adjust promptly and with agility to any new or amended laws and regulations that might apply to the storage, use, movement, retention, or security of such data. When control over client confidential information is relinquished to a cloud computing vendor, changes in the law can create obligations for compliance that may be difficult, costly, and potentially impossible to fulfill while the data remains in the control of the cloud

computing vendor. Such changes in the law or regulations tend to emerge and apply in specific regulated industries or activities such as health care, finance, securities, and defense and aerospace. As an illustration, we will review here the emergence of a rule proposed by the DoD: an amendment to the Defense Federal Acquisition Regulation Supplement (DFARS).[406] The proposed DFARS rule, if adopted, would add a new subpart and associated contract clauses that would establish, for the first time,[407] requirements applicable to DoD contractors and subcontractors for the safeguarding of unclassified DoD information and the reporting to the Government cyber intrusions that affect unclassified DoD information resident on or transiting a contractor's unclassified information systems (the "Cybersecurity Rule"). The Cybersecurity Rule was initially described in March 2010 in the DoD's advanced notice of proposed rulemaking, seeking public comment on the rule[408] and setting forth in greater detail in the proposed rule published in the Federal Register on June 29, 2011, seeking public comment to be considered in the formation of the final rule.[409] Neither the March 2010 nor the June 2011 drafts of the Cybersecurity Rule refers to cloud computing systems or appear to have any provisions that specifically address contractors that outsource their information systems to a cloud computer service provider.[410] However, the June 2011 draft provides a definition of "Contractor information system" in a proposed contract clause entitled "Enhanced Safeguarding of

406. DFARS is a set of rules designed to assist members of the DoD when procuring goods and services (e.g., ammunition for military personnel). *About Defense Acquisition Regulations System*, DPAP, http://www.acq.osd.mil/dpap/dars/about.html (last updated Sept. 29, 2011).

407. Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified DoD Information (DFARS Case 2011–D039), 76 Fed. Reg. 38,089, 38,089 (June 29, 2011) [hereinafter DFARS], *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-06-29/pdf/2011-16399.pdf (to be codified at 48 C.F.R. pts. 204, 252). The proposed DFARS are identified alpha-numerically, *e.g.*, with the letters such as XX or YY at the end of the numeric sequence to signal their relationship to provisions in the existing regulation. The DFARS does not presently address the safeguarding of unclassified DoD information within industry, nor does it address cyber intrusion reporting for that information. *Id.*

408. Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information (DFARS Case 2008–D028), 75 Fed. Reg. 9563, 9565 (Mar. 3, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-03-03/pdf/2010-4173.pdf (to be codified at 48 C.F.R. pts. 204, 252).

409. DFARS, *supra* note 407, at 38089.

410. *See* DFARS, *supra* note 407; Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information, *supra* note 408, at 9563.

Unclassified DoD Information" which would appear to apply to an information system that relies at least in part on a cloud computing system.[411]

A cloud computing system serving a DoD Contractor would probably qualify as an information system "operated . . . for"[412] the Contractor or a subcontractor, and there is no provision in the Cybersecurity Rule that appears to exclude it from the Rule's scope.[413]

The Cybersecurity Rule exemplifies a recent trend in amendments to the DFARS and Federal Acquisition Regulations: the setting of enhanced standards for contractor conduct combined with new requirements for self-reporting of violations by the contractor to the Government.[414] The Cybersecurity Rule establishes standards for contractor and subcontractor provision of cybersecurity for unclassified DoD information, requires contractors to report cyber intrusions that affect such information, and sets forth criteria by which the DoD's Contracting Officers will then evaluate whether such intrusions demonstrated whether the reporting contractor, if it complied with the reporting obligations, nonetheless failed to fulfill its contractor obligations under the Rule to protect the compromised information. As explained in the Cybersecurity Rule's policy statement:

> A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information safeguards for DoD unclassified information, or has otherwise failed to meet the requirements of the clause at 252.204–70YY . . . . A cyber incident will be evaluated in context, and such events may occur even in cases when it is determined that adequate safeguards are being used in view of the nature and sensitivity of the DoD unclassified information and the anticipated threats. However, the Government may consider any such cyber incident in the context of an overall assessment of the contractor's compliance with the requirements of the

411. DFARS, *supra* note 407, at 38093 ("As used in this clause . . . *Contractor information system* means an information system belonging to, or *operated* by or *for*, the Contractor or a subcontractor.") (emphasis added).

412. *Id.*

413. *See id.*

414. *See, e.g.*, Federal Acquisition Regulations; FAR Case 2007-006, Contractor Business Ethics Compliance Program and Disclosure Requirements, 73 Fed. Reg. 67,064, 67,075 (Nov. 12, 2008) (to be codified at 48 C.F.R. pts. 2, 3, 9, 42, 52).

clause at 252.204–70YY.[415]

The Cybersecurity Rule, if adopted in or near to its current form, will set two levels of data security or information protection that DoD contractors must implement and maintain: "basic safeguarding" and "enhanced safeguarding"[416] against cyber intrusions that might result in "exfiltration" of information (i.e., "any unauthorized release of [DoD information] from within an information system" includes "copying the data through covert network channels or the copying of data to unauthorized media").[417] Separate contract clauses set forth the requirements for "basic safeguarding" and "enhanced safeguarding" (respectively, DFARS 252.204-70XX and 252.204-70YY).[418]

"Basic safeguarding" requires the contractor to provide "adequate security to safeguard unclassified Government information" from unauthorized access and disclosure.[419] These requirements apply to a contractor's unclassified information system, but do not appear to apply to any such system operated for the contractor, except that the Rule appears to prohibit the contractor from handling such information in certain ways and thus would appear to require the contractor to flow down such requirements to any third-party operator handling such information on its behalf. There are seven basic safeguards that a contractor must implement, each of which amounts to a common sense precaution, or put differently, the avoidance of actions that would put Government information at an unnecessarily high risk of "exfiltration."[420] Examples include the following:

> (1) *Protecting unclassified Government information on public computers or websites:* Do not process unclassified Government information on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control . . . .
>
> (2) *Transmitting electronic information.* Transmit email, text messages . . . using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment.

415. DFARS, *supra* note 407, at 38091–92.
416. *Id.* at 38090.
417. *Id.* at 38092.
418. *Id.*
419. *Id.* at 38093.
420. *Id.*

> . . . .
>
> (5) *Sanitization*. At a minimum, clear information[421] on media that has been used to process unclassified Government information before external release or disposal.[422]

Each of the above-quoted "basic safeguarding" requirements would appear, to varying extents, to be difficult, if not impossible, to fulfill if the contractor or its outside legal counsel received unclassified Government information, in connection with a DoD contract that contained the "basic safeguarding" clause (DFARS 252.204-70XX), and processed and stored such information in a cloud computing vendor's servers subject to a typical standard service level agreement. This would be particularly the case if such agreement contained clauses similar to those discussed above in Amazon's Web Service Agreement (i.e., one that made the customer responsible for information security that omitted any requirement for the vendor to sanitize media that contained customer data, or that did not commit to using any specified or high standard of data security). If the cloud service level agreement did not require the vendor to ensure that its servers had "access controls," the contractor and its outside legal counsel would be barred by DFARS 252.204-70XX from having Government information processed on the cloud service provider's servers. If the service level agreement did not require the vendor to implement the "best level of security . . . available, given facilities, conditions, and environment" (a rather ambiguous standard), then the contractor and its outside legal counsel could not transmit electronic information to each other through their service vendor's cloud. And if the service level agreement contained no requirement that matched or incorporated by reference the DFARS 252.204-70XX requirement for clearing media that has been used to process unclassified Government information before disposal of such media, then the contractor and its outside legal counsel would be prohibited from allowing any such information

---

421. The Cybersecurity Rule's proposed text for DFARS 252.204-70XX defines "clearing information" as:

> [A] level of media sanitization that would protect the confidentiality of information against a *robust keyboard attack*. *Simple deletion of items would not suffice for clearing*. For example, overwriting is an acceptable method for clearing media. The security goal of the overwriting process is to replace written data with random data.

Id. at 38092 (emphasis added).

422. *Id.*

to be uploaded to their service vendor's cloud. Simple deletion of the data would violate the "clearing" requirement—overwriting of the data, or a similarly rigorous method, would need to be required of the vendor.[423] Thus, the current standard service level agreement for cloud computing is inconsistent with, and an impediment to, a contractor's obligations to implement and maintain "basic safeguarding" for unclassified DoD information. Neither the contractor nor its outside legal counsel could permit any such information to be uploaded to a cloud if the governing agreement were the current standard service level agreement, without putting the contractor at risk of breaching its contractual obligations to the Government under DFARS 252.204-70XX. It also would put its outside legal counsel at risk of violating professional ethical obligations, including to provide "competent representation" and to maintain "confidentiality" of the client's information.

The "enhanced safeguarding" requirements set significantly higher standards for security than the basic safeguarding requirements impose. As a consequence, "enhanced safeguarding" creates commensurately greater obstacles for a contractor seeking to comply with the contractual requirements of the proposed DFARS clause 252.204-70YY and for its outside legal counsel seeking to fulfill applicable ethical obligations under NYRPC or the Model Code. Proposed DFARS 252.204-70YY directly applies to a contractor's information system "operated . . . for, the Contractor" and thus to any cloud computing system used by the contractor for processing or storage of unclassified DoD information. Note that DoD contractors would be barred from processing or storing *classified* DoD information in the cloud, because doing so would almost certainly bring the contractor into noncompliance with the applicable requirements of National Industrial Security Program (NISP) Operating Manual (NISPOM), which establishes the requirements for all government contractors for the handling of classified information.[424] The "enhanced safeguarding" requirements apply to seven categories of unclassified DoD information, including:

- Information designated as "Critical Program Information,"

423. *See id.* (defining "clearing information").

424. The currently applicable NISPOM is the February 2006 version. U.S. DEP'T OF DEF., NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP), DEF. SECURITY SERVICE, *available at* http://www.dss.mil/isp/fac_clear/download_nispom.html (last visited Oct. 20, 2011).

defined as elements of a "research, development, or acquisition program, that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability";[425] or as "critical information";[426]

- Information subject to export controls under the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR);[427]
- Information designated for controlled access and dissemination (e.g., "For Official Use Only," "Sensitive But Unclassified," "Proprietary");
- Technical data, computer software, and certain other technical information designated by DoD directives;[428] and
- Personally identifiable information, including information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act ("HIPAA").[429]

Because those categories include information covered by the ITAR, EAR, HIPAA, as well as information that qualifies as "Proprietary" or as technical data and computer software, virtually all DoD contractors and subcontractors would have such information on their systems. If awarded a contract containing the Cybersecurity Rule's proposed clause 252.204-70YY, such contractors would need to implement policies and procedures to ensure fulfillment of the "enhanced safeguarding" requirements. There are, however, several of the "enhanced safeguarding" requirements that would be difficult, if not impossible, for a contractor to fulfill if it allowed such information to be processed or stored on the cloud under cloud vendors' current, standard service-level or customer agreements. The contractor must

- Implement, at a minimum, the security controls identified in

425. DFARS, *supra* note 407, at 38093. Such information is designated in accordance with DoD Instruction 5200.39. *Id.*

426. *Id.* Such information is designated in accordance with DoD Directive 5205.02. *Id.*

427. *Id.* at 38093.

428. The applicable directives are DoD Directive 5230.24, Distribution Statements on Technical Documents (D.O.D 1987), and DoD Directive 5230.25 (D.O.D. 1984), Withholding of Unclassified Technical Data from Public Disclosure. DFARS, *supra* note 407, at 38092–94.

429. *Id.* at 38094.

NIST Special Publication ("SP") 800-53, set forth in a table in the Enhanced Safeguarding clause of DFARS 252.204-70YY;[430]

- Procure and use only DoD-approved identity authentication credentials for authentication to DoD information systems;[431]
- Report to the DoD "within 72 hours of discovery of any cyber incident . . . that affects DoD information resident on or transiting through the Contractor's unclassified information systems";[432] and
- Take specific actions in response to a reported cyber incident. The contractor must
  - "Conduct an immediate review of its unclassified network for evidence of intrusion . . .";
  - Identify specific DoD information accessed by the intrusion;
  - Preserve and protect "images of known affected information systems and all relevant monitoring/packet capture data until DoD has received the image and completes its analysis, or declines interest"; and
  - Cooperate with the DoD Damage Assessment Management Office to identify systems compromised.[433]

Cloud vendors' current standard-service-level or customer agreements would not enable a contractor and the contractor's outside legal counsel to fulfill such requirements. Since such agreements omit any obligation for the cloud vendor to report to the customer any data breach or intrusion or to allow for post-intrusion investigations by the customer, the contractor and its outside legal counsel could not fulfill the cyber intrusion reporting obligations of the Cybersecurity Rule's "enhanced safeguarding" clause. Furthermore, the cloud vendor service-level agreements would, in their current form, not enable a contractor and its outside legal counsel to implement the required security controls and identity authentication credentials.

It may be that the Cybersecurity Rule will be further revised in response to comments to address the possibility of contractors allowing the covered information to be processed and stored in the

430. *Id.* at 38094 tbl.1.
431. *Id.* at 38094.
432. *Id.* The clause specifies that reportable cyber incidents include those "involving possible data exfiltration or manipulation or other loss or compromise of DoD information resident on or transiting through its, or its subcontractors', unclassified information systems." *Id.*
433. *Id.* at 30895.

cloud, but unless such permissions are explicitly expressed in the rule, it would not appear possible for a contractor to fulfill its obligations under either the "basic safeguarding" or the "enhanced safeguarding" contract clauses. For the same reasons, a DoD contractor's outside counsel could not allow information from the contractor, subject to the Cybersecurity Rule, to be processed or stored in the cloud without putting its client at risk of breaching the Cybersecurity Rule's contract clauses, and, by doing so, putting counsel at risk of failing to fulfill its professional ethical obligations. As a result, a lawyer or law firm whose clients include, or might come to include, a DoD contractor or subcontractor would need to take extraordinary precautions to avoid allowing such client information from being included, processed, or stored in the cloud, if counsel had decided to use cloud computing services. Although we have drawn this illustration from the DoD, because of its apparent commitment to implementing a final version of the Cybersecurity Rule in the near future, similar regulatory obligations could be imposed by other federal or state agencies. Such obligations could make it difficult and costly for a lawyer or law firm if they belatedly reconsider whether it was prudent to use cloud computing for processing and storing client confidential information.

l. Potential Ethical Risks from Emerging Technology that Causes Digital Data to Self-Destruct

Computer scientists at the University of Washington developed a research prototype version of a technology, referred to as "Vanish," which encrypts digital records (including documents and e-mails), but also enables the author to set a time after which the digital data self-destructs.[434] Some web services reportedly already offer to perform a similar function, and "electronic devices like FLASH memory chips have added this capability for protecting stored data by automatically erasing it after a specified period of time."[435] With the Vanish technology, the digital data would have a fairly precise time frame within which the data would cease to exist. The subject digital data, such as a file, an e-mail, or an instant message, is "encapsulated" in what the researchers termed a

434. Geambasu et al., *supra* note 339, at 1.

435. *See* John Markoff, *New Technology to Make Digital Data Disappear on Purpose*, N.Y. TIMES, Jul. 21, 2009, at D3, *available at* http://www.nytimes.com/2009/07/21/science/21crypto.html.

"vanishing data object" or "VDO." This VDO prevents the data contents from persisting beyond a specified time, causing it to self-destruct, thus averting it from becoming "a source of retroactive information leakage."[436] The researchers claim that the self-destruction prevents an "attacker" from accessing the data once it has been "encapsulated" in a VDO. Regardless of whether the VDO is copied, transmitted, or stored in the Internet, it becomes unreadable after a predefined period of time even if an attacker *retroactively* obtains both a *pristine* copy of the VDO from before its expiration and all of the user's past persistent cryptographic keys and passwords.[437]

The specified period of the digital data's persistence, once encapsulated in a VDO, is quite limited—between eight and nine hours:

> By default, the data will be available with high probability for 8 hours after its encapsulation and will become unavailable with high probability after 9 hours. During the one hour between 8 and 9 hours, the data's state is undetermined: it could be available or unavailable, although it typically remains available for close to 9 hours.[438]

Once that time expires, the digital data become irretrievable from "all Web sites, inboxes, outboxes, backup sites and home computers. Not even the sender could retrieve them."[439] The process by which the digital data is encrypted and timed to self-destruct is as follows:

> The Vanish prototype washes away data using the natural turnover, called "churn," on large file-sharing systems known as peer-to-peer networks. For each message that it sends, Vanish creates a secret key, which it never reveals to the user, and then encrypts the message with that key. It then divides the key into dozens of pieces and sprinkles those pieces on random computers that belong to worldwide file-sharing networks, the same ones often used to share music or movie files. The file-sharing system constantly changes as computers join or leave the

436. Geambasu et al., *supra* note 339, at 4.

437. *Id.*

438. Jared Moya, *"Vanish" Uses BitTorrent to Make Data Disappear*, ZEROPAID (Aug. 10, 2009), http://www.zeropaid.com/news/86800/vanish-uses-bittorrent-to-make-data-disappear.

439. *See* Press Release, Hannah Hickey, Univ. of Wash., This Article Will Self-Destruct: A Tool to Make Online Personal Data Vanish (July 21, 2009), *available at* http://www.eurekalert.org/pub_releases/2009-07/uow-taw072109.php.

> network, meaning that over time parts of the key become permanently inaccessible. Once enough key parts are lost, the original message can no longer be deciphered.[440]

Because the researchers developed Vanish to avoid the risks arising from the fact that "users' sensitive data can persist 'in the cloud' indefinitely . . . sometimes even after the user's account termination,"[441] the main requirement for use of the technology is connectivity to the Internet during the "encapsulating"[442] and "decapsulating"[443] of a VDO.

The Vanish prototype deployed exists in three applications, each posing different ethical challenges to lawyers and law firms who are asked by clients to advise on the adoption and use of the technology. In one application, "FireVanish," the technology is implemented in a Firefox browser plugin for Gmail and enables the sender to encapsulate Gmail-based e-mails that could be "decapsulated" by the recipient, provided the recipient does so before the VDO times out and causes the e-mail to self-destruct.

In a second application, "FireVanish Extension for the Web," the technology is implemented through a Firefox browser plugin that enables the user to "select text in any Web page input box, right click on that selected text, and cause FireVanish to replace that text *in-line* with an encapsulated VDO."[444] By that process, a user can cause "messages on Facebook, documents on Google docs, or instant messages on Google Talk" to self-destruct when the VDO time limit expires.[445]

In the third, and probably the most ethically problematic application, "Vanishing Files," the technology could create a "self-destructing trash bin" or self-destructing Microsoft Word autosave.[446] Files moved to a computer's "trash bin" or that have been backed up using Word's autosave would be collectively or individually wrapped in a VDO, and when the VDO expires, the cleartext of each file would be deleted from the storage disk and the VDO would be stored in place of the files.[447] Apparently, a very important arena for concern, a subsequent mirror image made of

---

440. *Id.*
441. Moya, *supra* note 438.
442. Geambasu et al., *supra* note 339, at 10.
443. *Id.* at 7 (explaining decapsulation as recovering cleartext back from a VDO).
444. *Id.* at 10.
445. *Id.*
446. *Id.*
447. *Id.*

the disk as part of a court-supervised e-discovery or a government investigation would be unable to recover the cleartext of the files, for as the researchers explain (referring to the party seeking the data as an "attacker"):

> This ensures that, even if an attacker copies the raw bits from the laptop's disks after the timeout, the data within the VDO will be unavailable. Like traditional file encryption, Vanishing Files relies upon existing techniques for securely shredding data stored on disks or memory.[448]

Although the researchers claim that, with their technology, "users can regain control over the lifetimes of their Web objects, such as private messages on Facebook, documents on Google Docs, or private photos on Flickr," their paper on the subject shows seemingly subversive interest in helping litigants evade the reach of lawyers and e-discovery processes.[449] For example, their paper provides the following text to a figure depicting the operation of the technology:

> Ann wants to discuss her marital relationship with her friend, Carla, but does not want copies stored by intermediate services to be used in a potential child dispute trial in the future . . . . The screenshot shows how Carla reads a vanishing email that Ann has already sent to her using our Vanish Email Firefox plugin for Gmail.[450]

The accompanying figure shows Ann and Carla linked by Hotmail and Gmail servers that are surrounded by a "cloud" outside of which is a frowning emoticon labeled "Husband's lawyer" and above which are the words "Future subpoena," suggesting that the technology could enable the sender to evade or circumvent court ordered discovery processes.[451] Moreover, in a section entitled "Avoiding Retroactive Privacy Attacks," the researchers reveal that undermining the legal discovery process is actually one of their primary motivations for development of Vanish.[452] They do not appear to have a high opinion of lawyers and judges' efforts to develop ways to manage e-discovery, or of the salient importance to fair trials or the access to, and admissibility of, contemporaneously generated written records. As they explain:

---

448. *Id.*
449. *Id.* at 1.
450. *Id.* at 2.
451. *Id.*
452. *See id.* at 11.

> **Attackers.** Our motivation is to protect against retroactive data disclosures, e.g., in response to a subpoena, court order, malicious compromise of archived data, or accidental leakage. For some of these cases, such as the subpoena, the party initiating the subpoena is the obvious "attacker." The final attacker could be a user's ex-husband's lawyer, an insurance company, or a prosecutor. But executing a subpoena is a complex process involving many other actors . . . . For our purposes, we define *all* the involved actors as the "adversary."
>
> . . . .
>
> **Deployment Decisions** . . . . Vanish is oriented towards personal users concerned that old emails, Facebook messages, text messages, or files might come back to "bite" them . . . .[453]

The researchers acknowledge that lawyers have advised them that, as they express it,

> 'Vanish is ahead of the law.' Specifically, Vanish in some commercial or government settings may raise interesting issues related to eDiscovery and public record laws.
>
> . . . .
>
> . . . [I]t is not absolutely clear what the legal implications of using Vanish might be.
>
> . . . .
>
> To the best of our knowledge, however, it is OK to use Vanish for personal purposes in the U.S. assuming that the user is not involved in a legal proceeding nor is expecting to be involved in a legal proceeding . . . . Some legal scholars have, however, observed that – because of their ephemeral nature – VDOs by design are more like 'conversations' than 'documents.' Data retention laws may therefore not apply to Vanish. However, we stress again that we are not lawyers.[454]

---

453. *Id.* at 11–12.

454. *Frequently Asked Questions*, VANISH [hereinafter Old_vanish_faq.html] (previously published copies of the Vanish FAQ on file with the authors). The authors would like to thank Professor Geambasu for providing us with a copy of the "old_vanish_faq.html" file and for re-posting the paper she and her University of Washington colleagues wrote in 2009 after our inquiry to her about its whereabouts. For some additional analysis of Vanish, see *Self Destructing Digital Data*, P2PNET, http://www.p2pnet.net/story/26730 (last visited Oct. 20, 2011).

i. Analysis of Ethical Issues

The developers of the new self-destructing digital data technology are clearly aware that use of such technology might cause the destruction of electronic records during a legal proceeding, or in anticipation of a lawsuit, or during investigation, and would raise serious ethical issues for any lawyer advising a client, because such actions would likely result in a judicial finding of spoliation and possibly severe sanctions. It is troubling that the researchers do not appear to recognize the value of contemporaneously generated records, and the greater accuracy and credibility that such records have when compared to a witness testifying on the basis of limited (and potentially biased) memory months or years after an event as to what may or may not have been communicated between parties on matters at issue in the litigation or investigation. Given the widespread reportage of parties suffering adversely from introduction into evidence of their electronic communications,[455] it should be anticipated that self-destructing digital data technology could come into popular use rather rapidly. Since the technology is already available, it is prudent to consider the potential ethical issues before clients become tempted to use it without consulting legal counsel.

If a lawyer is representing a client in a lawsuit or government investigation, or a client who reasonably anticipates the start of a lawsuit or government investigation, the lawyer should not advise the client to use any technology that would cause a communication of potential relevance to the lawsuit or investigation to self-destruct. Doing so would have the effect of suppressing evidence that the client is required to preserve and may be required to produce in the lawsuit or investigation. To assist in such conduct would likely violate NYRPC Rule 3.4(a)(1), which mandates that a lawyer shall not "suppress any evidence that the lawyer or the client has a legal obligation to reveal or produce."[456]

MRPC Rule 3.4(a) contains a slightly different mandate. The

455. See Tracey Tyler, *Email Evidence is Changing the Law,* TORONTO STAR (June 9, 2007), http://www.thestar.com/news/article/223386, for a non-comprehensive account of cases in which e-mail evidence has been determinative. As John M. Barkett observes, "[o]ne example that occurs frequently is the production of privileged records. As one commentator explains, 'E-discovery increases the potential for inadvertent production of privileged information. Producing parties typically do not have mechanisms in place to retrieve, restore, and cost-effectively identify electronically stored information that is privileged.'" JOHN M. BARKETT, THE ETHICS OF E-DISCOVERY 19 (A.B.A. 2009).

456. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 3.4(a)(1) (2011).

MRPC states that a lawyer shall not "unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having *potential* evidentiary value."[457] MRPC Rule 3.4(a) clearly encompasses the preservation of evidence based on the anticipation of litigation. The stated purpose of the rule is to maintain fair competition in litigation.[458] VDOs, clearly undermine the purpose of MRPC Rule 3.4(a).

There would appear to be little or no genuine support for the researchers' claim that written communications that have been "encapsulated" as VDOs are "more like 'conversations' than 'documents.'"[459] A lawyer who relied on that argument as the basis for his or her advice that such records were not subject to data retention duties under the applicable federal rules would be in violation of the prohibitions against suppressing evidence that the client has a legal obligation to produce contained in NYRPC Rule 3.4(a)(1) and MRPC Rule 3.4(a).

If the lawyer was aware that such an argument was without merit, then in advising a client to use a digital record self-destruct technology during a "litigation hold," for example, the lawyer also would be at risk of violating either NYRPC Rule 3.2 or MRPC Rule 3.2 on delay of litigation. NYRPC Rule 3.2 states: "In representing a client, a lawyer shall not use means that have no substantial purpose other than delay or prolong the proceeding or to cause needless expense."[460] MRPC Rule 3.2 contains a broader requirement that a "lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client."[461] MRPC Rule 3.2 was intended to encompass tactics used for the sole purpose of frustrating an opposing party's attempt to seek redress, even where the conduct would otherwise not bring the lawyer into conflict with the rules of the court.[462] In defending a client's use of vanishing data objects, a lawyer must therefore be aware of the boundaries of the lawyer's own ethical requirement in court.

More problematic are the potential ethical issues that might arise in the context of a corporate client asking whether it should adopt a digital data self-destruct technology for use in sending confidential communications, whether those are internal or with

457. MODEL RULES OF PROF'L CONDUCT R. 3.4(a) (2007) (emphasis added).
458. *See id.* cmt. 1.
459. Old_vanish_faq.html, *supra* note 454.
460. N.Y. COMP. CODES R. & REGS. tit. 22, § 1200, R. 3.2.
461. MODEL RULES OF PROF'L CONDUCT R. 3.2 (2007).
462. *See id.* at cmt. 1.

strategic allies in ongoing transactions. In the era before clients generated electronic records when they sent written communications, counsel would sometimes advise that clients not make any notes on such documents and that they place their notes instead on Post-Its that the client could remove a few days or weeks later. However, the new digital data self-destruct technology would affect the durability of the basic communication itself, not merely notes concerning it. And since the durability is limited to a mere eight or nine hours, the technology may make a poor choice for the kind of corporate communications needed for transactions and negotiations.[463] There would be many situations in which a client is far better served by creating a durable communication, because it may need such a record as evidence to support its position in the event of litigation.

However, what if the client has started to become apprehensive about a transaction that could turn into a legal dispute, but has not developed so clearly in that direction as to require the issuance of a "litigation hold"? The client wants to communicate internally about what it describes as "litigation avoidance" strategies, but which also contain elements of strategies to position the client in the event that litigation breaks out. Clients, of course, can be advised to communicate orally, but not in writing, in order to avoid creating a written record that could be misinterpreted or adverse to the client and that might have to be produced during an ensuing discovery. In such circumstances could counsel advise the client to make selective use of a digital data's self-destruct technology to ensure that any written communications that might otherwise be discoverable would destruct within eight or nine hours and, thus, not even exist by the time a litigation hold would be issued?

Advising a client to avoid making a written record does not promote a course of action that results in spoliation of evidence. Similarly, advising a client to implement and adhere to a "document retention" policy with routine destruction of documents in accordance with an established timetable (such as purging all records that are older than a set number of years) does not constitute spoliation of evidence, unless the lawyer fails to ensure that when a litigation hold is issued the document retention

463. *See* Geambasu et al., *supra* note 339, at ¶ 5.1 ("Nodes further remove from their caches all values whose store timestamp is more than 8 hours old. This process has a 1 hour grade period. The originator node must re-push its 8 hours old (index, value) pairs if it wishes to ensure their persistence past 8 hours.").

policy is suspended promptly and throughout the client's enterprise. Those are quite different from a hypothetical in which the client asks for its lawyer's approval of the use of a digital data self-destruct technology for written communications that may become relevant to a law suit whose potential is the subject of such communications. Here the conduct, while perhaps not illegal, appears to cross the line into the unethical. To recommend the use of such technology (which is precisely the situation in which the researchers appear to recommend that customers use their technology) would pose a serious risk of violating both MRPC Rule 8.4(c) and (d) as well as NYRPC Rule 8.4 (c) and (d), both of which mandate that a lawyer or law firm shall not "engage in conduct involving dishonesty, fraud, deceit or misrepresentation" or "engage in conduct that is prejudicial to the administration of justice."[464]

The ethical issues become potentially more perilous if the digital data self-destruct technology is used to eradicate and remove all traces of files moved to a computer's "trash bin." Clients facing a government investigation or a lawsuit and harboring doubts about the use that might be made by the government or adversaries of certain files might give serious consideration to making a "last minute" sweep of such files into a computer's "trash bin" that has been equipped with a "Vanishing Files" feature. The most likely ethical risk here for the client's lawyer(s) and law firm is not that the lawyers or law firm would have advised the client to take such action, but that the lawyers or law firm, aware of the technology and of the client's adoption of it, failed to oversee the "litigation hold" with sufficient vigilance to prevent any personnel of the client from causing such files to be encapsulated in a VDO and letting them to self-destruct when that VDO expires a few hours later. Because a client's litigation or trial counsel have a duty to oversee, and not merely to help issue, a "litigation hold" notice through the client's enterprise, and since counsel are also responsible for familiarizing themselves with the client's information technologies, such as those that perform back-ups and overwrites of electronic records (and to avert inadvertent destruction of potentially relevant records), such duties would appear to extend also to knowing of the existence, operation, and use of a digital data self-destruction technology.

Failing to develop that knowledge and to avert the misuse of it

464. N.Y. RULES OF PROF'L CONDUCT R. 8.4(c), 8.4(d) (2009).

to circumvent electronic discovery obligations would create grounds for a finding of spoliation, but could constitute a violation of NYRPC Rules 3.4(a)(1) (suppressing evidence), 8.4(c) (conduct involving deceit), and 8.4(d) (conduct prejudicial to the administration of justice). Such conduct also would implicate the corresponding MRPC rules.

ii. Considerations and Precautions

In light of the potentially disruptive effect that digital data self-destruction technology could have on a client's fulfillment of its electronic discovery duties and the adverse consequences that could result, it would be prudent for lawyers and law firms to familiarize themselves with the technology and to monitor closely its development and use. Clients that may be considering adopting the technology should be encouraged to develop clear policies for the use and cessation of use of the technology in order to avoid the risk of spoliation. Similarly, it would be prudent for law firms to develop internal policies that would educate associates who might fail to appreciate the risks of advising that a client use such technology when doing so might potentially be a disservice to the client, but might create ethical risks for the associate, the partner supervising the associate, and the law firm. Moreover, although the researchers use highly persuasive metaphors to tout the technology (e.g., using Vanish is like "writing a message in the sand at low tide, where it can be read for only a few hours before the tide comes in and permanently washes it away"),[465] it is important to notice that such metaphors can mislead as well as persuade, and that to the extent that they suggest that use of the technology is simply a "conversation" and not the creation of a "document" it is seriously misleading and ethically hazardous for lawyers and law firms who might not closely scrutinize the technology in the context of electronic discovery obligations.

Most importantly, the emergence of digital data self-destruction technology brings with it an implicit duty for lawyers and law firms (especially litigation counsel but also others who may advise during a pre-litigation phase) to familiarize themselves with the technology, the ways in which its touted capabilities may encourage a client to use the technology to the client's serious disadvantage (since spoliation often turns out to be a form of self-sabotage), and the extent to which the client may have made such

465. Hickey, *supra* note 439.

technology available to its personnel. The risks of misuse of such technology arise directly from the kinds of claims that the researchers make for their technology: that it can spare the user from getting "bitten" by correspondence and documents authored by the user. That view is not only short-sighted, but it also seriously misperceives and distorts the legal obligations that many corporate clients have to preserve records of transactions and to preserve potentially relevant evidence in anticipation of litigation or government investigation. Part of understanding a new communications technology is becoming aware of its potential appeal. Counsel also needs to understand that clients may be tempted to adopt the new technology in the mistaken belief that they are thereby going to escape the consequences of communications that may harm them in litigation.

V. WAVES OF RECENT CYBER-ATTACKS HAVE CHANGED THE INFORMATION SECURITY LANDSCAPE

Prior to submitting this article, several high-profile security incidents occurred.[466] The rapidity and intensity of such incidents suggests that cyber service vendors and subscribers of their services may be underestimating the vulnerabilities of, threats to, and risks for a company's digital assets (1) stored on its premises (but that remain accessible by attackers through the Internet because the storage media of such assets are not "air gapped" from it) and (2) stored in the cloud. These reported incidents and the trends that they suggest make it increasingly difficult for an organization to make a definitive risk assessment for its digital assets, because such incidents may provide evidence of assumptions and analyses that have obsolesced much earlier than anticipated and may need to be updated before making a major decision that relies upon them. As some commentators noted in mid-June 2011:

> The roster of hack victims over the last two weeks has been spectacular: the International Monetary Fund, the Central Intelligence Agency, Sony, the Turkish government, Citibank and the US Senate inter alia. If it wasn't obvious before, events in cyberspace have made it abundantly clear there are only two types of company in the world—*those that know they've been hacked and those that*

466. *See, e.g.*, Ian Sherr, *Hackers Breach Second Sony Service*, WALL ST. J., May 3, 2011, at B1; Jonathan Soble, *Sony Battles Further Hacker Attacks*, FIN. TIMES, May 25, 2011, http://www.ft.com/intl/cms/s/2/d4b34df2-86a1-11e0-9d41-00144feabdc0.html#axzz1e5e4QEHR.

> *don't* . . . . It is axiomatic that companies should have the security of their electronic networks at the top of their agenda . . . . [Notwithstanding the latest governmental and military safeguards] networked computer systems have never been more vulnerable.[467]

These attacks should dispel remaining doubts that enterprises are vulnerable to cyberattacks. The attacks also reveal that public clouds add to the vulnerability of enterprises that migrate data to the cloud. As another commentator observed:

> Recent high-profile hacking attacks, such as the theft of more than 100m customers' details from Sony and a four-day outage at Amazon that took down thousands of websites, have done nothing to reassure companies about the security of cloud computing . . . . Ryan Rubin, U.K. head of security and privacy at Protiviti, an IT security company says: 'There aren't many people putting mission-critical data in the cloud. The crown jewels—customer records, for example—are still very much embedded in the organization.' A director at one London investment bank says: 'We use the cloud for things such as e-mail. We would never put our client services on it.'[468]

As a result, decisions involving transactions based on due diligence assessments of the short- and long-term security of digital assets now appear increasingly to resemble decisions in corporate transactions where the findings of due diligence investigations completed before the signing of definitive contractual agreements are updated and reviewed to verify compliance with conditions for closing the deal. Similarly, because the addition of an information technology capability (whether it be in the form of a new web page, mobile app, or cloud-based feature) creates the potential for numerous new routes for attackers, it may be increasingly important for negotiators of corporate transactions to include consideration of a freeze on such additions or a closely monitored and evaluated reporting of such additions between the signing and the closing of major transactions. A recent observation by the chief executive of Korea's Hyundai Capital further acknowledges the growing risks of cyber attacks and the importance of technology risk assessment in corporate planning.[469]

---

467. Misha Glenny, *We Must Learn How the Hackers Think*, FIN. TIMES, June 17, 2011, http://www.ft.com/intl/cms/s/0/bf28f5a8-990d-11e0-acd2-00144feab49a.html#axzz1XaLHYSKt (emphasis added).

468. Maija Palmer, s*upra* note 7.

469. *See supra* text accompanying note 195.

VI. MOST RECENT RECOMMENDATIONS FROM NIST

When boards of directors and their legal counsel try to understand and assess the significance of security incidents at other organizations and the ethical challenges such incidents may add to an enterprise's decisions concerning the use of web-based and cloud-based communications, data processing, and storage, it would be prudent for them to include in such a review the comments and recommendations contained in NIST's "Cloud Computing Synopsis and Recommendations", Special Publication 800-146 (the "Cloud Synopsis"). The Cloud Synopsis was published in May 2011 as we were revising this article. Since time and space constraints preclude a full discussion of the Cloud Synopsis, in this part of the article, we summarize some of its most significant observations and recommendations.

NIST's Cloud Synopsis endeavors to describe the current types of cloud computing and to discuss their strengths and weaknesses. In doing so, the draft's most significant contribution may be its highlighting of certain problematic views of the cloud, starting with NIST's own earlier proposed definition of cloud computing. "Attempts to describe cloud computing in general terms . . . have been problematic because cloud computing is not a single kind of system, but instead spans a spectrum of underlying technologies, configuration possibilities, service models, and deployment models."[470]

NIST's Cloud Synopsis identifies the following security considerations that businesses would be prudent to consider carefully when deciding whether to move part or all of their digital assets and digital processing into the hands of a cloud computing service provider.

- *Aggregated data:* "Clouds . . . have potential to aggregate an unprecedented quantity and variety of customer data in cloud data centers. This potential vulnerability requires a high degree of confidence and transparency that cloud providers

470. NIST CLOUD SYNOPSIS, *supra* note 13, at ES-1. The NIST Cloud Synopsis now identifies five essential characteristics of cloud computing: on demand service, broad network access, resource pooling, rapid elasticity, and measured service. *Id.* at 2-1. The NIST Cloud Synopsis elaborates on NIST's definition of cloud computing by describing three service models (cloud software as a service (SaaS), cloud platform as a service (Paas), and cloud infrastructure as a service (IaaS), together with four deployment models: private cloud, community cloud, public cloud, and hybrid cloud. For more information about these characteristics, see text accompanying notes 161 to 164, *supra*.

can keep customer data isolated and protected."[471]

- *Reliance on web browsers:* "Cloud users and administrators rely heavily on Web browsers, so browser security failures can lead to cloud security breaches."[472] The security risks may begin at the handshake. The subscriber's browser and cloud provider's server start by negotiating a shared key and then use that key to encrypt communications between the subscriber and the cloud. However, this reliance on encryption offers only limited protection, "because past implementation errors or protocol flaws have enabled man-in-the-middle attacks that could allow an attacker to hijack a subscriber's cloud resources.[473] Moreover, strong encryption is susceptible to weakening by implementation errors, making "brute force guessing attacks" more likely to succeed.[474]
- *Importance of access boundaries:* The NIST Cloud Synopsis adopts the concept of "access boundaries to organize and characterize the different cloud deployment models."[475] NIST uses the term to refer to both an external boundary (such as enforced, in part, by firewalls) and more generically to boundaries "between different privilege levels of running software, e.g., between applications and operating systems." NIST emphasizes the need to avoid uncontrolled access paths—those without sufficient access boundaries:

  > When uncontrolled paths to computing resources exist, a security perimeter is weakened or may not even exist. Pervasive wireless communications, e.g., are a threat to security perimeters since there may be no reliable way to interpose a boundary controller between external and internal entities. Similarly, many organizations use mobile devices that are sometimes connected within an organization's security perimeter, and sometimes exposed directly, e.g., when on travel.[476]

- *Superior security of physical separation over logistical separation:* In U.S.-based nuclear power plants, sensitive data such as that related to the "design basis threat" and a plant's counter-measures and safeguards are secured by ensuring that they are

471. *Id.* at ES-2.
472. *Id.*
473. *Id.* at 5-1.
474. *Id.* at 5-5.
475. *Id.* at 4-3.
476. *Id.* at 4-3, n.5.

> "air gapped" from the Internet and not allowed to be on systems that communicate wirelessly. Such practices demonstrate the reliability of physical separation. Cloud computing services, however, rely instead on logistical separation for security, which is inherently less reliable. As NIST's Cloud Synopsis explains, "One aspect that is pervasive in cloud systems, however, is reliance on 'logistical separation', as opposed to 'physical separation' of user workloads, and the use of logical mechanisms to protect subscriber resources . . . [A]nd logical separation has not been shown to be as reliable as physical separation . . . ."[477]

- *Software and missions that are unsuitable for SaaS:* Decisions concerning use of cloud computing should consider the potential for a mismatch between the limits of cloud computing and the needs of the user. As the NIST Cloud Synopsis explains, "Different types of applications require differing levels of system performance. For example, email is generally tolerant of short service interruptions, but industrial automation and real-time processing generally requires both high performance and a high degree of predictability."[478] The authors observe, however, that even e-mail is not always tolerant of seemingly short delays. Certain company managers in high tech enterprises are known to expect immediate replies to their internal e-mail, which may become an impossible to meet expectation for subordinates whose receipt of replies are held up in a cloud computing message traffic bottleneck. Moreover, a manager will have no reliable way of verifying whether the delay was due to the subordinate or to the cloud. As the NIST Cloud Synopsis also noted, "Subscribers may lack visibility into how clouds operate. If so, they will likely be unable to tell if their services are being undertaken and delivered in a secure manner."[479]

NIST's Cloud Synopsis points out three key examples of mismatches involving potential migration to public SaaS. First, are operations required in real-time, such as flight control systems or factory robot controls. Because such operations require precise timing and coordination to complete tasks on reliable, recurrent times, they are unsuitable for SaaS, which can offer only variable response times. Moreover, additional delays and mis-timings can occur as a result of "unavoidable round trip delays for messages to be exchanged between SaaS subscribers and cloud providers."[480]

---

477. *Id.* at 8-7.
478. *Id.* at 8-1.
479. *Id.* at 8-5.
480. *Id.* at 5-8.

Imagine a combat pilot or submarine executive officer looking at a data display screen and suddenly realizing that the updates or refresh rates have ceased to be predictable, rapid, and that they are no longer making decisions based on real-time updates to the tactical picture. Increasingly businesses operate in a similar environment and such businesses should be cautious in placing themselves and their decision makers in a position where they believe they are acting upon real-time information when it is, in fact, being significantly delayed in updates, is being refreshed at irregular intervals, and may be obsolete at the time a critical decision needs to be made based on such data.

Second, are bulk-subscriber operations, such as monitoring of medical devices. These can generate suddenly high volumes of data that become infeasible for transfers in real-time over wide area networks to a SaaS provider. Businesses that need to be responsive to developments in economic or political crises, such as the trading of shares on a public exchange, might similarly find that the delays in response time would prove so costly as to outweigh the anticipated cost savings of migration to cloud computing.[481]

Third, are mission critical operations where a failure would impose intolerable consequences. Because avoidance of complexity is a key engineering strategy for reducing software failures, such a strategy is ill-suited for SaaS applications, which "depend on proper operation of a large and complex software stack that includes a network" and there are "no guarantees" that can be given that the "network will continue to provide acceptable levels of service."[482]

- *Cloud complexities increase vulnerabilities:* Cloud computing systems, by structure and operation, tend to be complex, and, as a result "prone to failure and security compromise."[483] The marketing promises of cloud service providers can be tested by comparing them to the disclaimers for reliability and security that the same providers insist upon in their standard Service Level Agreement, suggesting that the tendency of such systems to fail and to be breached by attackers is too high for the vendors themselves to accept and be financially responsible for. Potential subscribers need to be aware of the inherent weaknesses of cloud computing, which include the fact that:

> [S]oftware that must accommodate complex requirements such as concurrency, dynamic configuration, and large scale computations, may

481. *Id.*
482. *Id.*
483. *Id.* at 8.

> exhibit higher defect densities than typical commercial grade software. With this in mind, it is important to understand that cloud systems, like all complex computing systems, will contain flaws, experience failures, and experience security compromises. . . . [Therefore] techniques for detecting failures, understanding their consequences, isolating their effects, and remediating them, are central to the wide-scale adoption of clouds . . . . The technical means of providing the quality of service promised are usually not disclosed to the subscriber, thus raising questions about how subscribers can verify that the promised quality of service level has been provided.[484]

- *Difficulty of measuring a cloud's reliability:* Any decision concerning the migration to a cloud computing service should be based, in part, on an evaluation of the reliability needed and the reliability that the cloud computing service can be depended on to provide. Negotiating a Service Level Agreement on that issue for a customer can be compromised by the difficulties of measuring a cloud's reliability, both historically prior to the negotiations and during contract performance. The sources of the difficulties, as the NIST Cloud Synopsis explains, are as follows:

> > Reliability refers to the probability that a system will offer failure-free service for a specified period of time within the bounds of a specified environment. . . .
> >
> > Note that measuring the reliability of a specific cloud by the provider or subscriber will be difficult for two reasons. First, a cloud may be a composition of various components, each inheriting a particular degree of reliability when it was measured as a standalone entity. When these components are combined the resulting reliability is difficult to predict and may wind up being too course-grained [sic]. Secondly, reliability measurement is a function of an environment in which a cloud operates. . . . For clouds, and most systems of significant scale, each component has a specific reliability given a specific context, and therefore understanding the union of the contexts is complex and possibly intractable.[485]

  The authors recommend that Boards ask their counsel to test

484. *Id.* at 8.
485. *Id.* at 8-2.

the marketing promises of cloud service providers by comparing them to the disclaimers of reliability and security that the same providers insist upon in their standard Service Level Agreements. Where disclaimers of cloud performance undercut a promised level of performance, it is reasonable to infer that the vendor anticipates that the tendency of such systems to fail and be breached by attackers is too high for the vendors themselves to afford and they, therefore, shift this risk to customers. The customer's negotiation of a Service Level Agreement should include a careful comparison of the cloud vendor's performance promises and the cloud vendor's disclaimers in order to ensure that the customer is not tempted to believe it will be receiving performance promised by one section that another section gives the vendor a basis for denying. Where such inconsistencies exist they create the kind of ambiguity that can deprive a customer of the benefits of its bargain and increase the likelihood of serious disagreements with the vendor that could lead to costly litigation. A customer should insist on such inconsistencies being removed, and should be careful that the price of the vendor's services are re-evaluated in light of the results of the negotiation of such inconsistencies, since the benefits may have been diminished to the point where the price needs to be adjusted downward accordingly. If those terms are intractable, the assumptions on which the negotiations are based are not verifiable. If a cloud's performance levels cannot be measured and verified, the customer may be paying for rights to performance it will not be able to enforce.

VII. CONCLUSION

Web 2.0 communications technologies, cloud-based applications, and cloud computing deserve careful review by lawyers and law firms. Their rapid adoption may occur without a full awareness of the potential ethical risks or without adequate safeguards having been put in place to mitigate the likelihood that the vulnerabilities may give rise to security risks and ethical problems. The potential problems include:

- A lawyer's use of Twitter to advertise the lawyer's firm or practice without including, as required under the NYRPC, "attorney advertising."
- A lawyer's use of Twitter to make extrajudicial comments concerning an ongoing trial in which the lawyer is participating and that may have a substantial likelihood of materially prejudicing an adjudicative proceeding in the

matter.

- A law firm associate receives a "tweet" announcing a political rally and believes that she will be participating in a political demonstration, but it turns into a "flash mob" (like those that recently occurred in the U.K.) and she is arrested for having re-tweeted the invitation and contributing to the ensuing riot, injuries, and property damage.
- A lawyer's posting on a LinkedIn page a description of the lawyer as a "specialist" in a particular field or as "specializing" in such field without meeting the stringent conditions for such terms under the NYRPC.
- A lawyer's private Facebook page used in a manner that reflects adversely on the lawyer's character.[486]
- A lawyer's use of Facebook to communicate with a party represented by counsel without that counsel's consent.
- A lawyer's posting of an entry in a blog noting that a particular defendant has been charged with a crime, but failing to add a statement explaining that the charge is merely an accusation and that the defendant is presumed innocent until and unless proven guilty.

These situations and numerous others have the potential to cause easily overlooked ethical issues under applicable rules of professional conduct.

Counsel will need to monitor the ever-changing security environment of social networking sites. One method for such monitoring is to observe how the security environment is perceived by security experts engaged in efforts to test the cloud platforms for vulnerabilities. Other organizations treat the security of the data they possess as among the highest of priorities. Reports by such experts can provide the basis for due diligence examinations of prospective vendors of cloud services under consideration by a law firm.[487] A second method for monitoring the security environment

---

486. Material that may reflect adversely on a lawyer's character or involve disclosure of confidential information can be posted even without a lawyer's direct involvement, such as by a member of the lawyer's family who has access and authorization to place information on a Facebook page. *See, e.g.*, *MI6 Boss in Facebook Entry Row*, BBC NEWS (July 5, 2009, 10:34 GMT), http://news.bbc.co .uk/2/hi/8134807.stm (noting that a British diplomat's personal life details, including information about his children and the location of the family's flat, were posted on Facebook by spouse).

487. Such reports could include those from security conferences where findings of security deficiencies are announced and explained. *See, e.g.*, Joseph Menn, *Data Security Services Under a Cloud*, FIN. TIMES, Aug. 3, 2009, http://www.ft.com/intl/cms/s/0/5aa4f33e-7fc4-11de-85dc-00144feabdc0.html

is to observe the extent that such organizations have assessed the risks of social networking sites as unacceptably high. Despite the security precautions, such assessments should alert law firms and lawyers of the need to audit the security of the use of such sites by their personnel to ensure that the safeguards in place are reasonable in light of the risks recognized by organizations that have concerns for the safety of their data. There is, unfortunately, no existing single standard or one organization that sets a "gold standard" for risk assessments of social networking sites, cloud-based applications, or cloud computing. Moreover, organizations that have a high regard for the safety of their data and personnel are currently drawing conflicting conclusions with respect to whether such risks are tolerable or intolerable. For example, on August 9, 2009, the Marine Corps issued a one-year ban on use by its personnel of social networking sites (SNS) (even if access was through a virtual private network), citing the unacceptably high risks that such sites introduce:

> THESE INTERNET SITES IN GENERAL ARE A PROVEN HAVEN FOR MALICIOUS ACTORS AND CONTENT AND ARE PARTICULARLY HIGH RISK DUE TO INFORMATION EXPOSURE, USER GENERATED CONTENT AND TARGETING BY ADVERSARIES. THE VERY NATURE OF SNS CREATES A LARGER ATTACK AND EXPLOITATION WINDOW, EXPOSES UNNECESSARY INFORMATION TO ADVERSARIES AND PROVIDES AN EASY CONDUIT FOR INFORMATION LEAKAGE THAT PUTS OPSEC, COMSEC, PERSONNEL AND THE MCEN AT AN ELEVATED RISK OF COMPROMISE. EXAMPLES OF INTERNET SNS SITES INCLUDE FACEBOOK, MYSPACE, AND TWITTER.[488]

Four days earlier, on August 5, 2009, the U.K. Ministry of Defence (MoD) announced a policy that, contrary to that which was issued by the Pentagon, encouraged its personnel to "make full

---

(discussing security problems presented at the Black Hat USA security conference).

488. *Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET*, MARINES (Aug. 3, 2009), http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx. *See generally* David Gelles, *Marines Ban Social Networking Sites*, FIN. TIMES, Aug. 4, 2009, http://www.ft.com/intl/cms/s/2/6bc60434-812f-11de-92e700144feabdc0.html#axzz1XaLHYSKt (reporting on the Pentagon's concerns with the use of social networking sites, including incautious use by members of Congress when making confidential visits to U.S. military installations).

use of online presences" available through SNS, "but within certain limits to protect security, reputation and privacy."[489] In order to promote that policy, the MoD published "Online Engagement Guidelines" for such activities.[490]

As Web 2.0 technology becomes more deeply entrenched in commercial and corporate enterprises, lawyers and law firms need to keep abreast of the changes in the legal rules and their interpretation as applied to such technology. For example, the E.U.'s Article 29 Data Protection Working Party ("Working Party") in June 2009 issued an opinion on "online social networking" that noted, among other points, that the Data Protection Directive ("Directive") applies to social network sites, even if its headquarters are located outside the European Economic Administration.[491] Moreover, a law firm's associates who use an online social networking site can become responsible for fulfilling data controller responsibilities under the Directive if such an associate, as a user of the social network, "takes an informed decision to extend access beyond self-selected 'friends' [then] data controller responsibilities come into force."[492] U.S. law firms with offices in Europe, and European law firms with offices in the United States, may find that the Working Party's opinion on that issue may necessitate a review of the policies such firms have adopted for use of social networks by their associates. Additionally, it is prudent to counsel clients to make similar reviews of their policies for employees' use of online social networks.

In addition, the increased use of Web 2.0 communications raises the risks that clients, their counsel, or both, will find that their activities have unexpectedly come within the jurisdictional reach of foreign jurisdictions, subjecting them to potentially adverse consequences. If a law firm or lawyer fails to apprise a client of such risks in circumstances where counsel knew of the facts that made those risks apparent, ethical issues might arise

489. *Online Engagement Guidelines*, UK MINISTRY OF DEFENCE, 1–2 (Aug. 5, 2009), http://www.mod.uk/NR/rdonlyres/D2AC8314-3B15-4DEB-A769-6C85AF4BDA80/0/20090805UMODOnlineEngagementGuidelinesVersion10.pdf.

490. *Id.*

491. Press Release, Article 29 Working Party, Article 29 Data Prot. Working Party (June 25, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/news/docs/pr_25_06_09_en.pdf (rendering an opinion on online social networking).

492. Opinion 5/2009 on Online Social Networking, Article 29 Data Prot. Working Party, at 6 (June 12, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (discussing access to profile information).

concerning the competency of the representation. Although there may be instances in which the electronic communications at issue may not have originated with the person alleged to have sent them, instant messages and text messages have been deemed admissible by appellate courts when the appropriate foundation has been laid (e.g., through circumstantial evidence).[493] Examples of parties surprised by the jurisdictional consequences of their use of electronic communications technologies include the following:

- A senior investment officer of the Montana Board of Investments (MBOI) negotiated through a series of instant messaging exchanges an agreement for a $15 million sale of its client's holdings of Pennzoil bonds to Deutsche Bank Securities, Inc. ("DB") in New York.[494] When MBOI subsequently cancelled the sale, DB sued for breach of contract in New York Supreme Court.[495] MBOI moved for dismissal, contending that New York's "long-arm statute" did not reach MBOI in Montana for these activities.[496] The supreme court granted the motion and dismissed for lack of personal jurisdiction.[497] The appellate division reversed.[498] On MBOI's appeal, the court of appeals noted that New York's "'long-arm statute" was a "single act statute" and emphasized that "proof of one transaction in New York is sufficient to invoke jurisdiction, even though the defendant never enters New York, so long as the defendant's activities here were purposeful and there is a substantial relationship between the transaction and the claim asserted.'"[499]
- A California client who communicated with her New York lawyer via telephone, faxes, and e-mails created a continuing relationship with that lawyer and thereby projected herself into New York's legal services market; this was sufficient to

493. *See, e.g.*, United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (rejecting challenges to admission of instant messages); People v. Pierre, 838 N.Y.S.2d 546, 548 (App. Div. 2007) (holding that trial court properly admitted text message authenticated by circumstantial evidence); In the Interest of F.P., 878 A.2d 91, 93 (Pa. Super. Ct. 2005) (holding that instant messages were admissible and properly authenticated through the use of circumstantial evidence).

494. Deutsche Bank Sec., Inc. v. Montana Bd. of Invs., 850 N.E.2d 1140, 1141–42 (N.Y. 2006).

495. *Id.* at 1142.

496. *Id.*

497. *Id.*

498. *Id.*

499. *Id.* (quoting Kreutter v. McFadden Oil Corp., 522 N.E.2d 40, 43 (N.Y. 1988)).

support long-arm jurisdiction over the client when she was sued by her New York lawyer for unjust enrichment and breach of contract arising from her nonpayment of legal fees.[500]

- A law firm with more than 600 lawyers that maintained a practice on a "coast-to-coast" platform and one of its partners who worked in the firm's Columbus, Ohio office were sued in a Delaware chancery court for allegedly aiding and abetting a breach of fiduciary duty by top managers of a publicly-held company incorporated in Delaware and headquartered in Ohio.[501] The law firm and its partner challenged the complaint on the ground that they were not subject to personal jurisdiction in Delaware because the partner had never entered Delaware in connection with the representation and did not file any documents with any court or agency in Delaware in connection with the representation.[502] However, the plaintiff presented evidence that the client's Certificate Amendment was drafted by a paralegal under the partner's supervision and sent to the Corporation Service Company in Delaware for filling.[503] The defendants argued that they could not be sued simply for performing services for a client since they only received fees in exchange for those services.[504] The Vice Chancellor rejected their arguments, emphasizing that the law firm represented on its website that it had a "unique [ten office] coast-to-coast platform," and advertised itself as "being able to handle the full range of any corporation's legal needs, regardless of its location in the United States."[505] The Vice Chancellor observed that:

> For sophisticated counsel to argue that they did not realize that acting as the de facto outside general counsel to a Delaware corporation and regularly providing advice about Delaware law about matters important to that

500. Fischbarg v. Doucet, 880 N.E.2d 22 (N.Y. 2007); *see also* Stone v. Patchett, No. 08 CV 5171(RPP), 2009 WL 1108596, at *4, *10 (S.D.N.Y. Apr. 23, 2009) (finding that New York had jurisdiction over defendant in case involving communications by fax, e-mail, and telephone); Centrifugal Force, Inc. v. Softnet Commc'n, Inc., No. 08 Civ. 5463(CM)(GWG), 2009 WL 1059647, at *4 (S.D.N.Y. Apr. 17, 2009) (finding defendant created a relationship with a New York corporation, and, thus, New York had jurisdiction).

501. Sample v. Morgan, 935 A.2d 1046, 1048, 1052–53 (Del. Ch. 2007).

502. *Id.* at 1054–55.

503. *Id.* at 1054.

504. *Id.* at 1060–61.

505. *Id.* at 1053, 1063.

> corporation and its stockholders might expose it to this court's jurisdiction fails the straight-face test. The moving defendants knew that the propriety of the corporate action taken in reliance upon its advice and through its services would be determined under Delaware corporate law, and likely in a Delaware court.[506]

The Vice Chancellor held that the arranging for the filing of a corporate instrument in Delaware that facilitated transactions under challenge in litigation and the advising on Delaware law to a Delaware corporation that resulted in injury in Delaware were sufficient to constitute the transaction of business and to provide a basis for jurisdiction.[507] New communications technologies and the practices that coalesce around their use tend to raise novel issues under ethical rules. By routinely reviewing such rules counsel can mitigate, if not eliminate, the risk of misremembering the mandates or departing inadvertently from their spirit.

Routinely keeping abreast of new communications technologies is an increasingly important part of the practice of law. Doing so reduces the probability of being surprised by the misuse of such new technologies or failing to provide the requisite degree of supervision for associates, staff, and service providers.

Fulfilling the implicit ethical obligation to keep abreast of new communications technologies involves several tasks, including the basic ones of identifying new technologies that seem to be gaining widespread acceptance and learning of risks that may arise from their use and misuse, particularly by clients, lawyers, and law firms. Sometimes the risks will come from new technologies that are not widespread, not the subject of multiple reports in the media, and yet are important for counsel to be aware of. For example, there has been little reporting of the risks from "side-channel attacks," but they pose a severe risk to enterprises. These attacks exploit vulnerabilities in the reflective surfaces (such as eyeglasses and

---

506. *Id.* at 1065.

507. *Id.* at 1057, 1063. The Vice Chancellor also noted public policy reasons in support of the decision, stating that:

> Delaware has no public policy interest in shielding corporate advisors from responsibility for consciously assisting the managers of Delaware corporations in breaching their fiduciary duties. If well-pled facts can be pled that support the inference that a corporate advisor knowingly assisted corporate directors in breaching their fiduciary duties, Delaware has a public policy interest in ensuring that its courts are available to derivative plaintiffs who wish to hold that advisor accountable to the corporation.

Id. at 1065.

computer screens) throughout offices and capture them on the latest photographic and video recording devices. As explained in an article in the May 2009 issue of *Scientific American*:

> [A]n alarmingly wide range of objects can bounce secrets right off our screens and into an eavesdropper's camera. Spectacles work just fine, as do coffee cups, plastic bottles, metal jewelry —even . . . the eyeballs of the computer user. The mere act of viewing information can give it away.
>
> The reflection of screen images is only one of the many ways in which our computers leak information through so-called side channels, security holes that bypass the normal encryption and operating-system restrictions we rely on to protect sensitive data.
>
> . . . .
>
> "Side-channel" attacks exploit the unprotected area where the computer meets the real world . . . at a stage before the information is encrypted or after it has been translated into human-readable form. Such attacks also leave no anomalous log entries or corrupted files to signal that a theft has occurred, no traces that would allow security researchers to piece together how frequently they happen. The experts are sure of only one thing: whenever information is vulnerable and has significant monetary or intelligence value, it is only a matter of time until someone tries to steal it.[508]

In closing, we believe it is important to identify one other step that counsel may find prudent and valuable in fulfilling ethical obligations related to the emergence and use of new communications technologies. Integral to the ethical duty to keep abreast of technology, but easily overlooked in efforts to fulfill it, is the need to be alert to the use of words that create the appearance of an objective assessment of a new communications technology when, in fact, the words work to coax the reader to trust an assertion, when the reader should be examining, testing, and challenging it. In his 1946 essay, *Politics and the English Language*, George Orwell cautioned against uses of language that can cause readers to concede points that they should be examining; instead, words that "are used to dress up a simple statement and give an air of scientific impartiality to biased judgments" and that are used for

508. W. Wayt Gibbs, *How to Steal Secrets Without a Network*, SCI. AM., May 2009, at 58.

"the defense of the indefensible."[509]

As lawyers, we continuously train ourselves to be vigilant and critical of the use of words in contracts, board resolutions, replies to interrogatories, and other documents where what is written will be taken seriously, where it will be understood to be the expression of what was meant, and where inaccuracy or any effort to mislead may harm others and ultimately may harm the author and the author's legal counsel. In order to keep abreast of new communications technology, it is valuable to train ourselves to be equally critical of the uses of words that developers, vendors, and promoters use to describe such technologies and their capabilities and benefits. When the description of capabilities seems to omit a serious assessment of shortcomings or of ways in which performance may fall short of specifications or representations, or disclaims in one provision promises made in others, it should be seen as a red flag that important information is missing. When the description of benefits purports to address potential weaknesses, deficiencies, or risks, but does so in a manner that, on close examination, proves to have been written to persuade the reader that the risks do not exist or have been dealt with in ways not really disclosed, this too should be seen as a red flag. For example, when a web page document, entitled *10 Reasons to use Azure for Your Cloud Apps*, discusses the important topic of "Security," there should be a discussion of the vulnerabilities before there is an assertion that they have been minimized, mitigated, averted, or rendered nonexistent.[510] Instead, such document offers the following assurance designed to make the reader complacent, less vigilant, more trusting, and ultimately unquestioning of the assurances and the risks it obscures: "Knowing that security is one of the biggest concerns for companies considering a move to the cloud, Microsoft designed Azure with security in mind. . . . Microsoft has designed its compliance framework to meet regulatory requirements."[511]

A contract for the design and development of a computer-based system would provide the customer little protection of its interests if the specifications stated merely that the vendor must "design[] . . . [the system] with security in mind" and that it must

509. GEORGE ORWELL, POLITICS AND THE ENGLISH LANGUAGE (1946), *available at* http://www.mtholyoke.edu/acad/intrel/orwell46.htm.

510. Debra Littlejohn Shinder, *10 Reasons to Use Azure for Your Cloud Apps*, TECHREPUBLIC § 9 (Jan. 6, 2010, 9:41 AM), http://www.techrepublic.com /blog/10things/10-reasons-to-use-azure-for-your-cloud-apps/1282.

511. *Id.*

be "designed . . . to meet regulatory requirements."[512] Competent counsel would challenge such vacuous specifications. It is important for counsel to alert themselves, their law firms, and their firm's clients when a new communications technology contains risks that are being obscured, trivialized, or otherwise de-emphasized by the language the vendors have used not only in marketing literature, but in the service level agreements, white papers, and other documents that a client and its counsel should consider adding to their due diligence list. As in any due diligence exercise, where documents authored by a party to the transaction contain statements or omissions that should be clear red flags, it is prudent to ask questions in order to understand whether the red flag is evidence of a risk, and, if so, whether the risk can be mitigated—and whether the client can accept the risk to the extent mitigated.

Just as counsel often asks a client to explain its business, its manufacturing methods, and its technologies, and will compare those descriptions to the client's published statements to see where they match and where they might diverge, counsel in fulfillment of professional ethical obligations will often benefit from comparing what can be learned of a new communications technology to what the technologies' developers, vendors, and supporters say, write, and publish. As we have noted in this essay, there are many places where the cloud vendors' statements to promote their technology seem to diverge from what the vendors put in their standard service level agreements and seem also to diverge from the risks disclaimed or that one discovers in the reports of problems that the vendors' published statements did not hint at or seem uninterested in pointing out to potential customers.

Because the client's confidential information and interests are at stake, as is counsel's reputation and the ability to fulfill professional ethical obligations, it is worth learning and keeping abreast of the changes in technology and of the changes in the mismatches between the language vendors use to describe and emphasize and the language they use to de-emphasize. That is an important part of keeping abreast of new technologies. Failure to do so can lead counsel to underestimate the promises in a service level agreement to a client's detriment. For example, promises such as those that typically appear in the agreement's specification of "uptime" service level can be complex. When probed, the

512. *Id.*

specifications prove to be difficult for the customer to verify because key facts required for the computation of "uptime" are not accessible to the customer.[513]

Such failure can also cause counsel to be distracted by the drum beat of promotional discourse. As a result, counsel may become so accustomed to reading the praises of a new communications technology and the exhortations to "adopt it or be left in its wake" that counsel may come to believe that the new technology really performs as well its promoters promise it will and that the risks, whatever they might have been, have ceased to exist or never did or must have been exaggerated. Add to that the tendency for experienced lawyers to want to avoid appearing either ill at ease with new technology or not as technologically adept as younger colleagues, and it can be difficult for such counsel to remain vigilant and keenly observant for undisclosed defects and risks in a new, widely popular communications technology. To counteract the dulling of a lawyer's skeptical questioning of new technologies and the loss of a healthy wariness that should accompany the use of new communication devices there are some antidotes, one of which is for counsel to be presented with contemporaneous and sharply contrasting reports of the same technology with one praising it and one revealing an unsuspected

513. For example, Microsoft's Service Level Agreement for its Azure Storage Service Level Agreement, promises an "uptime" of "99.9%," but that is expressed as a "monthly uptime percentage." *Windows Azure Storage SLA-English.doc*, MICROSOFT § 4, http://www.microsoft.com/download/en/details.aspx?id=6656 (last visited Oct. 20, 2011). Such percentage is to be "calculated by subtracting from 100% the average Error Rate for the billing month for the customer's storage transactions . . . ." *Id.* The "Error Rate," in turn, is defined as the "total number of Failed Storage Transactions divided by the Total Storage Transactions" that occur during an hour. *Id.* § 3. To know if the "uptime" has not been achieved, a customer would have to be able to compute a value for the "Error Rate" denominator; and, to do that, the customer has to first know its own "Total Storage Transactions" for a month. *Id.* Few, if any, customers are likely to be keeping, or to be able to keep, an accurate count of such transactions, making the "Error Rate" incomputable. Furthermore, the customer would also need to be able to compute a value for the "Error Rate" numerator; and, to do that, the customer has to have access to the records of incidents of "Failed Storage Transactions." *Id.* The Service Level Agreement defines that as any of certain occasions when a request exceeds the specified "Maximum Processing Time," but it qualifies that by stating that "the amount of time spent processing a request . . . does not include the time it takes to transfer the request to/from the Windows Azure Storage service" and "only includes the time spent processing the request," neither of which a customer will be able to access. *Id.* § 2. Thus, both the numerator and the denominator of the "Error Rate" prove to be incomputable by a customer, making the "uptime" of "99.9%" an undeterminable and thus unenforceable term for a cloud customer.

risk and its damaging consequences.

An example of two such contrasting reports appeared in the morning newspapers on August 31, 2011, on the eve of the submission of this article for publication. The bright side of cloud computing received expression in an op-ed piece published in *The New York Times*, and in reading it one would be tempted to believe that any security risks inherent in the cloud had either been disarmed or never had existed. For the author cheerfully writes:

> The State Department, for instance, has raised concerns about whether the cloud approach introduces security risks, since data is stored off site by private contractors. But cloud computing is often far more secure than traditional computing, because companies like Google and Amazon can attract and retain cyber-security personnel of a higher quality than many governmental agencies. And government employees are so accustomed to using cloud services like Dropbox and Gmail in their personal lives that, even if their agencies don't formally permit cloud computing, they use it for work purposes anyway, creating a "shadow I.T." that leads to a more vulnerable organization than would a properly overseen cloud computing system.
>
> The United States cannot afford to be left behind in the cloud computing revolution.[514]

The dark side of cloud computing came to light in the *Financial Times*, which reported an incident that the author apparently found both alarming and discomforting:

> The worst breach to date in the dominant system for securing websites has raised fears that thousands of Iranians have had their Google e-mail read by government authorities. A Dutch company called DigiNotar . . . [which sells] certificates to authenticate sensitive sites, said on Tuesday that it discovered that it had been hacked on July 19, allowing unknown attackers to fake certificates and impersonate websites beginning with the letters "https" and displaying a padlock to visitors. Known formally as Secure Sockets Layer, the system is used worldwide by banks and communications providers, including Google mail or Gmail . . . . [Some makers of web browsers] decided to ban all DigiNotar certificates . . . . [DigiNotar] said it did not expect material harm to

514. Vivek Kundra, Op-Ed., *Tight Budget? Look to the 'Cloud,'* N.Y. TIMES, Aug. 31, 2011, at A27.

its business, but shares in the company fell 6 per cent.[515]

Whether counsel believes in the bright or the dark side of cloud computing, seeing two such reports juxtaposed should sharpen and reinvigorate the questions that counsel might find prudent to ask of the technology and its vendors before venturing to store client confidential information in the cloud with the attendant risks to reputation, client trust, and professional ethical obligations. Among those questions, counsel will probably find several that lawyers, law firms, and state bar ethics committees asked of earlier communications technologies that appeared attractive and nonetheless created brave new worlds of digital capabilities and digital risks.

Boards of directors also may need to reckon with cybersecurity threats and reported attacks. As they do so, priorities and the weights assigned to cybersecurity risks will change. Risks thought to be remote may be recalibrated as imminent threats. Having measured technologies for their probable benefits, boards may require that technologies be measured also for their vulnerabilities and the potential for damage to the enterprise. As the CEO of Hyundai Capital suggested, boards may ask if the enterprise can afford the total of adoption and management of the new cybersecurity technology.

New technologies in the last ten years have increased a lay person's ability to report—to publish and broadcast written utterance as well as photographs and videos that express each individual's account of events that they have witnessed or to which they are reacting.[516] And yet, ironically, the rush to adopt and adapt these technologies to benefit a corporate enterprise, eager to extract value from the use of social media externally and internally to the enterprise, has not led to greater care in the use of words to describe such technologies, but instead has led to a prolific use of vague terms that obscure from counsel and their clients the precise

515. Joseph Mann, *E-mail Breach in Iran Raises Surveillance Fears*, FIN. TIMES Aug. 30, 2011, http://www.ft.com/intl/cms/s/0/6bb480b4-d327-11e0-9ba8-00144feab49a.html#axzz1Y3gVT1p7.

516. As David Friend recently observed, "[o]n Sept. 11, 2001, there was no such thing as a YouTube video. Or a Facebook page. Or a Twitter feed. Cell phone cameras did not exist." David Friend, *Seeing 9/11 Through a Digital Prism*, WALL ST. J., Aug. 29, 2011, http://online.wsj.com/article/SB10001424053111903461304576524781716173962.html. However, since then, as he also notes, "the documentation of conflict—in the form of still photographs and moving pictures, often by civilians carrying camera—equipped mobile phones, whose footage can be viewed almost instantaneously across the globe—actually takes precedent [sic] in the public mind over context and analysis." *Id.*

nature and risks of such technologies.

It has become far easier today than a decade ago to release incautiously considered expressions that once posted remain sempiternally attached to and accessible on the Web, and thus on view for all the world to see. Before a letter was posted, it was often reread. There was time to reconsider its phrasing and content. And many times reconsideration of a handwritten or typewritten letter led to a decision to rewrite it or not to send it. Before an e-mail was transmitted, there tended to be much less time to reconsider the text, because e-mails were (and continue to be) often quick responses to other e-mails sent with the expectation of, if not the insistence on, a quick reply. As a result, lawyers often learned that pressing the SEND key prematurely could lead to unfortunate results: text that sorely needed revision, or a message that went to REPLY ALL when it was written for only one of the addressees, sometimes raising the risk of waiving the privilege concerning certain communications. The move towards brevity that has accompanied the adoption of communicating by texting, social network postings, and tweets should alert lawyers that learning each new communications technology brings with it a professional responsibility for using the technology in a manner consistent with counsel's ethical obligations, however inconvenient and contrary to our culture's social customs such caution may appear to be when observed by digital natives, laymen, and corporate executives.

Two of the most unsuspected risks from each new communications technology appear to be the increasingly incautious use of the media, which counsel must avoid while nonetheless learning and using such media, and the increasingly obscure use of words to describe the workings, benefits, and risks of such media, which counsel must diligently discern and highlight for clients. The measure of success or failure in averting such risks is not, and probably should not be, found in the precepts of a state bar association's code of professional responsibility. The practice of law is difficult to do well, and will not be improved by adding ethical liability as an incentive for using good judgment and common sense, especially when the rules in their current form supply adequate reminders of the need to use good judgment and common sense when communicating with old, as well as with new, technologies. Having new equipment to communicate sadly may make it harder to capture what we really need to say, and to avoid saying it in client-sensitive communications. And our efforts to

express our thoughts are already dependent on words and expressions that tend to deteriorate in ways that often escape our notice, as the poet T.S. Eliot recognized when he wrote:

> And so each venture
> Is a new beginning, a raid on the inarticulate
> With shabby equipment always deteriorating
> In the general mess of imprecision of feeling,
> Undisciplined squads of emotion . . . .
> For us, there is only the trying. The rest is not our business.[517]

517. T.S. ELIOT, *East Coker*, *in* THE COMPLETE POEMS AND PLAYS 1909–1950, at 123, 128 (1962).