ISSN: 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Op. J. Vol. I, n. I/2014

"Something's got to give" - Cloud Computing, as Applied to Lawyers – Comparative Approach US and EU and Practical Proposals to Overcome Differences

By

Nathan M. Crystal
Francesca Giannoni-Crystal

SOMETHING'S GOT TO GIVE
- CLOUD COMPUTING, AS APPLIED TO LAWYERS – COMPARATIVE APPROACH US AND EU AND PRACTICAL PROPOSALS TO OVERCOME DIFFERENCES

by

Nathan M. Crystal [*]
Francesca Giannoni-Crystal [**]

Abstract:

What is cloud computing? What are the advantages, disadvantages, and risks, both legal and ethical in using cloud computing services? What have US ethics advisory committees said about the ethical propriety of using cloud computing services? What are the elements of an ethical checklist for review of cloud computing services? What is the relationship between data privacy and cloud computing in the European Union? What differences and similarities can be found in the American and European approaches to cloud computing? Is it possible for an international law firm, with offices in both the EU and the US, to adopt a unified approach to review of cloud computing services that combines the American and European views? This article addresses these questions and others.

The article is divided into four parts. Part I describes what is meant by cloud computing and analyzes the benefits and risks, both ethical and legal from use of cloud services. Part II discusses the approach of US jurisdictions to cloud computing and offers a checklist that summarizes the requirements that result from these opinions. Part III compares the US and European approaches to cloud computing. Part IV offers a practical approach to reconciling US and European approaches.

Keywords: cloud computing, data privacy, international data privacy, encryption, Directive 95/46, Data Protection Directive, Article 29 Working Party, Duty of Confidentiality, IPAA, FACTA, COPPA, Data Controller, Data Processor, International Law Firm, Professional Secrecy, Attorney-Client Privilege, Privacy Law, European Privacy, Platform as Service,PaaS, Infrastructure as Service,IaaS, Software as Service, SaaS, CCBE Guidelines on Cloud, Opinion 8/2010, Opinion 1/2010, Opinion 05/2012

---

[*] Nathan M. Crystal, Distinguished Research Scholar, Charleston School of Law, Attorney at Law (admitted Georgia, New York and South Carolina), Partner, Crystal & Giannoni-Crystal, LLC www.cgcfirm.com.
[**] Francesca Giannoni-Crystal, Attorney at Law (admitted District of Columbia, New York, and Italy), Partner, Crystal & Giannoni-Crystal, LLC, www.cgcfirm.com.

TABLE OF CONTENTS

INTRODUCTION

As one of the co-authors wrote in 2011 "[c]loud computing offers a number of possible advantages for lawyers and their firms, including expanded data storage, immediate application updates, greater accessibility, and reduced cost."[1] However, "[b]ecause the cloud involves moving storage of firm data outside the firm to servers of various providers, it obviously poses issues of confidentiality."[2]

Since Professor Crystal wrote in 2011, the cloud has become even more pervasive in the practice of law, to the point where it maybe fair to conclude that cloud computing is "inevitable", both in the sense that it is already here, even for those who do not think they are using it[3] and in the sense that more and more law firms are shifting towards the cloud to maintain their competitiveness and to comply with their ethical duties to clients.

It has been effectively said that cloud computing is about dependence and confidence: Because the exact location of data is difficult to determine for users, they depend on providers for the safety of their data and must have confidence in the security measures adopted by providers.[4]

This article examines the ethical obligations of lawyers in using the cloud, not only under US law but under European privacy law, as embodied in European Directive 46/95. Our particular focus is on an American-based international law firm with offices in Europe. However, reversing this perspective, our analysis could be useful also for a European-based international firm with offices in the U.S. One conclusion from this examination is that global firms may be subject to conflicting standards. The article proposes a due diligence checklist to assist firms in complying with both American and European law.

The article is divided into four parts. Part I describes what is meant by cloud computing and analyzes the benefits and risks, both ethical and legal from use of cloud services. Part II discusses the approach of US jurisdictions to cloud computing and offers a checklist that summarizes the requirements that result from these opinions. Part III compares the US and European approaches to cloud computing. Part IV offers a practical approach to reconciling US and European approaches.

---

[1] Nathan Crystal, *Ethics Watch: Technology and Confidentiality, Part Two*, South Carolina Lawyer 8, Nov. 2011, available at http://www.nathancrystal.com/pdf/FileItem-222487-techconf2.pdf

[2] *Id.*

[3] For example a lawyer who is conducting a research on WestLaw is actually using a service in the cloud.

[4] Professor Olivier Deshayes (Université de Cergy-Pointoise) expressed this thought at the conference Getting around the cloud(s) – "Technical and legal issues on Cloud services", November 30, 2013, organized by the Scuola Superiore Sant'Anna, Pisa.

PART I --CLOUD COMPUTING – RISKS AND BENEFITS FOR LAWYERS AND ETHICAL IMPLICATIONS

A. WHAT IS "CLOUD COMPUTING"?

Cloud computing does not find a precise definition.[5] It might be the case because, as one author wrote

> "cloud" is a collective term for a large number of developments and possibilities. It is not an invention, but more of a "practical innovation", combining several earlier inventions into something new and compelling. [It comprises] … several existing concepts and technologies … [and] merges several already available technologies: high bandwidth networks, virtualization, Web 2.0 interactivity, time sharing, and browser interfaces."[6]

Opinion 05/2012 on Cloud Computing, issued by the Article 29 Data Protection Working Party ("Opinion 05/2012"), states: "Cloud Computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space."[7]

The National Institute of Standards and Technology (NIST)[8], in a "guideline … prepared for use by Federal agencies"[9] wrote that "[c]loud computing is an evolving paradigm." NIST defined cloud computing as

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.[10]

---

[5] We thank Avv. Federica Romanelli, Foreign Legal Consultant in New York, for her research on the definition and types of clouds. We do not intend what follows to be a comprehensive definition but only a working definition for the purposes of this paper.

[6] Gregor Petri, *Primer, Shedding Light On Cloud Computing* 4 (2010), available at http://www.ca.com/us/~/media/files/whitepapers/mpe_cloud_primer_0110_226890.aspx

[7] Opinion 05/2012 on Cloud Computing at 4, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[8] "Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories." ABOUT NIST, available at http://www.nist.gov/public_affairs/nandyou.cfm.

[9] The National Institution of Standards and Technology, US Department of Commerce, Computer Security Division, Information Technology Laboratory, Peter Mell Timothy Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145, Recommendations of the National Institute of Standards and Technology ("The NIST Definition of Cloud Computing") at 1, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[10] *Id.* at 2. Before giving a definition, NIST cautioned that

> The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation. *Id.* at 1

According to NIST the five essential characteristics of the cloud are: (i) On-demand self-service; (ii) Broad network access; (iii) Resource pooling; (iv) Rapid elasticity; (v) Measured service.[11]The three service models are: (1) Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS).[12] The four deployment models are: (1) Private cloud; (2) Community cloud; (3) Public cloud, and (4) Hybrid cloud.[13]

A private cloud

> describes an IT infrastructure that is dedicated to an individual organization; it is located at the organization's premises or else its management is outsourced to a third party (usually via server hosting) that is under the controller's strict authority.[14]

A private cloud is custom-designed for specific customers (often Fortune 500 companies, especially insurance companies or financial institutions)which have *complete* control over data, having the right to decide accessibility, location, and transfer of data.

NIST defines a public cloud as an

> infrastructure owned by a provider specializing in the supply of services that makes available – and therefore shares – his systems to/among users, businesses and/or public administrative bodies. The services can be accessed via the Internet, which entails transferring data processing operations and/or the data to the service provider's systems. Therefore the service provider takes on a key role as regards to the effective protection of the data committed to his systems.[15]

Social network sites are a good example of public clouds. The majority of cloud services offered to lawyers are public clouds. In a public cloud, customers lose a great deal of their control over the data that are transferred. However, public clouds enable smaller organizations, which might not have the time or the resources to manage an extensive data center, to obtain the benefits of cloud services.

A community cloud is "provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns"[16] while a "hybrid" is a cloud "where services provided by private infrastructures co-exist with services purchased from public clouds."[17]

As mentioned above, three main "service models" exist:[18] (i) Infrastructure as a Service (IaaS), (ii) Software as a Service (SaaS), (iii) Platform as a Service (PaaS).

In short, (i) "IaaS" is the most basic cloud service model, providing access to cloud-based, or "virtual" hardware (e.g., additional storage in virtual remote servers or processing capacity) which

---

[11] *Id.* at 2.
[12] *Id.* at 2-3.
[13] *Id.* at 3.
[14] See Annex to Opinion 05/2012, which relies on the definition given by the NIST.
[15] See Annex to Opinion 05/2012.
[16] The NIST Definition of Cloud Computing, at note 9 above . "It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises." *Id.* at 3.
[17] See Annex to Opinion 05/2012.
[18] *Id.*

customers use instead of installing hardware in their office (e.g., Amazon EC2).[19] The service provider owns the equipment and is responsible for housing, running and maintaining it;[20] (ii) SaaS provides cloud-based software to consumers and it is the type of cloud that most lawyers use (e.g., Google Apps); (iii) PaaS is an evolution of SaaS and allows users to rent hardware, operating systems, hardware, storage, and network capacity over the Internet (e.g., Salesforce.com).[21]PaaS is generally a composite "cloud" where several software and network providers are involved.

Because it is the most common type of cloud among lawyers, we will spend some more time on SaaS. SaaS makes available to users several application services, such as web-based office applications like spreadsheets, text processing tools, computerized registries and agendas, shared calendars, and similar applications. These services are meant to "replace conventional applications to be installed by users on their local systems"[22] and facilitate law firm practices, particularly in the areas of case management and time/billing platforms, but they also allow for web-based e-mails systems. There are several types of SaaS cloud for lawyers:[23] (1) time, billing and invoicing cloud services (e.g., Bill4Time), which allow lawyers to provides time and expense tracking billing services; (2) Electronic signatures service (e.g., DocuSign), which can provide encryption services and exchange of signature; (3) case and client management services (e.g., Clio) which generally include group calendaring, docket, and activity management, client management and marketing, project and matter management, time and billing, document management, account management, mobile access; and (4) online document management allowing lawyers to access files and documents from any computer connected to the Internet, as well as share files with clients, team members and others (e.g., Dropbox) or allowing virtual data room service (e.g., Firmex); (5) virtual law office arrangement allowing the online delivery of legal services (e.g., DirectLaw); (6) project management services (e.g., Basecamp); (7) online document storage and backup (e.g., Mozy); (8) remote access services to your computer (e.g., GoToMyPC); (9) Encrypted email and document services (e.g.,RPost).

---

[19] "Instead of purchasing, maintaining and utilizing personal hardware, users rent virtual data centers hourly/monthly/yearly and increase or decrease the amount of equipment as necessary. Iaas solutions include storage, hardware, servers and networking components." *Id.*

[20] *See, e.g.*, Nicole L. Black, *Cloud Computing for Lawyers*, available at http://www.llrx.com/features/cloudcomputingforlawyers.htm

[21] These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties." *Id.*

> A provider offers solutions for the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties. *Id.*

[22] See Annex to Opinion 05/2012.

[23] Limbro and Mighell, *Popular Cloud Computing Services for Lawyers: Practice Management Online,* Volume 37 Number 5, available at http://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html.

B. BENEFITS AND RISKS – IMPLICATIONS OF CLOUD ON ETHICAL OBLIGATIONS

1. Benefits of the use of the cloud for lawyers

Cloud computing offers many benefits to law firms, which can be summarized in four categories (three practical and one ethical): (a) efficiency, (b) convenience and flexibility, (c) reduced costs, and (d) compliance with the ethical duty of competency.

Thanks to cloud, lawyers can *efficiently* set up and operate their firms much faster than previously because cloud services can be activated quickly, no physical space is required, back up is usually automatic, and updates of applications are instantaneous. Law firms obtain increased efficiency also by the outsourcing tasks that previously were performed internally, such as electronic discovery, timekeeping, case management, and billing. As for *convenience and flexibility*, because the cloud is "located" in the Internet, lawyers can use and access the cloud also when they are outside their offices and from several devices. These features allow lawyers to work easily from almost any place with an internet connection. Cloud computing also allows lawyers based in different offices to cooperate on projects much easier than before. In addition, the cloud is generally very flexible and operating system "neutral": regardless of whether lawyers use Windows or Mac (or whether they uses a PC, a tablet, or a smart phone), they can generally use the same cloud application. Use of cloud services enable lawyers to *reduce costs* because they pay a monthly (usually modest) feefor the cloud and save on software licenses and updates, data centers, servers, and IT personnel. In addition, because they store their data in the cloud, lawyers do not need to pay for physical storage.

How the use of the cloud allows lawyers to *comply with their ethical duty of competency,* requires more explanation. In the U.S., the duty of competence (or competency as it is also named) is central to the profession.[24]

> Under the Model Rules of Professional Conduct, lawyers have an ethical duty to provide competent representation. The duty of competency is multidimensional, including knowledge of the law, skill, and preparation. … Lawyers who fail to adhere to their duty to provide competent representation may be subject to professional discipline.[25]

[24] "The most fundamental ethical obligation for a lawyer is the duty of competency, reflected in ABA Model Rule 1.1." Nathan M. Crystal & Francesca Giannoni-Crystal, *Do the Right Thing (for your duty of competency): Some Ethical and Practical Thoughts on "Notarization" in International Transactions*, Global Jurist. Volume 12, Issue 2, Pages –, ISSN (Online) 1934-2640, DOI: 10.1515/1934-2640.1412, December 2012, available at http://www.degruyter.com/view/j/gj.2012.12.issue-2/1934-2640.1412/1934-2640.1412.xml. Model Rule 1.1. (Client-Lawyer Relationship) requires lawyers to provide "competent representation to a client", which "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Full text of the Rule available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

[25] NATHAN CRYSTAL PROFESSIONAL RESPONSIBILITY – PROBLEMS OF PRACTICE AND THE PROFESSION 64-65 (Aspen Law & Business 5th ed. 2012).

While disciplinary proceedings against lawyers for violation of the duty of competence are rare, malpractice actions are much more frequent.[26]To be sure, as it is true for any other ethical duty, the violation of the duty of competency is not *per se* malpractice, however it is an *index* of malpractice.

> To establish malpractice liability for negligence, it is necessary to show that the attorney's conduct fell below generally accepted standards of conduct in the profession. This standard typically requires expert testimony. Most courts will allow experts to consider rules of ethics in deciding whether the attorney's conduct did not meet generally accepted standards of the profession. In addition, to establish malpractice liability a plaintiff must also prove that the attorney's breach of duty caused damages to the plaintiff.[27]

The violation of the duty of competence, in the form of "failure to know" has been reported by theAmerican Bar Association (ABA) as the most common ground for malpractice.[28]

Based on Model Rule 1.1. (and relevant state versions), the duty of competence already was intended to include the duty to be aware of modern technologies (e.g., electronic discovery). However, on August 6, 2012 to add more clarity the ABA, among other changes, added a new Comment [8] to Rule 1.1. ("Maintaining Competence"), which clarified that the lawyer's duty of competence includes an obligation to become and remain "tech-savvy":[29]

> 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 relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[30]

Up to date, among the fifty jurisdictions, only Pennsylvania has transposed the Comment.[31] However, because the Comment does not add any substantial content to the duty of competence as it was intended, the lack of adoption is not very significant.[32]

---

[26] *Id.* at 70-76.
[27] *Id.* at 75.
[28] Dan Pinnington, *The Most Common Legal Malpractice Claims by Type of Alleged Error*, available at http://www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_webonly_webonly07101.html/
[29] It has been said that the amendments to Rule 1.1 are a "wake-up call for technologically challenged lawyers". Matt Nelson, *New Changes to Model Rules a Wake-up Call for Technologically Challenged Lawyers*, available at http://www.insidecounsel.com/2013/03/28/new-changes-to-model-rules-a-wake-up-call-for-tech
[30] Full text of the Comments to Rule 1.1 available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html
[31] On Oct. 22, 2013, the Pennsylvania Supreme Court adopted changes to the Rules of Professional Conduct that, for the part that is interesting to us, update the guidelines for maintaining competence. The changes bring Pennsylvania Rules of Professional Conduct in line with the ABA Model Rules, in particular Comment [8] to Rule 1.1 See http://www.law.com/jsp/pa/PubArticlePA.jsp?id=1202625198396&Justices_Add_Tech_Savviness_to_Professional_Responsibility
[32] *Report Accompanying the Resolution of Amendment* 6, available at http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf:

> Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase "including the benefits and risks associated with relevant technology," would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather,

In conclusion, under American rules of professional conduct, knowledge of technology is not a choice for lawyers: it is a duty. "Lawyers owe clients an ethical duty to obtain technical proficiency sufficient to ensure competent representation of clients."[33]

In Europe the duty of competence is also central for lawyers. The Code of Conduct for European Lawyers ("European Code of Conduct") issued by the Council of Bars and Law Societies of Europe ("CCBE") includes a duty of competency.[34]The codes of conduct of several European countries also typically include such an obligation. For example, Article 12 of the Italian Code of Conduct[35] requires Italian lawyers to represent their clients competently,[36] while Article 13 requires lawyers to keep up to date professionally.[37]

We are not aware of any European formal provision or comment like Comment [8] to Model Rule 1.1. However, in some European countries, the duty of competence includes in some way the duty to become familiar with technology. In France, for example, there is a general obligation for lawyers to maintain technical legal knowledge with at least 20 hours of technical legal training per year. There is no specific provision requiring a lawyer to be trained on benefits and risks associated with technology. This knowledge, however, is considered part of the general obligations of a lawyer and expected by the bar. Exactly as locking the door of your office is normal and expected, so is the knowledge of the technologies that you use for your profession (including benefits and risks).[38] In Italy, it is basically the same.[39]In Germany, lawyers' technology training has not been the object of specific attention by the bar. The lack of a duty to be prepared on technology is to be seen in the context of German bar regulations on the general

---

> the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.

[33] Matt Nelson, *New changes to Model Rules a Wake-up Call for Technologically Challenged Lawyers*, above at note 29.

[34] Article 3.1.3 of European Code of Conduct:

> A lawyer shall not handle a matter which the lawyer knows or ought to know he or she is not competent to handle, without cooperating with a lawyer who is competent to handle it.

[35] Available in English at http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/Italy_EN_ethical__co1_1236161856.pdf. The translation is not updated with recent changes in the Italian Ethics Code but the text of Article 12 and 13 -- which we refer to hereunder -- are still the same. An updated text of the Italian Ethics Code is available at http://www.consiglionazionaleforense.it/site/home/area-cittadino/codice-deontologico-forense.html (Italian).

[36] Article 12 *(Duty to represent the client competently)*: "A lawyer shall not accept employment if he knows that he is not in a position to carry out the representation competently."

[37] Article 13 *(Duty to be professionally up to date).*

> It is a lawyer's duty to keep his professional preparation up to date, maintaining and improving his knowledge with particular regard to those areas in which he usually practices.
>
> I. The lawyer realises his continuing training by individual studies and by participating in cultural initiatives in the legal field and in the practice of law.

[38] Thanks to Frédérique David - TLD Legal- Avocats à la Cour - for her insights on French ethical obligations on this point.

[39] *See, e.g.,* Luca Giacopuzzi, *Aggiornamento Professionale e Nuove Tecnologie*, available at http://www.ilcaso.it/privacy/verona-atti/Avv_Giacopuzzi_relaz.pdf

duty of continued legal education, which are rather soft and unspecific, and therefore there does not exist a strong basis for professional obligations in relation to technology.[40]

The use of cloud computing can help lawyers to comply with their duty of being tech-savvy. At a minimum (in the U.S. for sure and very probably in Europe), lawyers who would simply ignore the technological advantages of technology (who, for example, would not use reasonable technological tools to protect the information of their clients) would not comply with their duty of competence. To be clear, we are not saying that a lawyer "must" necessarily use cloud computing to be competent. We are only suggesting that cloud computing may allow a lawyer to comply more easily with the duty to be updated on the use of current versions of software, back ups, and other features and revisions because they are automatic with the cloud.

If the use of the cloud can help lawyers to comply with their duty of competency, it can also create problems and risks from other ethical perspectives.

2. Ethical risks of the use of the cloud

While recognizing the advantages of the cloud, several authorities have warned lawyers that the cloud triggers several risks. For example, the CCBE stated:

> [A]longside many significant benefits, cloud computing also brings its own set of risks and challenges for lawyers, most significantly in relation, first to questions of data protection, second, to professional obligations of confidentiality and, third, to other professional and regulatory obligations incumbent on the lawyer. Though the first and second of these areas are closely related, they are not necessarily identical. The lawyer will also require to be sensitive to purely commercial risks to which he may be exposed, for example by a temporary unavailability of his cloud service causing disruption to his business.[41]

The duty of competence (ABA Model Rule 1.1.), which we have mentioned above as an advantage of the cloud, can also generate problems under the competency principle if lawyers do not become acquainted with the technology they adopt. In addition, cloud services pose risks under several ethics perspectives. The following are particularly important: (i) confidentiality, (ii) duty to safeguard client property, (iii) duty of supervision of nonlawyers, and (iv) duty to communicate with client.

(i)Confidentiality

Nathan Crystal wrote some years ago on the special concerns that technology poses to confidentiality. He made reference to South Carolina Rules of Professional Conduct 1.6 because the article

[40] We thank Hans-Michael Giesen, of Giesen Heidbrink (Partnerschaft von Rechtsanwälten), for his insights on German ethical obligations on this point.

[41] Conseil des Barreaux Européens – Council of Bars and Law Societies of Europe, *CCBE Guidelines on the Use of Cloud Computing Services by Lawyers* 5, available at http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf ("*CCBE Guidelines on Cloud*").

was directed to South Carolina lawyers but the thoughts have general applicability across the country because the confidentiality obligations in the several jurisdictions are basically the same.

> If you ask lawyers to list their most important ethical obligations, confidentiality will certainly be included by almost all of them. Complying with this fundamental ethical duty, however, has become increasingly difficult and risky with the widespread use of modern technology in the practice of law.
>
> The basic obligation of lawyers with regard to confidential client information is clear: lawyers must take reasonable steps to protect the confidentiality of such information. South Carolina Rule of Professional Conduct (SCRPC) 1.6, comment 18 [which is Comment [19] to Model Rule 1.6] states: "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." However, it is often difficult to determine what is reasonable and to implement reasonable precautions when using modern technology.[42]

Since Professor Crystal wrote that paper, the American Bar Association has approved a change in Model Rule 1.6. This change, which occurred in August 2012, consists of the addition of letter (c) to Rule 1.6:

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

The ABA also added language to what is today Comment [18]:

> [18] … The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. ….[43]

Even after these changes, it is not easy determine "what is reasonable and to implement reasonable precautions when using modern technology"[44] because the factors that lawyers should consider in their reasonableness analysis are difficult to "weigh": how sensitive is information, how likely is the information to be disclosed without additional safeguards, how difficult it is to employ safeguards, etcetera.[45] We are

---

[42] Nathan Crystal, *Technology and Confidentiality, Part I*, South Carolina Lawyer 12 (Sept. 2011), available at http://www.nathancrystal.com/pdf/FileItem-125212-Tech_Confidentiality_Sept2011.pdf

[43] Full text available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html

[44] Nathan Crystal, *Technology and Confidentiality (Part I),* above at note 42.

[45] See Comment [18] above at note 43.

talking about a facts-and-circumstances analysis, which – as always – triggers some difficult evaluations. However, if lawyers use "reasonable care" in selecting the cloud providers, violation of confidentiality should not be a major concern, as many ethics opinion around the U.S. have specified.[46]

> Cloud computing offers a number of possible advantages for lawyers and their firms, including expanded data storage, immediate application updates, greater accessibility, and reduced cost. Because the cloud involves moving storage of firm data outside the firm to servers of various providers, it obviously poses issues of confidentiality. A few opinions have examined the ethical propriety of lawyers using cloud computing. In broad terms these opinions have concluded that lawyers may ethically use cloud computing provided they take reasonable precautions to protect client confidentiality.[47]

If lawyers use the appropriate level of diligence in the choice of the cloud, cloud computing poses a lower level of danger than, for example, the use of public networks,[48]to the duty of confidentiality, the problem of loss of devices,[49] or the disposal of devices.[50] The issue is connected, of course, with the level of safety of cloud computing, discussed later in this paper. To be compliant with the duty of confidentiality in the use of the cloud, lawyers should be mindful that "reasonable care" does not mean that they are guarantors of the confidentiality of their clients' information, but they should do their homework to prove their diligence. Later sections of this paper develop the meaning of reasonable care and give specific guidance.

(ii)Duty to safeguard client property

Model Rule 1.15 (Safekeeping Property) imposes on lawyers the duty to safeguard client property for a period of five years:

> A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.[51]

The relevant part of the Rule is "Other property shall be identified as such and appropriately safeguarded(other property being clients' information). Relevant is also Rule 1.16 requiring lawyers to promptly deliver all property "to which the client is entitled", at the end of the representation. Complying with these obligations might be difficult with certain cloud services (especially when lawyers use a public

---

[46] See Part II of this paper.
[47] Nathan Crystal, *Technology and Confidentiality*, *Part II,* above at note 1. We analyze the several ethics opinion in Part II of this paper.
[48] See Nathan Crystal, *Technology and Confidentiality, Part I* (above at note 42) paragraph 1 "Public Use of Technology."
[49] *Id.,* paragraph 3 "Loss of Pen Drives, Smart Phones, Laptops, or Other Devices."
[50] *Id.*, paragraph 4 "Disposal of Devices".
[51]Full text available at
http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property.html

cloud, a situation in which as said they lose a substantial control over their data)[52] but this does not excuse noncompliance:

> Any use of cloud computing must comply with the obligations, under RPC 1.15, to safeguard client property. Thus, lawyers must take "reasonable precautions to ensure that electronic data stored in the cloud is secure and available while representing client."In addition, the "data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer preserve the file."Agreements with cloud providers must state that the customer – not the provider – owns the data. Otherwise, the lawyer may run afoul of Rule 1.15, which requires that the client's property be identified as property of the client.[53]

(iii) Duty of Supervision of Non-lawyers

Lawyers have an obligation to properly supervise any person (for example, contract lawyers or investigators) that lawyers use in the performance of their legal activities. The relevant rule in the U.S. is Model Rule 5.3 (Responsibilities Regarding Non lawyer Assistant)[54] and its state equivalent. Professor Crystal wrote on this regard:

> The Model Rules set forth three principles that apply to supervision of . . . nonlawyers. First, partners in a firm (or those with "comparable managerial authority") have a duty to make reasonable efforts to ensure that the firm has in place "measures giving reasonable assurance" that the conduct of . . . nonlawyers employed or retained by the firm conforms to the rules of professional conduct. See Model Rule. . . 5.3(a). Second, a lawyer having direct supervisory responsibility over . . . a nonlawyer has a duty to use reasonable efforts to ensure that the conduct of the . . . nonlawyer conforms to the rules of professional conduct. Model Rule . . . 5.3(b). Finally, a lawyer is subject to discipline for the conduct of . . . a nonlawyer if the lawyer (1) orders . . . nonlawyer to engage in conduct that violates the rules of professional conduct or with knowledge ratifies such conduct, or (2) is a partner, a lawyer with comparable managerial authority, or a supervising lawyer who knows of misconduct by the . . . nonlawyer and fails to take corrective action when the consequences of misconduct could be avoided or mitigated. Model Rule . . . 5.3(c).[55]

Comment [3] to Rule 5.3 addresses the specific case of "Non-lawyers outside the firm" and provides:

> [3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside

---

[52] See above Part I(A).

[53] Committee on Small Law Firm, New York City Bar, *The Cloud and the Small Law Firm: Business, Ethics, and Privilege Considerations* (2013) 21, available at http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf ("*New York City Bar's Report on Cloud*") (quoting NH Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), Pennsylvania Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011), and Oregon State Bar, Formal Op. 2011-188 (2011)).

[54] Full text of Model Rule 5.3 is available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html

[55] NATHAN M. CRYSTAL, PROFESSIONAL RESPONSIBILITY – PROBLEMS OF PRACTICE AND THE PROFESSION, above at note 25, at 564.

> the firm, a lawyer must make *reasonable efforts* to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations.(emphasis added).

This is exactly the situation with cloud providers. Lawyers must make reasonable efforts to ensure that the cloud provider is compliant with the rules of professional conduct. See the several ethics opinions around the country that have clearly opined on the propriety of using the cloud.[56] So, for example, New Hampshire,[57] North Carolina,[58] and Pennsylvania[59] clearly state that lawyers must use reasonable efforts to ensure that the cloud providers comply with the rules of professional conduct and Vermont mentioned Rule 5.3 as one of the relevant rules that impinges on the propriety of the use of cloud computing by lawyers.[60]

In 2004 the American Bar Association published guidelines for lawyers' ethical use of paralegals ("Guideline on Paralegals").[61] The Guideline spells out some important principles based on Rule 5.3 from which lawyers can receive inspiration in their dealing with cloud providers. For example:

> GUIDELINE 1: A LAWYER IS RESPONSIBLE FOR ALL OF THEPROFESSIONAL ACTIONS OF A PARALEGAL PERFORMING SERVICES AT THE LAWYER'S DIRECTION AND SHOULD TAKE REASONABLE MEASURES TO ENSURE THAT THE PARALEGAL'S CONDUCT IS CONSISTENT WITH THE LAWYER'S OBLIGATIONS UNDER THE RULES OF PROFESSIONAL CONDUCT OF THE JURISDICTION IN WHICH THE LAWYER PRACTICES.[62]

This guideline can be applied by analogy to any nonlawyer hired by a lawyer to assist in providing legal services, including cloud computing providers. Lawyers should take reasonable steps to make sure

---

[56] For more details about the several ethics opinion, see Part II of this paper.

[57] New Hampshire Ethics Committee Advisory Opinion #2012-13/4, available at http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp:

> This means that a provider of cloud computing services is, in effect, a nonlawyer retained by a lawyer. As a result, the lawyer must make reasonable efforts to ensure that the provider understands and is capable of complying with its obligation to act in a manner compatible with the lawyer's own professional responsibilities. N.H. Rule 5.3 (a). … When engaging a cloud computing provider or an intermediary who engages such a provider, the responsibility rests with the lawyer to ensure that the work is performed in a manner consistent with the lawyer's professional duties. Rule 5.3 (a).

[58] North Carolina, 2011 Formal Ethics Opinion 6, available at http://www.ncbar.com/ethics/printopinion.asp?id=855

> Although a lawyer may use nonlawyers outside of the firm to assist in rendering legal services to clients, Rule 5.3(a) requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer.

[59] Pennsylvania Formal Opinion 2011-200, available at available at http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computig.pdf

> At its essence, "cloud computing" can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations.

[60] VT Bar Ass'n Ethics Comm., Advisory Ethics Op. 2010-6 (2010), available at https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx

[61] *Model Guidelines for the Utilization of Paralegal Services* (2004), available at http://www.americanbar.org/content/dam/aba/migrated/legalservices/paralegals/downloads/modelguidelines.authcheckdam.pdf

[62] *Id.* at 2.

that providers comply with the rules that apply to lawyers. Good practice requires lawyers to carefully review the agreement with the cloud provider to verify that it does not contain anything that would be unethical for a lawyer. In the Pennsylvania ethics opinion on cloud computing that we cited above, the committee specified that

> [A] lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion. It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client's interests.[63]

Lawyers using the cloud should also refer to Guideline number 2 of the Guidelines on Paralegals.

> GUIDELINE 2: PROVIDED THE LAWYER MAINTAINS RESPONSIBILITY FOR THE WORK PRODUCT, A LAWYER MAY DELEGATE TO A PARALEGAL ANY TASK NORMALLY PERFORMED BY THE LAWYER EXCEPT THOSE TASKS PROSCRIBED TO A NONLAWYER BY STATUTE, COURT RULE, ADMINISTRATIVE RULE OR REGULATION, CONTROLLING AUTHORITY, THE APPLICABLE RULE OF PROFESSIONAL CONDUCT OF THE JURISDICTION IN WHICH THE LAWYER PRACTICES, OR THESE GUIDELINES.

As we said in Part I, cloud computing consists more and more of integrated services. For example, in some SaaS services of time, billing, and invoicing, lawyers simply input their time and the system generates an invoice. However, lawyers must remember that *they* are responsible for the billing, and they must make sure that the fees invoiced to clients are not "unreasonable" pursuant to the requirement of Rule 1.5 (and state equivalent) because if they are, lawyers could not defend themselves by blaming the cloud system for invoicing. The same is true, for example, for case and client management systems, which include calendaring of cases and docket management. If the system miscalculates the statute of limitation and the claim is time-barred, lawyers cannot defend a malpractice claim alleging that the statute of limitation was missed because of a system's fault.

Guideline number 6 is also quite interesting:

> GUIDELINE 6: A LAWYER IS RESPONSIBLE FOR TAKING REASONABLE MEASURES TO ENSURE THAT ALL CLIENT CONFIDENCES ARE PRESERVED BY A PARALEGAL.[64]

[63] Pennsylvania Formal Opinion 2011-200, above at note 59.
[64] *Guidelines on Paralegals*, above at note 61, at 9.

This principle is reflected also in some ethics opinions on cloud computing.[65]A North Carolina ethics opinion[66] talks specifically of lawyers' obligation to ensure that data are kept confidential by cloud providers. An Oregon ethics opinion states:

> [a] lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential. Under certain circumstances, this may be satisfied though a third-party vendor's compliance with industry standards relating to confidentiality and security, provided that those industry standards meet the minimum requirements imposed on the Lawyer by the Oregon RPCs.[67]

We will also offer some advice on compliance with Rule 5.3 in Part IV where we provide a checklist for lawyers.[68]

(iv)Duty to communicate with the client

Model Rule 1.4 imposes a general duty to communicate with clients.[69] Model Rule 1.4 has been adopted in very similar ways by almost all American jurisdictions. For example, Nevada Rule 1.4 – which is exactly the same as the ABA Model Rule in parts (a) and (b) but adds a subdivision (c) -- provides:

> Nevada Rules of Professional Conduct Rule 1.4. Communication.
> (a) A lawyer shall:
> (1) Promptly inform the client of any decision or circumstance with respect to which the client's informed consent is required by these Rules; (2) Reasonably consult with the client about the means by which the client's objectives are to be accomplished; (3) Keep the client reasonably informed about the status of the matter; (4) Promptly comply with reasonable requests for information; and (5) Consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.
> (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

The duty to communicate with the client extends to a law firm's technology choice. Law firms should develop policies on technology issues and should include them in the firm's engagement agreements seeking client consent to those policies, and inviting clients to inform their lawyers if they wish the firm to use different approaches. Law firm's use of cloud computing should be part of this

---

[65] See Part II of this paper.

[66] North Carolina, 2011 Formal Ethics, above at note 58, at 6

> The extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically with professionals competent in the area of online security.

[67] Formal Opinion No. 2011-188 (*Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials*), available at http://www.osbar.org/_docs/ethics/2011-188.pdf

[68] For other useful guidance on dealing with cloud provider under the perspective of complying with Rule 5.3, see Nathan Crystal, *Ethical Obligations in Using Paralegals, SC Lawyer 8* (July 2009).

[69] Full text of the Rule 1.4 at
http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_4_communications.html

communication.[70]To be sure, the duty to communicate law firm's technology policy is different from the duty of confidentiality to the client because, even if the law firm is compliant with its confidentiality obligation, the client has the right to make informed decisions on the representation (for example, clients might decide that they want to retain a law firm with a different technology policy or they have a special request on how their information must be handled).

In addition, in 2011, the ABA Committee on Ethics and Professional Responsibility issued Formal Opinion #11-459, which imposed a specific duty to communicate with the client when the lawyer is

> sending or receiving substantive communications with a client via e-mail or other electronic means . . . about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access.

Opinion #11-459 makes specific reference to the case of a lawyer representing an employee

> when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client- lawyer communications via e-mails or other electronic means, using a business device or system under circumstances where there is a significant risk that the communication will be read by the employer or another third party.[71]

Even if the opinion is based on Rule 1.6 (confidentiality) and Rule 1.1 (Competency), our opinion is that a similar obligation could also be grounded on Rule 1.4 (duty of communication). A similar obligation to communicate with clients has also been found by several ethics opinions dealing with cloud computing and encryption.[72]

The duty to communicate with clients is also required of European lawyers. This duty, however, is not as well develop in Europe as in the U.S. Article 3.1.2 of the European Code of Conduct provides that lawyers "shall keep the client informed as to the progress of the matter with which the lawyer has been entrusted."Article 40 of the Italian Code of Conduct provides, among other obligations, that "A lawyer

---

[70] Professor Crystal wrote that law firms should develop policies on technology issues (among which cloud computing) and should include in the firm's engagement agreements "a provision summarizing the firm's policies with regard to the use of technology, seeking client consent to those policies, and inviting clients to inform their lawyers if they wish the firm to use different approaches." *Technology and Confidentiality, Part I*, above at note 42. For an example of technology clause in retainer agreement, see *Technology and Confidentiality, Part II* (above at note 1):

> This law firm uses various devices in the representation of clients, including desk top and laptop computers, smart phones, tablets, copy and fax machines, and flash drives. These devices use a number of different applications, including word processing, email, and spread sheets. The devices also contain memory in which information is stored. These devices and their applications have increased the efficiency of the practice of law to the benefit of clients. At the same time the use of these devices, applications, and data storage systems have increased the transmission and storage location of client information, thereby increasing the risk that such information may be compromised. The firm has instituted various policies and procedures to protect the confidentiality of client information. A detailed statement of these policies and procedures is available at ----. By signing this engagement you consent to the firm's use of these technologies in accordance with the policies and procedures adopted by the firm. If you have any questions, concerns, or special requests regarding the protection of your confidential information, please discuss the matter with the attorney who is responsible for your case or with ---, the managing attorney of the firm.

[71] Full Formal Opinion #11-459, available at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf

[72] See Part II of this paper.

shall also inform his client about the proceeding of the case, every time the lawyer finds it useful and anyway every time that his client asks information." and also "A lawyer shall communicate to his or her client everything that the lawyer learns in performing the legal activities [for him or her] if useful to the client's interest."[73]

With specific reference to the cloud, the CCBE Guidelines on Cloud states that a lawyer "might consider" informing clients of lawyer's use of the cloud: "[i]n order to ensure transparency of legal services, a lawyer might consider informing his future clients that the law firm uses cloud computing services."[74]

3. Legal risks

Malpractice claims from the use of cloud computing services can arise in a variety of ways.[75] For example, in the bankruptcy of Adelphia Communications, when the law firm Boies Schiller & Flexner (which assisted Adelphia) requested payment of its legal fees, the trustee asked the judge to appoint a special examiner to explore a possible conflict of interests: David Boies' children owned a stake in Amici, a document management company that Adelphia had used for years at the law firm's recommendation.[76] So claims for conflict of interests in the choice of a cloud provider are not farfetched and neither are other grounds for possible malpractice claims: for example, failure to obtain client consent to certain costs connected to cloud, failure to follow the client's instruction on the choice of cloud, loss of files and documents, ancillary business issues, and so on. However, among the several possibilities of malpractice that a lawyer can face as a consequence of the use (or the nonuse) of the cloud ("Cloud Legal Malpractice"), we would like to focus our attention on three particular instances of possible Cloud Legal Malpractice: the negligent loss of proprietary information, the allegation that a certain attorney-client privilege was lost,[77] and the cloud provider's inappropriate response to subpoenas and court orders. As an example of the first, imagine that a lawyer is assisting a client who has proprietary know-how on a certain working method; the lawyer stores the client's file in the cloud, but the information is leaked on the Internet and becomes valueless. The client loses the possibility to license the know-how and sues the lawyer. As an example of the second, imagine that during a proceeding a lawyer gives a certain critical legal advice that would be protected by attorney client privilege[78] (and so inadmissible in evidence and not

[73] Unofficial translation made by the authors.
[74] *CCBE Guidelines on Cloud*, above note 41, at 9.
[75] The grounds for legal malpractice in the U.S. are many. *See, e.g.,* Dan Pinnington, *The Most Common Legal Malpractice Claims by Type of Alleged Error* (above at note 28).
[76] See Roger Parloff, *Boies firm says: Where's the beef?* available at http://money.cnn.com/2006/02/06/news/newsmakers/boies2_fortune/.
[77] CA Formal Op. No. 2010-179 cautions lawyers to weigh inadvertent disclosure and its impact on applicable privileges.
[78] For our non-American readers, attorney-client privilege is a rule of evidence that shields from discovery the information and documents that are exchanged in confidence between lawyer and client. The protection can be waived by inadvertent disclosure of confidential material. NATHAN CRYSTAL, PROFESSIONAL RESPONSIBILITY – PROBLEMS OF PRACTICE AND THE PROFESSION, above at note 25, at 127.

discoverable). However, unfortunately, the information stored in the cloud is revealed and the judge ruled that the revelation amounted to a waiver of the privilege under applicable law. The client loses the law suit and sues the lawyer alleging that but for the loss of the privilege, the client would have won the law suit.

In the first situation the lawyer can be held liable for failure to exercise due diligence with regard to the activities of the cloud computing service. This is a question of reasonable care and in a legal malpractice case the plaintiff will present expert testimony that the defendant lawyer violated the standard of care expected form lawyers. What is below the standard of care is determined by common law and is a question of fact for the jury.

The second situation is more complicated because an evidentiary rule (attorney-client privilege) is involved. In federal cases (and in some states) the issue of when inadvertent disclosure amounts to a waiver of the privilege, is regulated by Federal Rule Evidence 502; some states have also adopted rules similar to FRE 502. If FRE 502 or a similar state rule does not apply, the issue is unsettled; courts generally follow three different approaches on the issue of whether inadvertent disclosure amounts to a waiver of the attorney-client privilege.

> [US] [c]ourts apply three approaches to waiver of the privilege. The traditional approach was that any disclosure results in a loss of the privilege because the purpose of the privilege was to protect confidential communications; by definition, a communication that has been disclosed is no longer confidential. Other courts have held that the purpose of the privilege is to protect the client's reasonable expectations. Under this limited waiver approach, the privilege is lost only if the client intends to waive the privilege. Finally, the modern approach looks at the facts and circumstances, especially the precautions taken, to determine whether the privilege should apply.[79]

The inadvertent disclosure issue was so troublesome in discovery that

> [i]n 2006, the federal rules of civil procedure were amended to protect against the loss of the attorney-client privilege or work product protection through inadvertent production of privileged material during discovery"[80] and "[i]n 2008 the Federal Rules of Evidence were amended to deal with the issue of when inadvertent disclosure amounts to a waiver of the attorney-client privilege and of work product protection.

> [T]he attorney-client privilege is a rule of evidence that deals with the question when a lawyer may be compelled in court or other official proceedings or investigations to reveal information received in confidence from a client. Although the scope of the attorney-client privilege depends on the rules of evidence applicable in each jurisdiction, a frequently cited formulation is the one offered by Professor Wigmore:
>
> > (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived. (8 Wigmore on Evidence §2292, at 554 (McNaughton ed. 1961).

[79] *Id.* at 344. See Fed.R.Civ.P. 26(b)(5)(B).

[80] NATHAN CRYSTAL, PROFESSIONAL RESPONSIBILITY – PROBLEMS OF PRACTICE AND THE PROFESSION, above at note 25, at 345.

The first change concerns Federal Rule of Civil Procedure 26(b)(5)(B), while the second concerns the previously cited Federal Rule of Evidence 502.Thanks to the amendments to the FRE 502, we know today that in cases governed by FRE 502 under which circumstances disclosure of privileged material amount to a waiver of attorney-client privilege and work product protection with regard to the disclosed material and when the waiver applies beyond the particular document in question to cover other documents that are part of the same subject matter. And thanks to the amendment to FRCP 26(b)(5)(B), we have now "a method for a party who has produced information that is subject to a claim of either ACP or WPP to prevent use or dissemination of the material pending a resolution of the claim."[81]This is certainly helpful but the coverage of those rules is limited because both rules apply only when there is a federal procedure.[82]"If the disclosure is not in connection with such a proceeding, then the …[rules do] not apply and common law principles will determine whether a waiver has occurred."[83]

In conclusion, the use of cloud computing has the "potential" to generate a waiver of the privilege determined either by federal law or common law principles depending on where the proceeding takes place.

Cloud computing also has the potential to create special risks and required special precautions in specialized fields of practice. For example for law firms possessing information related to national defense matters relevant under the International Traffic in Arms Regulations. The use of cloud computing by those entities and also by their lawyers, when the cloud is located outside of the U.S., may amount to an "export" under applicable law.[84]Many of the recommended standards that apply in this special area are a heightened version of the standards that apply generally to law firms dealing with the cloud.[85] Similarly law firms possessing protected care information under HIPAA have to take additional protective measures.

---

[81] Nathan Crystal, *Inadvertent Production of Privileged Information in Discovery in Federal Court: The Need for Well-Drafted Clawback Agreements*, 64 S.C.L. Rev. 581 (2013).

[82] "Rule 502 extends beyond federal proceedings . . . [because] [u]nder section (d), if a federal court orders that a disclosure connected with litigation before the court is not a waiver, then the order applies "in any other federal or state proceeding." *Id.* However, there must be a federal procedure for the protection of FRE 502 to apply.

[83] *Id.*

[84] See International Traffic in Arms Regulations (ITAR), 22 C.F.R. pt. 120 et seq. which defines "Export" as "Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." *Id.* at 120.17(a)(4).
Full text of the regulation at http://www.ecfr.gov/cgi-bin/text-idx?SID=d306488fd350f4279b82026aaee8eb33&node=22:1.0.1.13.57.0.31.17&rgn=div8

[85] In April 2013, at the Annual Meeting of the ABA International Section, the program "Lost in the Clouds: How Do You Control the Export of Data to Anywhere When It's Stored Everywhere?" dealt with this point and the material for the program made the point that "Clouds may facilitate the transfer of controlled technology, technical data or software to a country other than the one in which it was uploaded, triggering export authorization requirements" (Palmeri powerpoint, slide 10, available at http://archive.aievolution.com/2013/aba1301/index.cfm?do=ev.viewEv&ev=3023). In the program, the panelists referred to Department of Commerce Advisory Opinion - January 2009 according to which a cloud provider is not considered the "exporter" when the user exports data on the cloud. It is interesting to notice that the panelists gave advice very similar to that given to law firms in general by the ethics opinions dealing with cloud computing (see Part II of this paper) and by the CCBE (see Part III of this paper):

Compliance Best practices:
• Risk Assessment

The third "peculiarly American" risk of the cloud is connected to pre-trial discovery.[86] A cloud provider is a nonparty in possession of relevant documents which pursuant to FRCP Rule 34(c) "may be compelled to produce documents and tangible things or to permit an inspection." The subpoena's requirements and procedures are established by FRCP 45. Under 45(c)(2)(B) the receiver of a subpoena can make several objections to the request or order of production;[87] the risk is that the cloud provider might not be equipped to properly answer subpoenas and to make all the possible objections. The New York City Bar's Report on Cloud highlights this risk:

> Other Types of Unauthorized Disclosure: data breaches are not the only causes of unauthorized disclosure of data. Data may also be disclosed if the service provider has inadequate procedures for responding to (or, when appropriate and permissible, resisting) subpoenas, court orders, or other process seeking production of information.[88]

4. Security of data

Probably a potential security breach is the most discussed cloud risk. While certainly a security breach is possible, the risk might have been overstated:

> [C]loud computing can trigger some thorny ethical and security issues for lawyers, but in many cases can also provide better security than that currently being used by many law firms. For example, encrypted communications via cloud computing platforms [which some providers provide] offer far more security than the unencrypted emails typically used by most law practices.[89]

•Policies and Procedures
•Transaction/Business Activity Monitoring, Screening, Surveillance
• Contractual Provisions
•Compliance Control Process Monitoring
•Metrics and Management Information
•Regulatory Reporting and Communication
•Training
•Advice and Counsel
•Program Change Management
•Independent Testing/Audit

86 For nonAmerican readers interested to know more about American discovery by way of comparison with Europe, see Nathan Crystal & Francesca Giannoni-Crystal, *Understanding Akzo Nobel: A Comparison of the Status of In-House Counsel, the Scope of the Attorney-Client Privilege, and the Discovery in the U.S. and Europe*, Global Jurist: Vol. 11: Iss. 1 (Topics) (2011), Article 1, available at http//bepress.com/gj/vol11/iss1/1

87 ***Objections.*** A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises -- or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the issuing court for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

88 *New York City Bar's Report on Cloud*, above at note 53, at 10.

89 Nicole L. Black, *Cloud Computing for Lawyer*, above at note 20.

In fact, the use of the cloud may *increase* security of data rather than the reverse. Cloud providers generally have certificates on the security level of their systems[90] that law firms' systems do not have. The reality is that law firms are a preferred target for cyber attacks in the U.S:[91]

> As larger companies have increased their security vigilance, they've made access to information much more difficult for thieves. As a result, hackers have turned their sights to easier victims—smaller firms of fewer than 100 employees that store data in electronic form.[92]

In addition, concern about a cloud provider's level of security might be regulated by confidentiality clauses in provider agreements and other clauses to ensure that the cloud provider has procedures in place to comply with personal information protection laws or the particular requirements of the data owner.

In the U.S., forty-six states, the District of Columbia, and some territories have enacted personal information protection laws requiring notification of security breaches involving personal information.[93]These laws require notification if there is a security breach, i.e. if personal client information stored in the cloud is inadvertently disclosed. For example, the New York law defines a "breach of the security of the system" to mean:

> unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.[94]

The information protected is only "private information" and does not "include publicly available information which is lawfully made available to the general public from federal, state, or local government records."[95]The notification requirements vary. In the District of Columbia, for example the statute provides that "[a]ny Entity to which the statute applies, and who discovers a breach of the security system,

---

[90] For example Google Apps has been issues SSAE 16 and ISAE 3402 certificates by an independent third party auditor, which verified several factors (Logical security, Privacy, Data center physical security, Incident management and availability, Change management, Organization and administration) and SAS70 Type II certificate (another certificate issued by an independent third party which verified similar factors). See https://support.google.com/a/answer/60762?hl=en

[91] The increasing number of data theft and espionage incidents in cyberspace has been widely reported, and law firms have become particularly attractive targets. One data security company reports that 10% of the advanced cyber attacks it investigated in the past 18 months were targeted at law firms. Alan W. Ezekiel, Hackers, Spies, And Stolen Secrets: Protecting Law Firms From Data Theft, 26 Harv, J.L & Tech.649, 650 (2013).

[92] *The Top 10 Hacker-Defense Strategies for Small Business*, WALL ST. J., July 21, 2011, available at http://www.wipfli.com/resources/images/23516.pdf.

[93] See National Conference of State Legislatures, *State Security Breach Notification Laws*, available at http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

[94] NY Gen. Bus. L. §899-aa(1)(c). Full text available at http://codes.lp.findlaw.com/nycode/GBS/39-F/899-aa

[95] *Id.*

shall *promptly* notify any DC resident whose PI was included in the breach"[96] and that in case of a breach involving the data of many people, notification to some agencies is also required.[97]In Florida

> [t]he notification shall be made *without unreasonable delay*, consistent with the legitimate needs of law enforcement . . . or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.[98]

In Illinois, the "disclosure notification shall be made *in the most expedient time possible and without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system" and shall include "(i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes."[99]At the federal level, the SEC (Division of Corporation Finance) has outlined requirements that companies report cyber theft and attack.[100]

Independently from security breach laws and federal regulations, and even when these laws and regulations do not apply[101]"a law firm representing . . . clients that suffered a security breach would be ethically required to inform the . . . clients about the breach so that they could make informed decisions regarding the matter [even where the law firm would be not required to do so by the security breach law]."[102]

---

[96] D.C. Code § 28-3851 *et seq*., "Notification Obligation". Full text available at http://www.perkinscoie.com/sc_dc/ (emphasis added).

[97] *Id.*

> **Notification to Consumer Reporting Agencies.** If any Entity is required to notify more than 1,000 persons of a breach of security, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.

[98] Fla. Stat. § 817.5681, (1)(a) available at http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0800-0899/0817/Sections/0817.5681.html. (emphasis added).

[99] 815 ILCS 530/1 *et seq.* available at http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815%C2%A0ILCS%C2%A0530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act. (emphasis added).

[100] CF DISCLOSURE GUIDANCE: TOPIC NO. 2, available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[101] For example the South Carolina security breach law, 39-1-90(A), only applies to personal information of individuals (not businesses):

> A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose *personal identifying information* that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. (emphasis added).

"Personal identifying information" means the name of a person in association with some other piece of important information such as a social security or bank account number by S.C. Code 16-13-510(D)

[102] Nathan Crystal, *Technology and Confidentiality, Part II*, above at note 1.

5. Technical risks

Which are the technical risks that lawyers face in using cloud computing services?To be sure: technical pitfall *may* result in an ethical violation, legal action (in tort or contract), damage to reputation, or all of the above. So the following discussion on technical risks should be read in conjunction with the discussion on possible ethical pitfalls,[103] and legal risks.[104] A technical pitfall can also mean a violation of security law.[105] However, to be clear, an ethical violation can result from the use of the cloud even when there is no technical pitfall. A lawyer could receive a disciplinary sanction for having adopted cloud computing without the appropriate due diligence[106] or a client could sue the lawyer for breach of contract or for breach of fiduciary duty because, for example, the lawyer and client had expressly agreed that the lawyer would not use cloud computing.[107]

Technical risks can be divided into two categories: external risks associated principally with the provider of the service and internal risks associated with the firm's ability to adopt and execute policies and procedures to deal with risks associated with the services.[108] The following are major risks associated with SaaS, the most common type of cloud service used by law firms:

(i)External risk[109]

> Unauthorized disclosure resulting from security breaches of the provider;

> Other unauthorized disclosures resulting from inadequate procedures by providers to deal with demands for information, such as subpoenas;[110]

> Lack of clarity about ownership and provider ability to license use of the data;

> Temporary loss of access to data due to Internet connection failure, provider maintenance, or provider failure;

> Permanent loss of data resulting from provider business failure;

> Geographical risks associated with location of servers housing the data in other countries where the governing law may be different;

> Problems of return of the data on termination of service.

These risks can be evaluated generally, but specific attorney-client relationships may generate particular problems. For example, if the client, whether a governmental entity or a private client dealing

---

[103] See Part I(B)(2).
[104] See Part I(B)(3).
[105] See Part I(B)(4).
[106] See below Part II of this paper.
[107] Even if an action against a law firm for breach of contract or breach of a fiduciary duty not to use the cloud might fail for lack of damage, a disciplinary action could still lie because damage is not an element of a disciplinary proceeding.
[108] *New York City Bar's Report on Cloud*, above at note 53, at 7.
[109] *Id.* at 10-12.
[110] See above Part I(B)(3).

with the government, handles information with national security implications, special precautions and protections are required. Similarly, if the information is protected by specific laws as is the case with information covered by the Health Information Portability and Accountability Act (HIPAA), the regulatory requirements imposed by this Act must be met.[111]

(ii) Internal risk

The internal risk is that the firm will fail to adopt and implement policies and procedures designed to eliminate or minimize the external risk associated with the use of cloud services. In addition, firms face their own internal risks in handling data regardless of whether they use cloud computing services;[112] they need to establish appropriate policies and procedures to eliminate or minimize risk associated with their own use of data. For example, firms need to have policies regarding the types of devices that lawyers can use in dealing with client data[113] and disposal of those devices.[114]

PART II -- THE APPROACH OF SEVERAL AMERICAN JURISDICTIONS TO CLOUD COMPUTING[115]

The business advantages to cloud computing are clear.[116] So are the possible ethical concerns. So, we should be asking: can a lawyer *ethically* reap the benefits of cloud computing? Ethics committees in at least sixteen U.S. jurisdictions[117] have answered the question affirmatively.[118] The opinions rely heavily on a lawyer's use of "reasonable care" or some variation of that term.[119] We will analyze these opinions first and

---

111 Part III(A).

112 See the discussion of security breach notification laws and the ethical obligation to disclose material information to clients, above at note 93.

113 Nathan M. Crystal, *Technology and Confidentiality*, *Part I*, above at note 42, paragraph "*Loss of pen drives, smart phones, laptops, or other devices*":

> Reasonable precautions require law firms to recognize the possibility of loss of devices and to develop appropriate policies to reduce the risk of loss. It would be useless to implement sophisticated protection from digital attacks, when the confidentiality of the client can be violated simply by the drop of a pen drive. . .. Which precautions to use with these portable devises Then? Simply enough, a firm could prohibit the use of personal devices on firm matters. Lawyer would be required to use only firm flash drives, PDAs, and laptops that have file encryption, that are password protected, and that contain confidentiality notices with instructions for return on the case of the device.

114 *Id.* (Paragraph "*Disposal of Devices"*):

> The number of devices with hard drives that can store confidential client information is enormous, including computers, printers, copiers, scanners, cellular phones, personal digital assistants, flash drives, memory sticks, and facsimile machines. When such devices are disposed of there is a risk of disclosure of confidential client information.

Professor Crystal cites a Florida Bar Professional Ethics Committee opinion (Opinion #10-2) addressing and providing advice to lawyers to deal with these issues.

115 We thank Richard Callison, Esq. contract attorney for Crystal & Giannoni-Crystal, LLC, for the primary work in the preparation of Part II of this paper.

116 *See* PA Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011) (listing the benefits of cloud computing).

117 In alphabetical order: Alabama, Arizona, California, Connecticut, Florida, Iowa, Maine, Massachusetts, New Hampshire, New Jersey, New York, Nevada, North Carolina, Oregon, Pennsylvania, and Vermont. For a commentary to some of these opinions, see Andrew L. Askew, *iEthics: How Cloud Computing has Impacted the Rules of Professional Conduct*, North Dakota Law Review; 2012, Vol. 88 Issue 2, p453, available at http://heinonline.org/HOL/LandingPage?handle=hein.journals/nordak88&div=20&id=&page=

118 *See* ABA, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (the ABA's list recognizes fourteen of the sixteen ethics opinions considered in this discussion).

119 *Id.*

then we will try to have a better understanding of the amorphous term "reasonable care" with a few detours. We will also talk of the cases in which the client's consent is advisable and when the encryption of communication should be considered a reasonable precaution. In Part IV of this paper we provide a checklist which takes account of these opinions.

A. A LAWYER MAY ETHICALLY STORE CLIENT INFORMATION IN THE CLOUD

The consensus among ethics opinions addressing the issue is that, with some caveats,[120] a lawyer may ethically use cloud-based services.[121] It would be tedious to discuss all the ethics opinion on cloud computing. Therefore, we will focus on a number of opinions. The opinions that we have chosen are illustrative of the evolution in terminology (which parallels the evolution of technology) and of the fact that the caveats remain much the same.

Ethics committees from Nevada and New Jersey were among the first to render cloud storage opinions back in 2006.[122] In Formal Opinion No. 33, the State Bar of Nevada Standing Committee on Ethics and Professional Responsibility[123] reformatted the inquiring attorney's question to address the storing, without client consent, of confidential client information in electronic format on a device that is not exclusively controlled by the lawyer.[124] The committee analogized the situation to storing confidential paper files in a third-party warehouse and concluded that contracting with a third-party to store information was not an ethical violation so long as the "lawyer acts *competently* and *reasonably* to ensure the confidentiality of the information."[125] The conclusion, states the committee, would not be altered even if an unauthorized or inadvertent confidentiality breach should later occur.[126] One of the rules relied upon by the committee in reaching its result was Model Rule 1.6[127] and comments as enacted at the time of the opinion which "reinforce the view that electronic communications and information require *no special security or confidentiality measures* that would not otherwise be required in communication in a more traditional format."[128]

In Opinion 701, the New Jersey Advisory Committee on Professional Ethics set forth principles similar to those of the Nevada opinion by analyzing New Jersey Rule of Professional Conduct 1.6.[129] The opinion cautions that reasonable care must be used to prevent unauthorized disclosure of client

---

120 *See* Part II(B) below.
121 NH Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013).
122 NJ Supreme Court Advisory Comm. on Prof'l Ethics, Op. 701 (2006); State Bar of NV Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. No. 33 (2006).
123 NV Formal Op. No. 33, available at http://www.nvbar.org/node/98
124 *Id.*
125 *Id.* (emphasis added).
126 *Id.*
127 MODEL RULES OF PROF'L CONDUCT R. 1.6 (1983).
128 NV Formal Op. No. 33. (emphasis added).
129 NJ Op. 701.

confidences but does not read Rule 1.6 "as imposing a per se requirement that, where data is available on a secure web server, the server must be subject to the exclusive command and control of the firm through its own employees."[130]

Turning to the most recent opinion, 2012 the Massachusetts Bar Association Committee on Professional Ethics interpreted Rule 1.6 of the Massachusetts Rules of Professional Conduct in a similar fashion but in a more technologically-modern setting.[131] The committee considered storage and synchronization of client files in cloud-based systems such as "Google docs", Microsoft's "Windows Azure", Apple's "iCloud", or Amazon's "S3".[132] The committee framed the issue as whether the small, but real, risk of unauthorized access is unreasonable in violation of Rule 1.6.[133] Relying on several previous Massachusetts opinions, the committee concluded that use of Internet based storage systems would not result in an ethical violation so long as the lawyer expends reasonable efforts to comply with the lawyer's ethical obligations, including the responsibility to protect client confidences.[134]

More recently, the Connecticut Ethics Committee answered the question whether "it is permissible under the Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law." The Committee considered that "[t]here is a great deal being written about cloud computing every day" and cuts its opinion on the SaaS. The Committee acknowledges the financial and "technological benefit for the user" but warns lawyers that they have the "ultimate responsibility for insuring the privacy and security of the data" and that '[w]hile much of the physical, technical, and administrative safeguards are handled by the cloud service provider, the user will still retain responsibility for a significant portion of these safeguards." Lawyers should read carefully the "Service Level Agreement ("SLA") or Terms of Service" to see if these terms impact on their ethical obligations and how. The Committee reminded lawyers that the use of the cloud impacts on all the following obligations: Comment [8] to Rule 1.1. ("keep abreast of changes in the law and its practice, including . . . technology"), Rule 1.6 (confidentiality), Rule 1.15 (safeguard of clients' property), Rule 5.1 (supervision of lawyers), and Rule 5.3 (supervision on nonlawyers). The Committee concluded:

> Lawyers may use cloud services in their practice to promote mobility, flexibility, organization and efficiency. However, lawyers must be conscientious to comply with the duties imposed by the Rules to knowledgeably and competently maintain confidentiality and supervisory standards. The Rules require that lawyers make reasonable efforts to meet their obligations to preserve the confidentiality of client information and to confirm that any third-party service provider is likewise obligated.

---

130 *Id.*
131 Mass. Bar Ass'n Comm. on Prof'l Ethics, Op. 12-03 (2012), available at http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03
132 *Id.*
133 *Id.*
134 *Id.*

Between the early opinions addressing electronic third-party storage of client files (Nevada[135] and New Jersey[136]) and the more recent opinions depicting current cloud-based systems and their features and policies (for example Massachusetts,[137] and Connecticut[138]), other ethics committees have put forth opinions with varying degrees of detail and recognition of modern trends on this issue.[139] However, a clear common theme permeates all the opinions: while cloud computing is ethical, a lawyer must use "reasonable care".[140]

In addition, some opinions have addressed the issue of obtaining client consent under certain circumstances and others have discussed encrypting email correspondence.[141] The result for our discussion is a necessity to understand the parameters of "reasonable care" as applied to cloud computing, including whether consent from the client is warranted in a particular case and the instances when email encryption should be considered.

B. MEANING OF "REASONABLE CARE"

What level of care is reasonable? Model Rule 1.6(c) uses the term "reasonable efforts" to describe an attorney's obligation to take preventative measures to avoid unauthorized or inadvertent disclosure of, or unauthorized access to, client information.[142] Comment [18] to the rule adds a non-exhaustive list of factors for determining reasonableness of the efforts.[143] But the rule and comments do not, and could not, encompass all the choices available to a tech-savvy lawyer. Ethics opinions provide more guidance in this regard. The approach of most ethics committees has been to decline to explicitly set forth specific conditions precedent to cloud computing by specifically defining the concept of "reasonable care".[144] This is appropriate given the evolving nature of available services. The State Bar of California Standing Committee on Professional Responsibility and Conduct – which rendered an opinion in the context of

---

135 State Bar of Nevada Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. No. 33 (2006).
136 New Jersey Supreme Court Advisory Comm. on Prof'l Ethics, Op. 701 (2006).
137 Massachusetts Bar Ass'n Comm. on Prof'l Ethics, Op. 12-03 (2012).
138 Connecticut Bar Ass'n Prof'l Ethics Comm., Informal Op. 2013-07 (2013), available at http://www.ctbar.org/userfiles/Committees/ProfessionalEthics/Opinions/Informal_Opinion_2013-07.pdf
139 Alabama State Bar Disciplinary Comm'n, Formal Op. 2010-02 (2010); State Bar of Arizona Comm. on the Rules of Prof'l Conduct, Ethics Op. 09-04 (2009); State Bar of California Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 2010-179 (2010); Florida Bar Prof'l Ethics Comm., Op. 12-3 (2013); Iowa State Bar Ass'n Comm. on Ethics and Practice Guidelines, Op. No. 11-01 (2011); Bd. of Overseers of the Bar State of Maine, Op. #194 (2008); New Hampshire Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013); New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 842 (2010); North Carolina State Bar Ethics Comm., 2011 Formal Op. 6 (2012); Oregon State Bar, Formal Op. 2011-188 (2011); Pennsylvania Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011); Vermont Bar Ass'n Ethics Comm., Advisory Ethics Op. 2010-6 (2010).
140 *Id.*
141 *See* Parts II(C) and (D) below on client consent and encryption.
142 MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (1983).
143 *Id.* cmt. 18.
144 VT Bar Ass'n Ethics Comm., Advisory Ethics Op. 2010-6 (2010), above at note 60.

using a public wireless Internet connection -- has astutely recognized that such an opinion "would likely become obsolete shortly."[145]

Ethics committees, however, have not left lawyers empty-handed. A lawyer, conducting an investigation related to a technological service, has a plethora of guidelines from ethics opinions to help in fulfilling the duty to use reasonable care.

Pennsylvania has set forth likely the most extensive list of considerations.[146] The opinion shrewdly groups various types of software and services, including email, under the label of "cloud computing" and then asks "[m]ay an attorney ethically store confidential client material in 'the cloud'?"[147] While the question is presented modestly, the committee's venture into the background and risks of cloud computing is rigorous. Ultimately, the committee presents a 15-point list, with additional sub-points, to help define the cloud computing standard of reasonable care.[148] The Committee does not present its list as containing mandatory requirements ("standard of reasonable care for 'cloud computing' *may* include")[149] however the suggestions are quite stringent.[150] The opinion also provides summaries of ethics opinions from other bodies.[151]

---

145 The State Bar of CA Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 2010-179 (2010), available at http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3D&tabid=836

146 PA Formal Op. 2011-200, available at http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf

147 *Id.*

148 *Id.*

> [T]he standard of reasonable care for "cloud computing" may include:
> • Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
> • Installing a firewall to limit access to the firm's network;
> • Limiting information that is provided to others to what is required, needed, or requested;
> • Avoiding inadvertent disclosure of information;
> • Verifying the identity of individuals to whom the attorney provides confidential information;
> • Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
> • Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
> • Implementing electronic audit trail procedures to monitor who is accessing the data;
> •Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;
> • [Agreeing on several clauses with the cloud provider, among which the fact that provider] explicitly agrees that it has no ownership or security interest in the data; . . . includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;. . . will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania; provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity;
> •Investigating the provider's:
> o security measures, policies and recovery methods;
> o system for backing up data;
> [and other aspects of the provider's data protection policies and procedures]
> •Employees of the firm who use the SaaS must receive training
> •Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.
> •Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

149 *Id.*

150 While we cannot conduct a specific discussion of the Pennsylvania opinion, we want to notice that should the suggestions given by the Pennsylvania Committee on reasonable care be interpreted as required (which the opinion does not seem to say), it would be very difficult for

The level of detail in ethics opinions from other jurisdictions varies. For example, Arizona's opinion, due no doubt to the context of the inquiry (a lawyer had asked the committee to opine about the ethical propriety of using "a service to clients that would allow clients online access to view and retrieve client file"[152]), provides a humble set of guidelines.[153] In fulfilling the reasonable care requirement of Rule 1.6, the committee wrote that lawyers "should consider firewalls, password protection schemes, encryption, anti-virus measures, etc."[154] The committee also noted that lawyers should be aware of their technical limitations.[155] A lawyer should take the time to become competent about security measures or consult an expert.[156] The committee hedged that the measures taken in this instance might not be adequate in the future as safeguards evolve, and lawyers should periodically revisit the safety of client information.[157]

The California opinion cited above expanded an inquiry it received to address a lawyer's duty of confidentiality and competence when transmitting and storing client information through the use of technology that is susceptible to third-party interception or access.[158] Because technology continues to rapidly evolve, the "opinion sets forth the *general* examination that an attorney should undertake when considering use of a particular form of technology."[159] Among other guidance, the opinion suggests not only reviewing the security a particular form of technology affords but also additional security that can be used as enhancement.[160] The legal ramifications, such as civil or criminal penalties, of third-party interception favor an expectation of privacy.[161] A lawyer should take into account the risk of inadvertent disclosure and its impact on applicable privileges.[162] Other considerations identified by the committee include the sensitivity of the information,[163] the urgency of the situation, and adhering to client instructions regarding the use of technology.[164]

The North Carolina State Bar Ethics Committee has, after revision, issued a formal opinion addressing a lawyer's use of "software as a service."[165] Predictably, the committee concluded that use of SaaS is ethical provided that appropriate measures are taken.[166] The committee properly refused to define

---

a Pennsylvania attorney to use the cloud. Some of the suggestions (for example, about agreeing on the geographical location of the servers) would require a contractual power towards the cloud provider that a cloud user usually does not have.

151 *Id.*; *see also* VT Advisory Ethics Op. 2010-6, above at note 60, (discussing cloud computing ethics opinions from various jurisdictions).

152 *Id.* The system would utilize encryption and three layers of randomly generated folders and passwords.

153 *Id.*

154 *Id.*

155 *Id.*

156 *Id.*

157 *Id.*

158 CA Formal Op. No. 2010-179, above at note 145.

159 *Id.* (emphasis added).

160 *Id.*

161 *Id.*

162 *Id.*

163 The advice to evaluate the sensitivity of information is a common theme in ethics opinions. See Part II(B)(4) on encryption.

164 *Id.*

165 NC State Bar Ethics Comm., 2011 Formal Op. 6 (2012), available at http://www.ncbar.com/ethics/printopinion.asp?id=855

166 *Id.*

reasonable care "because mandatory security measures would create a false sense of security in an environment where the risks are continually changing."[167] The committee set forth a five-point list of suggested security measures that should be included in the cloud service. In particular, the committee recommended inclusion of clauses in the cloud provider's terms of service or service level agreement dealing with how data management and data security will be handled that are in accord with the lawyer's ethical obligations.[168]

Similar to the ethics opinions just discussed, the New York State Bar Association Committee on Professional Ethics has provided a list of protective measures a lawyer might take in the exercise of reasonable care.[169] The committee noted that reasonable care requires a lawyer to check several aspects: (i) to ensure that the provider has an enforceable obligation to preserve security and confidentiality and to notify if the provider is served with process requiring the provider to produce client information; (ii) to investigate the provider's security measures and recovery procedures for adequacy; (iii) to evaluate how technology is used to prevent reasonably foreseeable attacks on stored client information; (iv) and to review procedures in the event the lawyer changes storage provider.[170]

The four-point list provided by the committee does not drastically differ from the conclusions of other ethics committees.[171] However, the committee adds that "technology and the security of stored data

---

[167] *Id.*

[168] *Id.*

> Although a lawyer may use nonlawyers outside of the firm to assist in rendering legal services to clients, Rule 5.3(a) requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer. The extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically with professionals competent in the area of online security. Some recommended security measures are listed below.
> • Inclusion in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.
> • If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.
> • Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy.
> • Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.
> • Evaluation of the extent to which the SaaS vendor backs up hosted data.

[169] The NY State Bar Ass'n Comm. on Prof'l Ethics, Op. 842 (2010), available at http://www.nysba.org/customtemplates/content.aspx?id=1499

[170] *Id.*

[171] *Id.*

> "Reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:
> (1) 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;
> (2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
> (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

are changing rapidly" and "[n]ot only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly."[172] With regard to the rapid change of technology, the committee stated that a lawyer should periodically review safeguards in place in light of advances in technology and should take appropriate action if the provider experiences a breach in security.[173] Appropriate action includes investigating whether any client information has been breached, notification to impacted clients, and discontinuance of service unless the lawyer receives assurances that the security issues have been remediated.[174] With regard to the rapid change of the law relating to technology, lawyers should stay abreast of developments particularly as they relate to waiver of privileges that might otherwise be applicable.[175]

Ethics opinions from Connecticut[176] and Maine[177] recite several of the considerations already discussed.[178] Notably, Maine opinion add that "the lawyer should also take care to ensure that confidential information is conveyed to the service provider in a secure manner."[179]The Connecticut opinion reminds that "online outsourcing" is subject to the rules pertaining to supervision of those hired by a lawyer and "a lawyer must ensure that tasks are delegated to competent and reliable people and organizations."[180]

C. CLIENT CONSENT TO CLOUD COMPUTING

A lawyer who handles particularly sensitive client information should consider obtaining informed consent from the client before transmitting client information to a cloud provider. The lawyer's engagement agreement is an appropriate vehicle to seek and obtain client consent because execution of the agreement occurs at the inception of the relationship; this is the moment when lawyers should learn if their clients have any objections or qualifications to the firm's use of cloud services.

Formal Opinion 2011-200 from Pennsylvania states that

> if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.[181]

---

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

172 *Id.*
173 *Id.*
174 *Id.*
175 *Id.*
176 Connecticut Bar Ass'n Prof'l Ethics Comm., Informal Op. 2013-07 (2013), above at note 138.
177 Bd. of Overseers of the Bar State of Maine, Op. #194 (2008), available at http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=86894&v=article
178 CT Bar Ass'n Prof'l Ethics Comm., Informal Op. 2013-07 (2013); Bd. of Overseers of the Bar State of ME, Op. #194 (2008).
179 *Id.*
180 CT Informal Op. 2013-07.
181 PA Formal Op. 2011-200, above at note 59.

Similarly, an ethics opinion from Vermont urges giving notice to the client about the method of data storage.[182]The Massachusetts opinion cautions that a lawyer should "refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so."[183] An opinion from New Hampshire is in accord expressing that "[n]ot all information is alike . . . where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."[184]The California opinion states that informed consent might be required depending on the sensitivity of the matter.[185]

In the case of highly sensitive information, client consent alone may not be sufficient; a lawyer may need to consider additional security measures or forgo cloud storage. A Florida opinion warns that a "lawyer should consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information."[186]

D. EMAIL ENCRYPTION

An issue that is "contiguous" to cloud computing and which law firms should carefully consider, is encryption. The issue is contiguous not only because email is the most widely used cloud computing service but also because encryption is a tool that can apply to any flow of data, not only email. Therefore, the issue whether a lawyer is ethically required to encrypt communication is important to cloud computing.

At least twenty-five jurisdictions (in addition to the ABA) have opined on the use of encryption of communication by lawyers. The overwhelming view is that encryption is not necessary unless special circumstances exist (for example, transmission of highly sensitive information). To be sure, while twenty ethics committees have clearly approved of the use of unencrypted communication,[187]a few committees have been more cautious.[188]

---

182 VT Advisory Ethics Op. 2010-6, above at note 60.
183 Mass. Op. 12-03, above at note 131.
184 NH Advisory Op. #2012-13/4, available at http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp
185 CA Formal Op. No. 2010-179, above at note 145.
186 Fla. Bar Prof'l Ethics Comm., Op. 12-3 (2013), available at http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+12-3?opendocument. *See also* VT Advisory Ethics Op. 2010-06 (noting that cloud storage may not be appropriate where client property is particularly sensitive, such as when trade secrets are involved).
187 Alaska Bar Association Ethics Committee, Opinion 98-2 (1998); Ethics Op. No. 2001-2 (2001); District of Columbia Bar Legal Ethics Committee, Opinion 281 (1998) & 302 (2000); Florida Ethics Op. No. 00-4 (2000); Illinois State Bar Association Committee on Professional Ethics, Opinion 96-10 (1997); 1999 Formal Advisory Opinion Board's unofficial answer to Georgia Bar's Computer Law Section; Hawaii Ethics Op. No. 40 (2001); Kentucky Bar Association, Ethics Opinion KBA E-403 (1998); Massachusetts Bar Association Ethics Opinion, Opinion 00-1; Professional Ethics Commission, Opinion 195 (2008); New York State Bar Association Committee on Professional Ethics, Opinion 709 (1998); Association of the Bar of the City of NY, Formal Opinion 1998-2 (1998); State Bar Association of North Dakota Ethics Committee, Opinion 97-09 (1997); Supreme Court of Ohio Board of Commissioners on Grievances and Discipline, Advisory Opinion 99-2 (2000); Supreme Court of Ohio Board of Commissioners on Grievances and Discipline, Advisory Opinion 99-2 (2000); Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Opinion 97-130 (1997); South Carolina Bar Ethics Advisory

In 1999, the ABA Standing Committee on Ethics and Professional Responsibility opined that unencrypted e-mail sent over the Internet are not unethical because "transmission affords a reasonable expectation of privacy from a technological and legal standpoint . . . [However, a] lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation."[189] This was confirmed in the more recent Opinion #11-459.[190]

The jurisdictions that have approved of the use of non encrypted communications[191]have always indicated at least one caveat that can be summarized as "unless special circumstances reasonably require encryption". For example, the Maine Professional Ethics Commission addressed email encryption and opined, as a general proposition, that sending unencrypted email is not an ethical violation unless reasonable judgment dependent on the circumstances dictates otherwise.[192] The commission added

> as general guidance attorneys should discuss with clients their preferred method(s) of communication and follow the client's wishes, should consider the degree of confidentiality of particular information in determining appropriate means to send it, and should take reasonable precautions to make sure that the address is correct and properly targeted.[193]

The Maine opinion represents the majority view, particularly among the most recent email encryption opinions, and aligns with the ABA's stance.[194]

The California opinion[195] -- which is one of the five jurisdictions that are more cautious about the ethical propriety of unencrypted emails--[196] expressed a slightly modified view, albeit where the inquiry pertained to transmission of client information from a public wireless connection.

> [E]ncrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous.[197]

Committee, Opinion 97-08 (1997); Utah State Bar, Ethics Advisory Opinion Committee, No. 00-01 (2000); Vermont Bar Association Committee on Professional Responsibility, Opinion 97-5; Virginia Ethics Op. No 1791 (2003).

188 Among the opinions, more uncertain about this principle are Arizona, California, Iowa, Missouri, and North Carolina. State Bar of Arizona, Committee on Rules of Professional Conduct, Opinion 97-04 (1997); The State Bar Of California Standing Committee On Professional Responsibility And Conduct, Formal Opinion No. 2010-179; Iowa Supreme Court Board of Professional Ethics and Conduct, Opinion 97-1 (1997); Advisory Committee of the Missouri Supreme Court, Opinion 990007; N.C. Ethics Op. 215.

189 ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (Protecting the Confidentiality of Unencrypted E-Mail), available at http://cryptome.org/jya/fo99-413.htm#http://www.abanet.org/cpr/fo99-413.html

190 ABA Comm. on Ethics & Prof'l Responsibility, Formal Op 11-459 (Duty to Protect the Confidentiality of E-mail Communications with One's Client) available at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf

191 See above at note 187.

192 Bd. of Overseers of the Bar State of ME, Op. #195 (2008), available at http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=63338&v=article

193 *Id.*

194 ABA Formal Op. 99-413 (1999), above at note 189.

195 The State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179, available at http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3D&tabid=836

196 See above at note 188.

197 *Id.*

In addition, even if New York is one of the jurisdictions that have unequivocally approved of unencrypted emails, the New York opinion curtailed its conclusion that sending unencrypted email is not an ethical violation under normal circumstance by adding

> in circumstances in which a lawyer is on notice…that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature…the lawyer *must* select a more secure means of communication than unencrypted Internet e-mail.[198]

PART III --EUROPEAN APPROACH V. AMERICAN APPROACH TO PRIVACY: THE INTERSECTION OF CLOUD COMPUTING WITH DATA PROTECTION DIRECTIVE IN EUROPE

> This paper generally treats "privacy" and "data protection" as synonyms. In fact, they are not:
>
> Although data protection and privacy share certain features and goals, and are frequently used as synonyms, they are not identical. . . .Although clearly engrained in privacy protection, data protection does not necessarily raise privacy issues. Contrary to privacy rules, data protection rules are not prohibitive: they organise and control the way personal data are processed. Data protection is therefore both more narrow and more broad than privacy … [199]

We could say that "data protection" is an evolution of the right of privacy, extending the protection of the right of privacy of the individual to "data" about the individual. So, probably, it would be more correct to speak at least of "data privacy." However, the term "privacy" as catchy synonym for "data protection" has so entered into common usage that we adopt that expression.

The right of privacy in the U.S. is immediately associated with Warren and Brandeis' well-known 1890 article, *The Right to Privacy*.[200]Warren and Brandeis defined the right of privacy as "the right to be let alone" from external interferences.[201] The right of privacy is well developed in the U.S. The protection goes from the Fourth Amendment's right to be free from unwarranted searches and seizures from the government, to the protection against the intrusion of solitude and seclusion into private quarters and

---

198 New York State Bar Association Committee on Professional Ethics, Opinion 709 (1998), available at http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6317&TEMPLATE=/CM/ContentDisplay.cfm(emphasis added).

199 See DLA Piper, *EU Study - Legal Analysis of a Single Market for the Informational Society, New Rules for a New Age? A. The Future of Online privacy and Data Protection*, available on the Internet.

200 Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 Harv.L.Rev. 193 (1890) available at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

201

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons … and [for] the evil of invasion of privacy by the newspapers …. [T]he question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration. Of the desirability -- indeed of the necessity -- of some such protection, there can, it is believed, be no doubt. *Id.*

against the public disclosure of private facts, from the right not to be cast in "false light," to the protection against the appropriation of a person's name and likeliness. Even abortion in the U.S. is seen as a privacy right.[202] It is not farfetched to say that the right of privacy (with the exclusion of data protection), being the product of the Anglo-Saxon culture, is more developed in the U.S. than in other parts of the world. Not so developed in the U.S. is "data protection": while intensively regulated in Europe, in the U.S., save special instances,[203]data protection is generally limited to "data breach" laws.[204]

To be sure, cloud computing has the potential to conflict with both privacy in the Warren's and Brandeis's sense and with "data privacy". However, our paper will be limited to the second. So that, in this paper, the expression "privacy law" or "privacy" should be intended as data protection.

A. EUROPEAN VS. AMERICAN APPROACH TO DATA PROTECTION

Before discussing the European approach to cloud computing and the type of issues that a law firm must consider in choosing the cloud, to the benefit of non-European readers we will briefly discuss the basic principles of European data protection law.

The approach to privacy in Europe and in the US is quite different. One commentator said that the divergence in attitude has philosophical reasons: "the reason that privacy laws in Europe and the U.S. are so different springs from a basic divergence in attitude: Europeans reserve their deepest distrust for corporations, while Americans are far more concerned about their government invading their privacy."[205] The European deeper concern about data protection can also be grounded in history.[206] Whether or not the bases of the different attitudes are still valid,[207] the result is that, while Europe has a quite

---

202 *Roe v. Wade,* 410 U.S. 113 (1973).

203 See below, Part III(A).

204 See above in Part I(B)(4).

205 Bob Sullivan, *La "difference" is stark in EU, U.S. Privacy Laws*" available at http://www.nbcnews.com/id/15221111/#.UmGYUxYTvjA

206

> Some privacy experts argue that heightened European sensitivity to privacy stems from the horror of the Holocaust, when the Nazis used public and church records to identify Jews to be rounded up and sent to concentration camps. But others say the historical difference dates back much further – to Dumas, or even earlier, and the notion that governments are charged with actively protecting people. *Id.*

207 Europeans are starting to be distrustful of governmental surveillance, too. *See, e.g.,* the recent *CCBE Statement on mass electronic surveillance by government bodies* (including of European lawyers' data),
available at http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_14142013_CCBE_Sta1_1382086457.pdf

> On 1st July, 2013, the CCBE issued a statement … on governmental practices involving mass data mining for purpose of surveillance, in which the CCBE expressed its deep concern that a core value of the profession, professional secrecy, known in some countries as legal professional privilege, is at serious risk. . . .
> The CCBE statement was based on reports of mass violation of the human rights to private life and personal data, being carried out on a systematic scale by governmental agencies of leading Western powers, including Member States of the European Union [. . .]
> [T]he CCBE is of the opinion that the greatest threats to clients' trust in professional secrecy can be traced back to two sources: a) lack of trust in state bodies with secret investigatory powers … ; and b) an objective lack of technical means at the disposal of law firms to secure effectively professional secrecy. […]

comprehensive general data protection law based on Directive EU 95/46,[208] the U.S. does not have a general law on data protection:

> On a federal level, the United States maintains a sectoral approach towards data protection legislation where certain industries are covered and others are not. At a state level, most states have enacted some form of privacy legislation"[209]

The most important "federal data protection laws" are "the Health Insurance Portability and Accountability Act (HIPAA), the Fair and Accurate Credit Transaction Act (FACTA), and the Children's Online Privacy Protection Act (COPPA)."[210]HIPAA applies to "individually identifiable health data"[211] and "defines who can have access to health information . . . [which usually is limited to] . . . health care professionals who are using it for treatment and care coordination purposes."[212] FACTA "protect[s] consumers' credit information from the risks related to data theft."[213] COPPA

> protect[s] the privacy of children under the age of 13 . . .[and] imposes [for example] an obligation on the operators of . . . websites [visited by children] to publish privacy policies specifying whether or not personal information is being collected, how this information is being used, as well as the disclosure practices of the operators of the websites.[214]

"At a state level, most states have enacted some form of privacy legislation."[215] However, as we have mentioned above, these laws tend to regulate more data breach than data processing.[216]"Beyond that, US data privacy laws are a patchwork."[217]

In Europe data protection law is much more organic and comprehensive and "[p]rivacy is a human right."[218]The protection and processing of personal data in Europe is currently governed by Directive

---

> [In conclusion] [t]he CCBE, therefore, urges the EU institutions to create the necessary legal and technological framework in order to remedy the current situation as regards electronic mass surveillance and to safeguard professional secrecy, which is a right of all EU citizens and one of the core values of the legal profession.

[208] Data Protection Directive 1995/46/EC and e-Privacy Directive 2002/58/EC.

[209] Daniel V. Dimov, *Differences between the privacy laws in the EU and the US*, available at http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] See Part I(B)(4) above.

[217] Constance Gustke, *Which Countries are better at protecting privacy?*, available at http://www.bbc.com/capital/story/20130625-your-private-data-is-showing

> American retailers, for example, are largely self-policing. And enforcement is limited to a company's own privacy policy. Consumers who want to do business with a particular retailer usually must agree to its privacy policies — in many cases there is no option to opt-out except to not buy from a merchant. The US Federal Trade Commission, charged with protecting American consumers, only steps in when a company doesn't keep its self-developed privacy promise. Some states have their own privacy laws, separate to the federal statutes. Massachusetts and California are the best at protecting consumer data among states, said Daren Orzechowski, a partner in White & Case's Intellectual Property Group.
>
> But otherwise, consumers must scrutinize the policies posted by retailers and decide what privacy they are willing to give up making a purchase.

[218] Bob Sullivan, *La "difference" is stark in EU, U.S. Privacy Laws*", above at note 205.

95/46/EC[219] dealing generally with the protection of individuals with regard to the processing of their personal data ("Data Protection Directive").

In January 2012, the European Commission made a proposal for a new legal framework for the protection of personal data[220]consisting actually of two legislative proposals: (i) a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Regulation Proposal"),[221] and (ii) a Directive on the protection of individuals with regard to the processing of personal data by governmental authorities for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[222] Relevant to this paper is only the Data Protection Regulation Proposal. Among the differences from the current Data Protection Directive, Article 3 of the Regulation Proposal sets a wider territorial scope. Once approved, the European privacy would cover the processing of personal data by (i) a natural or legal person controlling or processing personal data established in the European Union (respectively the controller or the processor), *and* (ii) a controller *not* established in the Union, if the processing activities are related to: (a) the offering of services to data subjects in the EU; or (b) the monitoring of their behavior.

Because the Data Protection Regulation has not been approved yet,[223]the legislative privacy framework for the cloud is currently still the Data Protection Directive (and its member states' transposition). We notice that among the benefits of the future Data Protection Regulation is the fact that because it will be a "regulation" and not a "directive", it will provide a uniform privacy regulation in the 28 member states,[224] unlike the present situation where individual state variations exist.

We cannot go into details of the several national laws of transposition of Data Protection Directive;[225] we can only say that there are differences among the national privacy laws, some of the national privacy laws being more restrictive than others. For the purpose of this paper, however, we must disregard these differences and only refer to European privacy law as if every EU member had transposed the Data Protection Directive exactly in the same way or as if the Directive was actually a regulation.

With this fiction in mind – and only as a primer for non-European readers --we will say that the

---

219 Article 1, Directive 95/46/EC, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

220 Communication COM (2012) 9 final available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF

221 Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

222 COM(2012) 10 final, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

223 As for the status of the legislative procedure, on March 12, 2014, the European Parliament approved in its plenary section the Commission's data protection reform proposal. (information available on http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en). The next step is the adoption of the proposal by the EU Council. It is difficult to estimate an exact time of approval or to foresee possible amendments that could be implemented as a result of the co-decision procedure enacted at a European legislative level.

224 Article 288 of the Treaty on the Functioning of the European Union. Unlike a directive that is binding only "as to the result to be achieved" but leaves "to the national authorities the choice of form and methods", a regulation is "binding in its entirety and directly applicable in all Member States."

225 See *Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data*, available at http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm

basic principles of European data protection are the following:[226] (1) the processing of personal data is subject to transparency, legitimate purpose, and proportionality;[227] (2) in every EU member there is a supervisory authority (independent agency) that monitors the data protection in that country, gives advice to the government on privacy, issues opinions binding on data controllers, and engages in legal proceedings when the authority finds violations;[228] (3) personal data can be transferred outside the European Union (the Directive talks about "third countries") only if "the third country in question ensures an adequate level of protection."[229]

The U.S. and the EU have agreed to a "safe harbor" scheme (approved by the EU in 2000). American companies can elect to comply with this scheme to demonstrate an "adequate level of protection".[230]To be clear: the participation to the Safe Harbor would not be enough for a US entity that is inside the scope of the Data Protection Directive (as identified by Article 4 of Data Protection Directive),[231] for having an establishment in Europe or for using equipment located in Europe to process data.[232]Indeed, the Safe Harbor framework, which was studied by "the U.S. Department of Commerce in consultation with the European Commission,"[233]only deals with the finding of "adequacy" for the transfer of data from Europe to the U.S.

> All 28 Member States of the European Union will be bound by the European Commission's finding of "adequacy";
> Participating organizations will be deemed to provide "adequate" privacy protection;
> Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted;

---

226 We are aware that the following is a very simplistic approach but because of the comparative view of this paper, we expect some readers not to be aware of the features of European privacy law. For this reason we deemed necessary to list the basic principles of it.

227 Personal data can be processed only if the data subject is informed of the processing (transparency), if the processing is done with a specified, expressed legitimate purpose (legitimate purpose) and in the limits of it (proportionality).

228 Article 28 of the Data Protection Directive.

229 Article 25 of the Data Protection Directive. To be sure, the publication of data on a website which is accessed by third country users, is not a transfer. See ECJ JUDGMENT 6. 11. 2003 — CASE C-101/01:

> The reply to the fifth question must therefore be that there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.

In Ireland, for example, "Section 11 of the Data Protection Acts 1988 and 2003 specify conditions that must be met before personal data may be transferred to third countries" (Transfers Abroad, available at http://www.dataprotection.ie/docs/Transfers-Abroad/37.htm)

230 See *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, available at http://export.gov/safeharbor/:

> While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework and this website to provide the information an organization would need to evaluate – and then join – the U.S.-EU Safe Harbor program.

231 See below at note 242.

232 *See* Donald C. Dowling, Jr., *International Data Protection and Privacy Law* (Aug. 2009), http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf (noting that the safe harbor permits in certain instances data to flow from European countries to U.S. entities, but does not impact data processing that occurs in Europe).

233 *U.S.-EU Safe Harbor Overview*, available at http://export.gov/safeharbor/eu/eg_main_018476.asp

> Claims brought by EU citizens against U.S. organizations will be heard, subject to limited exceptions, in the U.S.; and
> Compliance requirements are streamlined and cost-effective, which should particularly benefit small and medium enterprises.[234]

Participation in the framework is totally voluntary, but once a company has decided to opt-in, it must state this participation publicly in its privacy policy and is bound by that.[235]

> To qualify for the U.S.-EU Safe Harbor program, an organization can (1) join a self-regulatory privacy program that adheres to the U.S.-EU Safe Harbor Framework's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the U.S.-EU Safe Harbor Framework.

To be part of the program, "[o]rganizations must comply with the seven Safe Harbor Privacy Principles"[236] which are (i) Notice; (ii) Choice; (iii) Onward Transfer (Transfers to Third Parties); (iv) Access; (v) Security; (vi) Data integrity; (vii) Enforcement.[237]

As noted above, the Safe Harbor is a scheme that only applies to the flow of data from Europe to the US and does not apply to US entities that are subject to the Data Protection Directive. We have said above that Article 3 of the Data Protection Regulation Proposal will enlarge the scope of EU privacy law. To be sure, the scope of the future Regulation will be connected to the subject of protection (i.e., the data subjects): if an organization offers service to EU residents or monitors their behavior, then EU privacy law will apply.[238] The changes in the scope are determined by the acknowledgment that new technologies have simply destroyed geographical boundaries.[239]These changes will greatly impact American organizations (including law firms and cloud providers).

It should be noted that also the current Directive has an extraterritorial effect. According to Article 4, each member state shall apply its national privacy law if

---

234 *Id.*

235

> Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the U.S.-EU Safe Harbor Framework's requirements, which includes elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the Safe Harbor Privacy Principles. *Id.*

236 *Id.*

237

> Enforcement of the U.S.-EU Safe Harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's U.S.-EU Safe Harbor commitments the force of law vis a vis that organization. *Id.*

238 Article 3 of Data Protection Regulation Proposal.

239 Proposal for a Regulation of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, Explanatory Memorandum 6, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf,

> Personal data are transferred across national boundaries, both internal and external borders, at rapidly increasing rates. In addition, there are practical challenges to enforcing data protection legislation and a need for co-operation between Member States and their authorities, which needs to be organised at EU level to ensure unity of application of Union law. The EU is also best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries. *Id.*

> (a) the processing is carried out[240] in the context of the activities of an establishment[241] of the controller on the territory of the Member state; … (c) the controller is not established on Community territory and, for purposes of processing personal data makes *use of equipment*, automated or otherwise, situated on the territory of the said Member state, unless such equipment is used only for purposes of transit through the territory of the Community.[242]

An opinion by the Article 29 Working Party (the organism whose main task is providing expert opinion from the member state level to the Commission on questions of data protection)[243] has applied this Article to cloud computing: the Data Protection Directive "applies in every case where personal data are being processed as a result of the use of cloud computing services."[244]

Why this "extraterritorial" approach? The recital to the Data Protection Directive states "the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals").[245]

B. THE INTERTWINEMENT BETWEEN EUROPEAN DATA PROTECTION LAW AND THE CLOUD

1. Overview: law firm as "controller" and cloud provider as "processor" of data

The Data Protection Directive[246] has two definitions that are relevant for the cloud: "data controller" and "data processor." For American readers not familiar with these concepts, the "controller" is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[247]The "processor" is the "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."[248]

The Data Protection Directive imposes the major responsibilities on the controller. For example Article 17 (Security of Processing) provides that

> the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration,

---

240 See Article 29 Data Protection Working Party, Opinion 8/2010 on Applicable Law ("Opinion 8/2010") available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf, p. 12 and the following, for examples of "processing of personal data".

241 "The decisive element to qualify an establishment under the Directive is the effective and real exercise of activities in the context of which personal data are processed". Opinion 8/2010, p. 11.

242 Data Protection Directive, Art. 4. (emphasis added).

243 See http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/tasks-art-29_en.pdf

244 Opinion 05/2012, page 6. See also Opinion 8/2010, above at note 240.

245 Data Protection Directive Recital 20

> Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.

246 See above at note 219.

247 Data Protection Directive, Art. 2(d).

248 *Id.* Art. 2(e).

> unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[249]

However, certain duties are also imposed on the processor. Article 16 imposes a duty of confidentiality on both the controller and the processor.[250] In addition, the Directive requires the processor to conform to obligations imposed by its contract with the controller.[251]

Based on these provisions, if a law firm decides to use the cloud, the law firm is the data controller (because the law firm is the one that "determines the purposes and means of the processing of personal data" under Article 2(d) of the Data Protection Directive). The role of the cloud provider depends on whether we are talking about a private cloud or a public cloud. In a private cloud, the provider is only data processor because under Article 2(e) it is the one that "processes personal data on behalf of the controller" and does not "determines the purposes and means of the processing of personal data" (Article 2(d)). In a public cloud, however, in which the cloud provider has a greater role and control overdata, the provider may also be treated as a controller.[252] These conclusions find support in two opinions by the Article 29 Data Protection Working Party. In Opinion 1/2010 the Working Party opined on the interaction between "controller and "processor".[253] In Opinion 05/2012 on Cloud Computing[254]the Working Party applied those concepts to the cloud environment.

Whatever is the role of the cloud provider (be it a processor or also a controller itself), the cloud client (in our case, the law firm) is a controller for the data that it entrusts to the cloud provider and therefore it is fully liable for any breach of privacy law committed by the provider.

But before proceeding with our discussion, we want to clarify three important points. First clarification: while in every case of data processing, you have a "controller," you do not always have a "processor":

> the existence of … [the processor] depends on a decision taken by the controller, who can decide either to process data within his organization or to delegate all or part of the processing activities to an external organization. Two basic conditions for qualifying as processor are on

---

[249] *Id.* Art. 17(1).

[250] *Id.* Art. 16 (Confidentiality of Processing)

> Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

[251] I*d.* Art. 17(3).

[252] Prof. Romain Perray & Prof. Celia Zolynski at the conference "Getting around the cloud(s) – "Technical and legal issues on Cloud services"', November 30, 2013 organized by the Scuola Superiore Sant'Anna, Pisa.

[253] Opinion 1/2010 *on the Concepts of "Controller" and "Processor,"* adopted on 16 February 2010 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf ("Opinion 1/2010").

[254] Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

> the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf.[255]

Second clarification: we stated above that in private cloud situation, the cloud provider is a processor only, while in a public cloud situation, the provider can also be a controller. This is certainly the case for social networks. However, this is not the case where a public cloud does not have autonomy in the choice of the purpose and means of the processing. Opinion 5/2012 of the Article 29 Working Party confirms that it is the

> [t]he cloud client [that] determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. The cloud client therefore acts as a data controller."[256]

The Working Party also opines that the general principle for cloud providers is that they are processors:

> When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor.[257]

At least one scholar has expressed his support for this view:

> First of all, even if the cloud provider maintains a degree of autonomy and decision-making, tasks and specifications are clearly and strictly defined by the user through the contract . . . Secondly, only the user is directly empowered by the data subject to process the data and the cloud provider receives the information to be processed in the interest of the user. Finally, the typical arrangements of cloud computing services … give broad significance to service performances and service level agreement (SLA), binding the parties in such a way that it is not possible to consider them as two autonomous controllers. For these reasons we must conclude that the cloud client takes on the role of controller and the cloud provider takes the role of processor. Confirmation also comes from the fact that the services offered by cloud providers are only part of the processing which users carry out. In addition, cloud providers do not have the specific or exclusive competences necessary to play a dominant role in managing the data, which entails a high degree of autonomy.[258]

Third clarification: Article 17(3) of the Data Protection Directive imposes on the controller (in our case, a law firm) a duty to enter into a quite detailed contract with the processor (in our case, the cloud

---

> The concept of data controller and its interaction with the concept of data processor play a crucial role in the application of Directive 95/46/EC, since they determine who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can operate.

[255] Opinion 1/2010.

> [The Working Party] recognises the difficulties in applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility.

[256] Opinion 05/2012, at 7.

[257] *Id.*

[258] Alessandro Mantelero*, Cloud Computing, Trans-Border Data Flows And The European Directive 95/46/Ec: Applicable Law And Task Distribution* , European Journal of Law and Technology, vol.3, No. 2 at 1-2 (2012) available at http://ejlt.org//article/view/96,

provider), which, among other requirements, must state that the "processor shall act only on instructions from the controller."[259]As a result of this provision a law firm must carefully evaluate the cloud service agreements with prospective providers. Opinion 05/2012 refers to two possible model forms that controllers could use to contract with cloud providers.[260] However, the Opinion also acknowledges that it is difficult for cloud clients to negotiate terms with providers, which are often big entities with significant contractual power.[261] This circumstance, however, far from diminishing the responsibility of a law firm in the choice of a cloud provider, results in the necessity for law firms to use due diligence to identify cloud providers compliant with the Directive.

2. Peculiar case: When the cloud provider is also the controller of data

While cloud providers will normally be classified as processors rather than controllers, depending on the nature of the provider's activities, a provider may be treated as a controller. In Opinion 1/2010 the Working Party states that "the role of processor does not stem from the nature of an actor processing personal data but from its concrete activities in a specific context and with regard to specific sets of data or operations."[262]

Opinion 1/2010 offers several examples of possible situations in which a processor becomes a controller. In Example No. 16: Internet service providers of hosting services, the Opinion specifies:

> [T]he lawfulness of the processor's data processing activity is determined by the mandate given by the controller. A processor that goes beyond its mandate and acquires a relevant

---

[259] Article 17(3)-(4):

> 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
> - the processor shall act only on instructions from the controller,
> - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
>
> 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

[260] Opinion 05/2012, at 10:

> A possible model of assurances that can be used to clarify the duties and obligations of processors when they subcontract data processing was first introduced by the Commission Decision of 5 February 2010 on the standard contractual clauses for the transfer of personal data to processors established in third countries. [. . .] A similar solution regarding assurances in the course of sub-processing has been proposed recently by the Commission in the proposal for a General Data Protection Regulation. The acts of a processor must be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that, among other requirements, the processor shall enlist another processor only with the prior permission of the controller (Article 26(2) of the proposal).

[261] Opinion 05/2012, at. 23:

> The Article 29 Working party considers that . . . [the Commission proposal for a data Protection Regulation, still to be approved] goes in the right direction to remedy the unbalance that is often a feature in the cloud computing environment, where the client (especially if it is a SME) may find it difficult to exercise the full control required by data protection legislation on how the provider delivers the requested services.

[262] Opinion 01/2010, at 25 (emphasis in original).

> role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor.[263]

In the same way, if the cloud provider takes significant decisions in relation to the data entrusted to it, then it becomes a controller and assumes the relevant responsibilities. Opinion 5/2012 gives some guidance on this issue:

> [S]ome criteria can be used for assessing controllership of the processing. As a matter of fact, there may be situations in which a provider of cloud services may be considered either as a joint controller or as a controller in their own right depending on concrete circumstances. For instance, this could be the case where the provider processes data for its own purposes.[264]

The opinions recognize, however, that providers may have certain degree of discretion in technical choices *without* becoming controllers. Opinion 01/2010 when dealing with Internet service providers of hosting services states:

> [D]elegation may still imply a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.[265]

As we will discuss in Part IV, the selection of a reliable cloud provider is one of the tasks that should be performed as part of due diligence necessary before using cloud services. The analysis of the interplay of responsibilities (controller/processor) must be part of this process.[266]A careful analysis of the concrete situation is particularly important because there might be cases in which the division of roles between the cloud client and the cloud provider is not clearly defined. A law firm using the cloud should consider that there might be situations in which, under a European privacy law perspective, the cloud provider is a joint controller or a controller of a different processing, depending on specific circumstances. For instance, as said, a provider could become a controller where it processes data for its own purposes, for example, to plan some market strategies, or to provide further services. To make another example,

---

[263] *Id.*

[264] Opinion 5/2012, at 8.

[265] *Id.*

[266] Some cloud providers think that their users do not go deeply enough into the privacy consequence of using a cloud instead of keeping the data in-house, and do not perform a sufficient due diligence on "where, how, why, when and whom the data is processed." They simply do not stop to consider that the "reasonability" of this evaluation "firmly resides with the client." *See, e.g.*, Ospero (International Cloud Service Provider with headquarters in London), *A cloud provider's view: sharing privacy responsibilities with clients*, available at http://www.ospero.com/component/k2/item/374-a-cloud-provider-s-view-sharing-privacy-responsibilities-with-clients:

> The client is, in legal terms, the data controller; . . .This is in itself an onerous responsibility and one which I truly do not think most companies fully understand…
> A cloud service provider is legally defined as a "data processor." It is our responsibility to provide digital and physical layers of protection and security to protect the data assets of our clients. Service providers should also provide a comprehensive Service Level Agreement (SLA) which should encompass how support requests are prioritised and handled.
> Service providers should also furnish their clients with details of audits achieved and also details of penetration and breach testing that should be regularly performed by recognised third party organisations… Both parties must implement strict policies and procedures on how, who, when and why people are allowed to access data and data processing capability. The biggest threat to an organisation's data generally comes from within organisations and it is usually human-related.

consider the difference between a cloud service that allows users to insert their billing time (cloud is mere processor) versus a cloud service that autonomously processes the data inserted to provide further billing services or time and expense tracking.[267] Law firms should also consider that cloud computing is increasingly a composite service for which there might be more than one cloud provider or in which the cloud provider hires subcontractors to render services to the client.[268]The Data Protection Directive impliedly authorizes processors to hire subcontractors,[269] and Opinion 1/2010 considers cases of cooperation among several processors.[270]However, even if allowed, delegation of activities triggers some obligations: when a cloud provider chooses to hire a subcontractor, under Article 17 of the Data Protection Directive,[271] the relationship between the subcontractor and the controller must be governed by a contract:

> All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider.[272]

Making sure that this contract between cloud provider and subcontractors exists, is part of the due diligence that a law firm should make before transferring its data to the cloud.

3. Issues of applicable law for cloud computing

It is no surprise that European law firms are subject to EU privacy law; and that their use of the cloud must be consistent with privacy law. In fact, the CCBE has prepared guidelines for law firms on the use of the cloud which discuss in detail the privacy implications of the use of the cloud.[273]

But are American-based law firms subject to EU privacy law? The question actually is twofold: (1) Can a nonEuropean-based law firm become subject to EU privacy *per se*, i.e. independently from the use of a cloud located in Europe?; (2) Does an American firm become subject to EU privacy by virtue of the use of a European cloud?

---

[267] Example based on WP 29, opinion 8/2010 on applicable law, above at note 240, at 21.

[268] Opinion 05/2012:

> Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. If processors subcontract services out to sub- processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC.

[269] See Article 2(f) definition of "third party" and Article 16 (Confidentiality of processing).

[270] Opinion 01/2010, at 27:

> Nothing in the Directive prevents that on account of organisational requirements, several entities may be designated as processors or (sub)processors also by subdividing the relevant tasks. However, all of them are to abide by the instructions given by the controller in carrying out the processing.

[271] See above at note 259.

[272] Opinion 05/2012, at 9.

[273] See above at note 41. For a more detailed discussion of the CCBE Guidelines on Cloud see part IV of this paper.

As we said above, currently EU privacy law applies[274]if the processing is done by a controller with an establishment in the EU or, in case of a controller not established in the EU, if the controller "for purposes of processing personal data makes use of equipment . . . situated [in the EU] . . . unless such equipment is used only for purposes of transit through the . . .[EU]."[275] If an American law firm has an office in the EU, it obviously has an *establishment* that makes it subject to the European privacy. However, even those law firms that do *not* have an office in Europe, can become subject to EU privacy, if they make "use of equipment" in the EU.[276] In 2002 the Data Protection Working Party issued a working document on "determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites,"[277]which states:

> The Working Party considers that the concept of "making use" presupposes two elements: some kind of activity undertaken by the controller and the intention of the controller to process personal data. This implies that not any "use" of "equipment" within the European Union leads to the application of the Directive.[278]

The Working Party lists several examples of "equipment" that trigger the application of European privacy law: cookies, JavaScript, banners and other similar applications are considered as "equipment" pursuant to Article 4(1)(c) of Data Protection Directive.[279] The Working Party opined that a "case-by-case assessment is needed whereby the way in which the equipment is actually used to collect and process

---

274 Recall that the Data Protection Regulation Proposal will enlarge the scope of EU privacy protection. See Part III(A) above.

275 Article 4 - National law applicable

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
>
> 2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

276 We will not deal here with the issue of what particular national privacy law the nonresident controller would be subject to. However, it is worth remembering that, until the Data Protection Regulation is approved, there are in the EU twenty-eight potentially different privacy laws.

277 Article 29, Data Protection Working Party, Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Web Sites, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf ("Working Document")

278 *Id.* at 9. In addition, the application of the Directive is rendered uncertain because of the "difference between the word used in the English version of Article 4(1)c 'equipment', and the word used in other language versions of Article 4(1)c, which are more akin to the English word 'means'". Opinion 8/2010 on applicable law, at 20:

> The terminology used in other language versions of Article 4 (1) c is also consistent with the wording of Article 2(d) defining the controller: the person who decides about the purposes and the "means" of the processing. In view of these considerations, the Working Party understands the word "equipment" as "means". It also notes that according to the Directive this could be "automated or otherwise."

279 Working Document, above at note 277, at 10.

personal data is assessed."[280]The Working Party recognized the possibility that the collection of personal data through the computers of users, as for example in the case of cookies or Javascript banners, triggers the application of Article 4(1)c and thus the application of EU data protection law to service providers established in third countries.[281]

It is worth mentioning that pursuant to Article 4.2 of the Data Protection Directive, a controller not established on European territory but that makes use of equipment located on a member state should designate a representative established on the territory of the member state.[282]

When applying these principles to cloud computing, a significant issue arises: where is a cloud "located"? One author has described the problem as follows:

> Cloud architectures pose several challenges with regard to data management. Firstly, it is difficult to determine who has the effective control over the data and assumes the related liability, in a model where ITC companies provide cloud services to their clients, but at the same time define the levels and the features of the services and have a relevant control over the software and hardware resources. Secondly, the trans-national nature of cloud computing structures amplifies the issue concerning the applicable law, due to the continuous fast flow of data between the different data centers located in various parts of the globe.[283]

Also Opinion 8/2010 has acknowledged the problem of "locating" the cloud:

> Cloud computing, where personal data are processed and stored on servers in several places around the world, is a complex example of the application of the provisions of the Directive. The exact place where data are located is not always known and it can change in time, but this is not decisive to identify the law applicable.[284]

The Opinion suggests that location of the data is not of fundamental importance because application of the Directive turns on the controller, not the location of the cloud:

> It is sufficient that the controller carries out processing in the context of an establishment within the EU, or that relevant means is located on EU territory to trigger the application of EU law, as provided in Article 4(1)c of the Directive. The first decisive step will be to identify who is the controller, and which activities take place at which level.[285]

The issue remains, however, for those controllers (for example, an American-based law firm) that are *not* located in Europe (not having an establishment there and not using any equipment there) but that do use a cloud that *might* use equipment located in Europe.

---

[280] Opinion 8/2010, above at 240.
[281] *Id.* at 21. The Data Protection Working Party went on to discuss whether the use of outsourcing of data as opposed to direct acquisition would trigger the application of EU privacy law. This issue, which is central to the use of cloud computing, is discussed in more detail below.
[282] Article 25 Data Protection Proposal, under certain conditions, still obliges controllers not established in the UE - but subjected to the Regulation's territorial scope - to designate a representative in the Union.
[283] Alessandro Mantelero, *Cloud Computing, Trans-Border Data Flows And The European Directive 95/46/Ec: Applicable Law And Task Distribution*, above at note 258, at 1-2.
[284] Opinion 8/2010, above at note 240, at 21 (Example No. 8; Cloud Computing).
[285] *Id.*

To recap: (i) when an American-based law firm has an office in Europe, EU privacy law generally applies because it has an "establishment" pursuant to Article 4(1)(a)), unless (but this is unlikely) this office does not have anything to do with the processing of data, neither directly or indirectly through the use of a cloud.[286](ii) When an American-based law firm directly uses equipment (example cookies) in the EU, then the EU privacy law applies. The same is true in case in which an American-based law firm processes data through a European-based cloud. But what if an all-American law firm (without an office in the EU and with no direct use of equipment in the EU), uses a *non-European* cloud provider, which unbeknown to the client, uses equipment located in the EU? *Technically*, if the cloud provider uses European equipment, the firm *should be subject* to EU privacy law, whether or not the law firm knows of this European equipment (non-EU based entity "makes use of equipment, automated or otherwise, situated on the territory [of EU].")[287] However, according to the Working Group, the term "equipment" should be defined as "means",[288]which would imply a *positive decision* (as opposed to an incidental consequence) of the controller to undertake the processing of personal data in Europe. Opinion 8/2010 acknowledges that a strict interpretation of "making use of equipment" creates an issue for outsourcing of activities, as is the case with cloud computing:

> There is a question whether outsourcing activities, notably by processors, carried out in the EU/EEA territory on behalf of controllers established outside EEA may be considered as "equipment". The broad interpretation advocated above leads to a positive answer . . .

For the Data Protection Working Group, this is not always desirable:

> However, account should be taken of the sometimes undesirable consequences of such an interpretation . . . if controllers established in different countries over the world have their data processed in a Member State of the EU, where the database and the processor are located, those controllers will have to comply with the data protection law of that Member State.[289]

To solve this issue, the Working Group advocates for a "case-by-case assessment . . . whereby the way in which the equipment is actually used to collect and process personal data is assessed."

Despite this Working Group's acknowledgement of undesirability,[290] the problem remains: an American-based law firm without an office in Europe, is subject to EU privacy law because of the use of a

---

[286] Consider that, as Opinion 8/2010 makes clear in another context, to be relevant

> the establishment of the controller … [must be] involved in activities implying the processing of personal data, taking into consideration its degree of involvement in the processing activities, the nature of the activities and the need to guarantee effective data protection. Opinion 8/2010, above at note 240 , at 2.

[287] Article 4(1)(c).

[288] See above at note 278.

[289] Opinion 8/2010, above at note 240, at 20.

[290] See *id.* at. 31

> Additional criteria should apply when the controller is established outside the EU, with a view to ensuring that a sufficient connection exists with EU territory, and to avoid EU territory being used to conduct illegal data processing activities by controllers established in third countries. *Id.*

For the Data Protection Working Party these additional criteria should be the following: (1) the "targeting" criteria, meaning that EU privacy applies when the controller "targets" EU residents; (2) the "means" criteria, which would apply in case of data about non EU residents by

cloud provider that uses equipment in Europe to process the data on behalf of the American firm.[291] The problem is particularly thorny because, as we said above, where a cloud is "located", is not always clear: a law firm might hire an American cloud provider and without being aware that this provider has servers or other "equipment" in Europe, which would trigger the application of EU privacy.

Two final points: as discussed above, there might be cases in which a "processor" becomes a "controller" (assuming the relevant responsibilities) by virtue of the performing of activities that are typical of a "controller." In case of a cloud, Opinion 8/2010 opines that a cloud provider that is offering a service of "synchronisation of appointments and contacts" would be performing an activity that is typical of a controller and that would subject it to the EU privacy "if the cloud service provider uses means in the EU."[292]

Lastly, we want to mention a very recent decision of the European Court of Justice that significantly broadens the extraterritoriality application of the EU privacy law.

On May 13, 2014, the European Court of Justice (ECJ) in the Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) — Case C 131-12, issued a preliminary ruling (i.e. an interpretation decision) on referral of the Spanish Audiencia Nacional (National High Court). The ECJ found that a search engine's retrieval and listing of information to the benefit of the searcher is "processing of personal data" if the information retrieved are personal data and that the search engine is a controller. The ECJ also finds that a search engine is subject to EU privacy law if it established a branch or subsidiary to sell advertising spaces orientating "its activity towards the inhabitants of that Member State" and that, by doing so, the search engine was carrying out "processing of personal data … in the context of the

---

"*controllers having no link with EU*" if "where there is a relevant infrastructure in the EU, connected with the processing of information." See *id.* at 31-32.

However, this is not the law but only suggestions by the Data Protection Working Party on what the law should be.

[291] See *id.* at 21 (Example No. 8: Cloud Computing)

> The user of the cloud service is a data controller: for instance, a company uses an agenda service on-line to organise meetings with clients. If the company uses the service in the context of the activities of its establishment in the EU, EU law will be applicable to this processing of data via the agenda on-line on the basis of Article 4(1)a. The company should make sure that the service provides for adequate data protection safeguards, notably with regard to the security of personal data stored on the cloud. It will also have to inform its clients of the purpose and conditions of use of their data. *Id.*

[292]

> The cloud service provider can also in some circumstances be a data controller: this would be the case when it provides for an agenda on-line where private parties can upload all their personal appointments and it offers added value services such as synchronisation of appointments and contacts. If the cloud service provider uses means in the EU, it will be subject to EU data protection law on the basis of Article 4(1)c. As demonstrated below, the application of the Directive would not be triggered by means used for transit purposes only, but it would be triggered by more specific equipment e.g. if the service uses calculating facilities, runs java scripts or installs cookies with the purpose of storing and retrieving personal data of users. The cloud service provider will then have to provide users with information on the way data are being processed, stored, possibly accessed by third parties, and to guarantee appropriate security measures to protect the information. *Id.* at 21 (Example No. 8: Cloud Computing).

activities of an establishment of the controller on the territory of a Member State".[293] As it is clear, the "minimum contacts" (to use an American concept) between an Internet provider and Europe that justify the application of EU privacy law to the provider are less and less. It would not be surprising to see the same type of reasoning being applied to cloud providers.

4. Some specific cases of application of national privacy law

Until here we have reasoned generally about the consequence of the EU privacy law for an American-based firm as if the Data Protection Directive would apply directly in the 28 EU members,[294] which is not the case. Every EU member has implemented the Data Protection Directive in a slightly different way and has its own Data Protection Authority, whose approach on applicability of the EU privacy law controls in that jurisdiction. We cannot discuss the approaches of all the member countries, but we want to give some examples, which we take from Italy. Alessandro Mantelero reports three recent significant decisions of the "Garante per La Protezione dei Dati Personali," (Italian Data Protection Authority) ("DPA"):[295]

(1) in a decision of May 24, 2006 (doc. web n. 1299063)concerning university researchers' personal data, the DPA held that measures could not be taken against data privacy violations consisting of the publication of personal data of Italian residents when the publication was on a *website hosted abroad* (in that case the website was hosted in the United States) since the "violations have been performed through websites to which the [Italian] Code on Data Protection was not applicable, because located in third countries outside of the EU."[296]

(2) in the Heinz S.p.A. decision of November 4, 2010 (doc. web n. 1771838) – issued on request of an Italian group that wanted to know if a certain prospective project was consistent with Italian privacy law – the DPA found that the following was compliant with Italian privacy law:

> The [employees'] feedbacks which are given electronically are analyzed through an outsourcing company (which is located in the U.S. and has opted for the "Safe Harbor") which has been appointed as processor pursuant to Article 29 of [Italian] Code [of privacy]; the data subjects [i.e., employees] have given their informed consent to the arrangement, also to the transfer of their data abroad.[297]

---

[293] See more about this case at http://www.technethics.com/right-to-disappear-fromsearch-results. Full ECJ's decision available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=243691

[294] This will be the case once the Data Protection Regulation is approved. *See* above at note 223.

[295] *See* Alessandro Mantelero, *Cloud Computing, Trans-Border Data Flows and The European Directive 95/46/Ec: Applicable Law And Task Distribution*, above at note 258.

[296] The full text of opinion is available (in Italian) at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1299063

[297] The full text of opinion is available (in Italian) at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1771838

(3) in the Google Street View decision of October 15, 2010(doc. web n. 1759972), the DPA[298]dealt with the receipt of "several complaints from individuals that do not wish to be displayed on the images posted online by Google Inc.in connection with its StreetView service."The description of the operation by Google was the following:

> the images are captured by special cameras on cars and automatically sent to a server held by Google Inc. in the USA, where they are processed and posted on the relevant website; in some cases, the images also contain personal data such as pictures of individuals or car plates.[299]

The DPA held that "[t]he processing falls within the scope of application of the Italian Data Protection Code, as it is performed by means of equipment located in Italy (see section 5 of legislative decree no. 196/2003 …)[300]"and that Google's "current arrangements[301]for informing data subjects are insufficient."[302] The DPA acknowledges that "providing information to every single data subject whose image is captured by the cameras would entail a disproportionate effort" but lists other arrangements that Google must implement within 30 days.[303]

PART IV -- PRACTICAL TIPS FOR A LAW FIRM OPTING FOR CLOUD COMPUTING

In this Part IV we offer some practical tips to law firms considering using the cloud, based on the benefits and risks (Part I of the paper) the ethics opinions (Part II), and the privacy issues (Part III.) In Part IV(A) we consider the steps that a purely American law firm should go through to choose the cloud.[304] In Part IV(B) we discuss a checklist that the CCBE has issued for European firms (CCBE Guidelines on Cloud.)[305] In Part IV(C) we reconcile the two approaches.

---

[298] The full text of opinion is available (in Italian) at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1759972 (some excerpts in English available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1759984)

[299] *Id.*

[300] *Id.* The DPA goes on to say that, while "there is no need for the data subjects' consent regarding image acquisition, since the images in question are captured in public places", "the processing of personal data … must be compliant with fairness, lawfulness, proportionality and necessity principles." In addition:

> Data subjects have the right to object to the processing of their data even if they can be identified only indirectly, also following the "blanking" or "blurring" performed by Google Inc. on captured images Data subjects have also the right to be adequately informed on the processing (section 13 of the DP Code) since they must be in a position to decide whether to subject themselves to the "capturing" of their images; *Id.*

[301] *Id.*

> [L]ist of the cities/towns where Google cars are expected to be around, posted a few hours beforehand plus a short general information notice on Google's website

[302] *Id.*

[303] *Id.* Google must appoint a representative established in Italy pursuant Section 5 of Italian privacy code, must publish three days in advance in its website a detail account of where the pictures will be taken (complete route), must inform the data subjects through radio ads and ads on local newspapers, must equip its Streetview cars with conspicuous stickers clarifying that pictures are being taken. *See, id.*

[304] We thank Richard Callison, Esq., contract attorney for Crystal & Giannoni-Crystal, LLC, for the initial research on this topic.

[305] We thank Avv. Federica Romanelli, Foreign Legal Consultant in New York, for the initial research on this topic.

A. WHAT A U.S. LAW FIRM SHOULD DO TO USE THE CLOUD

How should law firms go about deciding whether to use a cloud computing service? We have prepared a five-step process for firms to consider using in making this decision. The process includes a list of questions that law firms should ask as part of the due diligence process. Of course, no checklist can cover all situations, however, we believe that lawyers need more than the general standard to use "reasonable care". Lawyers should be aware that they have a personal obligation to keep abreast of technological developments as applied to their practice.[306] If they are unable or unwilling to do so personally, they should employ experts to assist them in these matters.

A warning on the use of this checklist: we have elaborated it based on the Model Rules of Professional Conduct, ethics opinions of the several American jurisdictions, other documents cited in this paper, and general principles of legal ethics. It is meant to be for consideration only and should not be relied upon without consulting the law of the specific jurisdiction or jurisdictions in which lawyers practice. In particular, if lawyers practice in a jurisdiction that has issued guidance for lawyers' use of cloud computing (if, for example, the bar ethics committee of that jurisdiction has issued an ethics opinion on the cloud), then lawyers should carefully consult that guidance to make sure that our checklist covers all of their jurisdiction's requirements.

1. Identify the type or types of cloud services that the firm is considering using and conduct a cost/benefit analysis

As discussed in Part I, all or almost all of the services that small to medium-sized firms will consider fall in the category of "Software as Service (SaaS)."[307]Very large firms may consider using Platform as Service (PaaS) or Infrastructure as Service (IaaS), but those uses of the cloud will be beyond the capability or interest of almost all firms.[308] These services will generally be through public clouds,[309]unless the firm is quite large.[310]

---

306 *See* Comment [8] to Model Rule 1.1.

307 *See New York City Bar's Report on Cloud*, above at note 53, at 4-5.

308 *Id.* at 6.

309 According to the *2012 ABA Legal Technology Survey Report*,

> the largest demographic segment of law firms to move into the cloud this past year consisted of solo and small firms. They are migrating into the stratosphere at just over twice the rate of large firms. In the past year, the number of solo lawyers who reported having used cloud-based software increased six percent (to 29%); use among lawyers in small firms of 2–9 lawyers also increased 6 percent (to 26%). Compare that to lawyers in firms of 100 or more, where there has been no increase in cloud use from the previous year, and total usage is just 11 percent.
>
> You are probably curious about what all those lawyers are using in the cloud. Based on the referenced survey, more than 46 percent are using Google Docs, more than 16 percent are using practice management (Clio 12% and Rocket Matter 5%+), and more than eight percent are using data storage (iCloud 4%+ and Dropbox 3%+). Ellen Freedman, *Moving to the Cloud*, available at http://www.americanbar.org/publications/gpsolo_ereport/2013/april_2013/moving_to_the_cloud.html

310

> Large firms definitely have the advantage in remote access options without having to move to the cloud. They can economically create a VPN (virtual private network), create a private cloud, or deploy their own Citrix-server environment so

We have discussed in Part I that within the category of SaaS, a wide variety of services exist. The two that are most familiar to lawyers are legal research services like Lexis or Westlaw and email services like Google. As we said inPart I(A),beyond these basic offerings, a wide variety of SaaS can be found, including, accounting, case management, ediscovery, file and data storage, file transfer, time keeping and billing, and word processing.[311]

For each SaaS that a firm is considering adopting, a cost/benefit analysis should be done to determine whether it makes economic sense for the firm to adopt the service in question. In our opinion the analysis is clarified if the economic costs and benefits are evaluated *before* moving to a second step of evaluating the ethical and legal risks; if a service does not make economic sense, evaluation and management of risk becomes unnecessary.

A number of components of the cost/benefit analysis can be quantified, but some will be subject to a more judgmental determination. Take the use of a legal research service. Lexis and Westlaw provide various levels of service at different costs. Once the level of service is chosen, the analysis can turn to the benefits. A research service dramatically reduces the need for a library of books, the cost of the space associated with the library, the cost of updates, and staff time devoted to managing the library. In addition, the service reduces the need for lawyers to travel to libraries for books not contained in their home library and increases productivity by ease of use and greater availability. Other SaaS can be the subject of a similar cost/benefit analysis. Email is probably the most ubiquitous cloud service used by lawyers. Why? While it may be unclear whether many SaaS pass a cost/benefit test, email passes with flying colors. The cost of email is minimal and may even be nonexistent, while the benefits in terms of efficiency, speed, and cost reduction through saving of postage, paper, and staff time are great.

In Part I we also discussed another benefit of the cloud: it allows lawyers to stay abreast of technology and so comply with their duty of competence. As we said, the cloud usually allows lawyers to use the latest technologies, the software updates are automatic and so are the backups.[312]

2. Identify the risks associated with the particular cloud service

Lawyers have various ethical obligations that are associated with the use of cloud services and should identify the risks associated with the particular cloud service that could result in ethical violations,

---

that remote users can log in from most devices and get the same experience as being at the office, all without giving up many of the bells and whistles one must do when using cloud-based software. *Id.*

311 See Part I(A).

312 See Part I(B)(1).

legal liability, damage to the reputation of the firm, or all of these. Especially important, as seen in Part I of this paper, are the following:[313]

>Competency under ABA Model Rule 1.1. As amended in 2012, Comment 8 provides that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

>Communication to client of material information under Rule 1.4, which would include the duty to inform a client of a security breach regarding the client's data.

>Confidentiality regarding client information requiring the lawyer to use reasonable care to protect against the unauthorized disclosure of client information, as set forth in ABA Model Rule 1.6, Comment 18.

>Maintenance, preservation, and delivery of client property on termination under ABA Model Rules 1.15 and 1.16.

>Supervision of the work of both lawyers and nonlawyers, including contractors providing cloud services under Model Rule 5.3.

As discussed in Part I, violation of these ethical obligations could be the basis of disciplinary action against a lawyer. In addition, lawyers face the possibility of lawsuits for violation of duties to their clients with regard to the use of cloud services. These lawsuits could be based on professional negligence, breach of fiduciary duty, or violation of applicable statutory or regulatory provisions. In addition, improper handling of data even if it does not result in disciplinary or legal action can be extremely damaging to the reputation of a firm, resulting in the loss of substantial business.

In addition to ethical risks, as we have discussed in Part I, there are other risks associated with the cloud: legal risks,[314] security of data risks (i.e. violation of personal information protection laws),[315] and technical risks, both external and internal risks.[316]

3. Steps that can (and should) be taken to eliminate or minimize the risk associated with use cloud services

Ethics opinions and rules of ethics seem to be in general agreement that lawyers are not strictly liable if the unauthorized use or disclosure of client data occurs.[317] Instead, the standard is one of reasonable care. For example, Comment 18 to Rule 1.6 states: "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not

313 *New York City Bar's Report on Cloud*, above at note 53, at 12-21. See also Part I of this paper where we discuss more deeply the several ethical risks of cloud computing.
314 Part I (B)(3).
315 Part I(B)(4).
316 Part I(B)(5).
317 See Part II above.

constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure." What follows is a list of questions/areas of inquiry that firms should consider using to exercise reasonable care with regard to the risks associated with use of cloud providers:[318]

(1) What is the general reputation of the provider for quality and security? Has the provider been recommended by bar associations or otherwise received recommendations or certifications from reputable businesses or organizations?

(2) What are the measures that the provider takes to protect the security of the data from unauthorized access?

(3) What are the industry standard measures of security?

(4) Is the provider compliant with such standard measures?

(5) What does the Service Agreement say with regard to steps that the provider will take if there is a security breach to mitigate the breach?[319]

(6) What does the Service Agreement state with regard to notification of a security breach?

(7) Does the firm have in place internal policies and procedures that require any lawyer or nonlawyer employee who learns about a security breach to notify firm management?

(8) What does the Service Agreement provide with regard to notification to the firm if the provider receives a subpoena or other request for information?[320]

(9) What does the Service Agreement provide with regard to ownership of the data, use of the data by the provider, and licensing of the data by the provider?[321] The agreement must provide that the law firm or the client, as the case may be, is the owner of the data. Use of subcontractors by cloud provider should only be allowed with the express written consent of the law firm or client as the case may be. In case the Service agreement has a non negotiable clause that allows the outsourcing of data, the law firm will have to obtain client consent to use that provider. If the Service Agreement allows the provider to use the data, the nature of the use must be evaluated to determine if it complies with lawyer's professional obligations and with the protection of attorney client privilege; such use will require client consent as well, unless it is for the benefit of the client-lawyer relationship (e.g., those services that allow the uploading of a lawyer's time in a case and automatically generate an invoice).

(10) What does the Service Agreement provide with regard to interruption of service due to provider maintenance?

---

[318] This list of questions draws upon but adds to guidelines suggested by the *New York City Bar's Report on Cloud*, above at note 53.

[319] This at a minimum means that the service agreement must require the provider promptly to notify the law firm of any data breach so that the law firm can comply with its ethical obligation to communicate with its clients under ABA Model Rule 1.4 and its legal obligations under data security laws, see Part I(B)(3).

[320] See the discussion of the issue of management of subpoenas or orders by cloud providers in Part I(B)(3).

[321] These questions are important under Model Rule Model Rule 1.15 (Safekeeping Property). See above at Part I(B)(2).

(11) What does the Service Agreement provide with regard to access and recovery of data if the provider suffers an interruption of service either temporary or permanent?

(12) What methods of backup of data does the provider have?

(13) Does the firm have in place methods of backup and retrieval of data if the data cannot be obtained from the provider?

(14) Where are the servers of the provider located? If the servers are located in other countries where the applicable law governing data security differs from that of the US, does that law apply to the data in question? If so, what steps, if any, can the firm and the provider take to avoid the storage of your data of those countries? The location of the servers is particularly important for the application of European privacy law.[322] Appropriate provisions could be included in the Service Agreement to address this issue.[323] In case the law firm knows that the cloud servers are located abroad, prudence suggests that law firm should inform the client of this fact and maybe obtain client consent (law firm can do this by inserting a technology policy clause inside its retainer agreement).

(15) What does the Service Agreement provide about return of data on termination of service?[324]

(16) Has the firm adopted appropriate policies and procedures, including training of lawyers and nonlawyers regarding use of cloud services and use of devices associated with those services?

These questions can be summarized into a shorter due diligence standard that combines the external and internal risks: in deciding whether to use a cloud service a firm should do due diligence on the provider, review the Service Agreement for compliance with the lawyer's professional obligations (competency, confidentiality, communication, protection of property, and supervision of nonlawyer providers), and institute internal policies and procedures with regard to the use of the service to comply with the firm's professional obligations.

4. Making the decision

The next step in the process is the decision. The firm must decide whether to employ the service based on its cost/benefit analysis, identification of the relevant risks, and steps that it can take to minimize the identifiable risks. The decision is in part objective – the direct economic costs and benefits associated with the service. However, a significant part of the decision will be subjective based on anticipated benefits that are difficult to measure, such as projected increases in productivity, the likelihood of

[322] See above Part III(B)(3).

[323] American law firms could, for example, try to obtain from the providers a list of all the locations in which the provider maintains servers or a declaration that their data will not be stored in servers located in the European community. If this is the case, an American law firm may become subject to the EU privacy law of the EU country in which the server are located (*see* Article 4 of the data Protection Directive). If the provider has servers located in the EU, then the provider should certify its compliance with EU privacy law.

[324] This question is again triggered by Model Rule Model Rule 1.15 (Safekeeping Property). See above at Part(B)(2).

occurrence of a risk factor, and the consequence to the firm and its clients if one of the identifiable risks materializes. Notice that these difficult-to-measure benefits are such not only for the law firm but also for clients (for example: an increase in productivity will also mean that law firm will be able to answer a client's questions more quickly).

If the firm decides that it wishes to use a particular service, but is unable to eliminate a risk, it would be at the very least prudent to identify this risk in the firm's engagement agreement so that affected clients can either consent or express their objections; the data of a client who object could be handled without using the cloud service if possible.

An example of such a disclosed risk might be a provision in the cloud service agreement that relieves the provider of liability for any unauthorized disclosure of data. For most providers this clause is nonnegotiable. If a law firm is going to proceed with such a provider, the law firm might consider disclosing this situation to its clients in order to make their consent to the use of cloud providers as informed as it could be.[325] The same might be true for other nonnegotiable provisions in the provider's service agreement or its T&C. One way for a law firm to disclose such limitations to its clients without a tedious listing of specific provider's conditions -- which might itself be incomplete -- is by disclosing the name of the provider with a link to the provider's T&C in the law firm's engagement agreement with its clients.

5. Post decision obligations

The cloud computing inquiry should not be static. As technology and the law related to technology evolve, a lawyer's understanding should keep pace. A lawyer should: (i) Periodically review current data security measures, both those of providers and internally; (ii) stay abreast of best practices in data security and implement them, and (iii) keep informed of changes in the law, particularly as they relate to privileges and waivers thereof.

B. CCBE GUIDELINES ON THE USE OF CLOUD COMPUTING SERVICES BY LAWYERS

As discussed above, the processing of personal data in Europe involves detailed regulations. A European law firm choosing to use the cloud certainly must consider the privacy implication of this

[325] The issue of whether cloud providers are liable to the data subjects in either contract or tort is beyond the scope of this article. The existence of particular breach law (see above Part I(B)(3) should also be considered. However, in making the decision about disclosure to the client of the cloud provider's disclaimer of liability, we note the following considerations: (1) lawyers using the cloud remain responsible to their clients for compliance with their ethical obligations. The standard is reasonableness, not strict liability; (2) Even if a cloud provider may legally disclaim liability for a security breach, lawyers cannot do so. *See* ABA Model Rule 1.8(h)(1); (3) It may be sufficient to disclose to clients the T&C of the provider, which contain limitation of liability, without specific reference to the limitation of liability clause.

choice.[326] The same type of analysis must be done also by an American-based law firm with offices in Europe.[327]

However, privacy risk is not the only factor that a European law firm choosing to use cloud computing should consider. The CCBE - aware of the risks that may arise for a law firm employing cloud services - issued guidelines to help lawyers correctly address the use of such services, both under a privacy perspective and an ethical perspective.[328]

The CCBE lists the following as the most direct concern for lawyers using cloud computing services:

1. Issues relating to professional secrecy and data protection

The CCBE suggests lawyers might need to (i) clarify reliability and the safety of the cloud where clients' data are stored; (ii) define the extent of client's consent necessary to store or transmit confidential information; (iii) establish security measures to prevent risks of unauthorized access. The concerns are very similar to those that an American law firm faces when choosing to use the cloud;[329] in the same way the CCBE's advices are similar to those given in the ethics opinions of the several U.S. jurisdictions.[330]

2. Issues relating to extraterritoriality

Issues relating to extraterritoriality should be a concern for European lawyers wishing to use the cloud, especially where the data processing would take place on servers in countries with less effective legal protection mechanisms for electronically stored information than Europe, or where non-EU national authorities might have access to data. This concern is "typically European" and comes from the EU privacy law. We do not find an equivalent in the ethics opinions of the several U.S. jurisdictions.[331]

3. Issues relating to contracts with cloud computing service providers

Issues relating to contracts with cloud computing service providers should also be a concern for lawyers. For example, there might be (i) unclear policies regarding ownership of stored data, notification of security breaches, duration of data storage, data destruction; (ii) no adequate back up of data; (iii) insufficient data encryption; (iv) issues in the event that a law firm terminates its relationship with the cloud

326 See Part III of this paper.
327 In this Part when we talk about "European lawyers" or "European law firms" we also include "American-based law firms with offices in Europe" or to "American lawyers practicing in Europe".
328 CCBE's Guidelines on Cloud, above at note 41. CCBE's Guidelines on Cloud is available at http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf
329 See Part I(B) of this paper.
330 See Part II of this paper.
331 See Part II of this paper.

computing provider or when the provider changes or goes out of business. These issues are substantially the same as the due diligence cloud agreement analysis that an American law firm should do.

4. What a law firm should do to solve those issues according to the CCBE

In order to avoid such issues, the CCBE advises lawyers seeking to deploy cloud computing in their firms to consider the following:

- *Data protection laws and professional secrecy principles*

> Lawyers should verify whether they are allowed under the rules of their home state bar or law society to store data outside their law firm and, if so, ensure that the cloud computing service provider is not subject to a jurisdiction with long-arm legislation obliging them to hand over European lawyers' data stored on a cloud server to, as the case might be, non-EU national authorities. Lawyers may wish to consider whether, in view of these concerns, it might not in any given case, be more appropriate to use a cloud service provider established within the EEA and (wherever situated) so far as practicable not subject to such long-arm jurisdiction.[332]

-*Preliminary examination of cloud computing services*

---

[332] CCBE's Guidelines on Cloud at 4.

Media around the globe have been talking a lot about collection of data by non-EU authorities recently. The reference is obviously to the now famous (but unknown until the Washington Post and The Guardian revealed its existence on June 2013) "Prism" program, which

> is a system the NSA uses to gain access to the private communications of users of nine popular Internet services. We know that access is governed by Section 702 of the Foreign Intelligence Surveillance Act, which was enacted in 2008. Timothy Lee, *Here's everything we know about PRISM to date*, June 12 2013, available at http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/
>
> Under Section 702 of the amendments, the NSA was empowered to compel technology companies to turn over information about their users. A special court oversees the program, renewing it once a year. Barton Gellman, Ashkan Soltani, And Andrea Peterson, *How we know the NSA had access to internal Google and Yahoo cloud data,* November 4, 2013, available at *http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/*

In August 2013, the public learned that

> The National Security Agency is paying hundreds of millions of dollars a year to U.S. companies for clandestine access to their communications networks, filtering vast traffic flows for foreign targets in a process that also sweeps in large volumes of American telephone calls, e-mails and instant messages. Craig Timberg & Barton Gellman, *NSA paying U.S. companies for access to communications networks*, August 29, 2013, available at http://articles.washingtonpost.com/2013-08-29/world/41712151_1_nsa-national-security-agency-companies

The payment seems to be done

> to reimburse technology firms for complying with requests for user data, according to documents from former NSA contractor Edward Snowden shared with the Guardian newspaper. Report: NSA pays tech companies for data, August 24, 2013 available at http://www.foxnews.com/politics/2013/08/24/report-nsa-pays-tech-companies-for-data/
>
> It is estimated that the NSA's surveillance touches 1.6% of the entire data exchanged in the Internet ("Internet carries 1,826 Petabytes of information per day"). Out of this 1.6%, only 0.25% is actually selected for review. Imagine the Internet as a basketball court, NSA is looking only at a dime on the court. "The dime on the basketball court, as the NSA describes it, is still 29.21 petabytes of data a day. That means the NSA is "touching" more data than Google processes every day (a mere 20 petabytes)" Sean Gallagher, NSA "touches" more of Internet than Google http://arstechnica.com/information-technology/2013/08/the-1-6-percent-of-the-internet-that-nsa-touches-is-bigger-than-it-seems/, August 13, 2013.

A detailed analysis of the Prism system is beyond the scope of this paper. We simply wanted to make the point that the recommendation of the CCBE to lawyers to consider where the cloud provider stores their clients' data, in these days, is more current than ever.

The CCBE advises law firms to preliminarily understand which kind of service they need (for example, SaaS, IaaS, public or private cloud provider):

> Before contracting, a lawyer, as the end user of the cloud service, should verify:
> [a] the experience,
> [b] the reputation,
> [c] the specialisation,
> [d] the registered address and location of the cloud computing service provider.
> In addition, a separate verification of the following should be conducted:
> [a] the providers' solvency, reliability, ownership and capital adequacy,
> [b] any potential conflicts of interests,
> [c] risks of any misuse of the stored information,
> [d] exact localisation of the storing servers,
> [e] so far as practicable, the security both physical and electronic of the servers and the data centre in which they are located.[333]

- *Pre-evaluation of data sensitivity*

The CCBE advises that

> Any decision to store information on the cloud server should be necessarily accompanied by considerations on the type of information (employee data, criminal data, general legal archives, etc.) and the level of protection measures that should be adopted accordingly.[334]

This recommendation sounds like the recommendations of the several ethics opinion of the U.S. jurisdictions that we have discussed in Part II, where they caution law firms that entrusting of data to cloud might be unreasonable if the clients' data is particularly sensitive unless the lawyer takes special precautions.[335]

-*Assessment of security measures*

The CCBE opinion, like the Model Rules of Professional Conduct,[336]requires lawyers to be tech-savvy or hire experts to assist them in such matters. Before choosing a cloud, lawyers should always make a technical evaluation of the cloud provider.

> Assessment of cloud-service providers should involve evaluation of adopted technical, physical and organizational security measures in accordance with national and international IT-risk-management standards, such as ISCO 27001:2005 (security management) and ISO 9001 (quality management) Certificate issued by acknowledge IT auditors could also serve as a test criterion. (. . .) In general, a lawyer should always consider obtaining professional support and advice when selecting and monitoring cloud-service providers.[337]

---

[333] CCBE's Guidelines on Cloud at 6.
[334] CCBE's Guidelines on Cloud at 7.
[335] For example Vermont opinion, 2010-6, above at note 60, opines that

> Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

[336] See Comment [8] to Rule 1.1. ("Maintaining Competence") Model Rule of Professional Conduct, discussed in Part I of this paper.
[337] CCBE's Guidelines on Cloud at 7.

- *Comparing existing in-house IT infrastructure with cloud services*

The CCBE invites lawyers to think carefully on whether using the cloud is the best option for them. Law firms considering switching from in-house to cloud services should do a comparison to "decide if switching to a separate cloud service might reduce or increase risks."[338]

- *Assessment of ability to recover data in the event of the failure of the cloud service provider, failure of the law firm or contractual dispute between the provider and law firm*

The "tech-savviness" required by the CCBE is certainly not superficial:

> [I]n evaluating cloud service providers, a lawyer should assess his own vulnerability to adverse professional or regulatory consequences arising through such an unavailability of data. He should consider whether it is necessary to seek to negotiate appropriate contractual terms to ensure such continued availability, even in the event of a contractual dispute or failure of either the provider or his own law firm. He may also require to assess whether it is necessary also to seek technical means to overcome such unavailability.[339]

- *Contractual precautions*

The CCBE opinion invites lawyers to be particularly careful in analyzing the several terms of the cloud service agreement:

> It is important to at least consider the following aspects:
> [a] scope of service,
> [b] system availability,
> [c] deadlines for error corrections and removal of malfunctions,
> [d]contractual fines for non-performance and delays (if enforceable under the applicable national laws),
> [e] changes in service requirements,
> [f] service provider's obligation to system adaptations required due to regulatory or legislative amendments,
> [g] exclusion of engagement of sub-contractors without prior consent,
> [h] licenses, particularly assurance that the software used by the provider has been properly licensed to it,
> [i] ownership of data stored and exclusive right of access,
> [j] data protection agreements, in particular if and to the extent required by applicable national laws
> [k] security measures and responsibility,
> [l] non-disclosure obligations,
> [m] monitoring and reporting,
> [n]technical documentation, process documentation and user/system administrator documentation,
> [o] right to control and audit, including standard certifications,
> [p] back-up, disaster recovery contingency plan,

[338] *Id.*
[339] *Id.*

> [q] provision for Software-ESCROW in case of insolvency or business incapability of the cloud-service provider,
> [r] location of servers - national, EEA or outside of the EEA but with the European standards in respect to privacy and confidentiality,
> [s] insurance, guarantees, warranties, damages,
> [t] term, termination,
> [u] end of service and exit-management provisions, including on transmission and deletion of data,
> [v] mediation, conciliation and/or arbitration,
> [w] applicable law and jurisdiction.[340]

- *Contingencies*

The CCBE warns lawyers that, notwithstanding the utmost attention paid in the choice of the cloud, in reviewing its technical features and in analyzing the terms of the cloud service agreement, unexpected contingencies can occur. It is advisable to provide for these contingencies:

> Attention should always be paid to the fact that cloud-service availability depends on an uninterrupted network connection. The lawyer should consider whether it may be necessary to have an alternative or back-up means of connecting to the internet in the event that his primary connection should fail.[341]

- *Transparency*

Last but not least: communication with clients. We have discussed in Part I(B)(2) how important is the duty to communicate for American lawyers (but also – even if less spelled out – for European lawyers). The CCBE builds on this important duty and opines:

> In order to ensure transparency of legal services, a lawyer might consider informing his future clients that the law firm uses cloud computing services. This could be achieved by inserting the information into the general conditions of any legal-service agreement, subject to changes as negotiated with individual clients. This formula would enable the giving of more detailed information on cloud computing exclusively upon individual request. It should be noted that there may be certain jurisdictions where client consent is necessary.
>
> The insertion of information into the general conditions of a legal-service agreement would be particularly advisable in cases when a law firm uses services of a cloud provider with servers located in a different jurisdiction. In such a case, a lawyer might need to obtain informed consent from his client to store confidential data on such servers. Information on the cloud-service provider as well as legal standards on data protection, privacy law and professional privileges of lawyers in a country where the servers are located should be provided to the client.[342]

340 *Id.* at 8.
341 *Id.*
342 *Id.* at 9.

C. IS THERE A TENSION BETWEEN THE "ALL-AMERICAN" CHECKLIST AND THE EUROPEAN CHECKLIST?

1. A reconciliation

The practice of law is often multi-jurisdictional and stretches often from one continent to another. We want to deal here with the situation of those American law firms that have crossed the pond and now have offices also in Europe ("American-based International Law Firms", for short "ABIL"). ABIL, for having offices located on the two sides of the Atlantic, can benefit from the cloud even more than a local law firm. We will try here, step by step, to see if the checklist for an ABIL should be different and why.

The first step of the analysis that an ABIL should perform is the evaluation of the type of cloud that it needs. It is the first step of our checklist for American law firms[343] and it is also a recommended step in the CCBE's checklist.[344]For a more specific discussion of what this step means, you can read above Part IV(A)(1) and Part IV(B)(4) "Preliminary examination of cloud computing services", the substance of which is very similar.

The second step is the identification of risks associated with the particular cloud service, which could result in ethical violations, legal liability, or damage to the reputation of the firm, as we discussed in Part IV(A)(2). Among the ethical obligations that we mentioned are: confidentiality, competence, communication to client, maintenance, preservation, and delivery of client property on termination, and supervision of nonlawyers.[345] We have also mentioned that the adoption of cloud services can trigger legal liability,[346] can result in violation of safety breach laws,[347] and can generate external and internal risks (which, in turn, can result in disciplinary sanctions, actions in tort or contract or all of that).[348] Also the CCBE suggests that lawyers should analyze the risks associated with cloud computing. CCBE's analysis is less detailed in point of ethical obligations and more detailed in point of privacy concerns (which is understandable considering the importance of data privacy in Europe.) Indeed, the CCBE focuses on professional secrecy and data protection,[349] issues relating to extraterritoriality,[350] and issues relating to contracts with cloud computing service providers.[351] However, the CCBE's focus on professional secrecy and data protection should not be understood as a disregard of the need to consider other issues, such as

[343] See Part IV(A)(1) ("Identify the type or types of cloud services that the firm is considering using and conduct a cost/benefit analysis")
[344] See Part IV(B)(4) ("Preliminary examination of cloud computing services.")
[345] Part IV(A)(2).
[346] Part 1(A)(3).
[347] Part 1(A)(4).
[348] Part 1(A)(5).
[349] Part IV(B)(1).
[350] Part IV(B)(2).
[351] Part IV(B)(3).

communication and supervision, concepts that are somewhat more developed in the U.S. than in Europe.[352]

The third step for an ABIL is the implementation of cautionary measures to eliminate or minimize the risks they have identified. In broad terms, the American and European approaches seem similar in attempting to deal with identifiable risks. In addition, each approach can "learn" from the other. For example, American authorities recommend careful attention and review to the SLA.[353] The CCBE Guidelines, however, identify specific aspects of SLAs that should be reviewed by European firms.[354]

Assuming that the cloud service passes a cost/benefit analysis and a risk control analysis, the next step in the process is the decision, i.e. the firm must decide – based on the comparison of benefits and risks - if the use of the cloud is advisable. We said that this decision is in part objective (costs vs. benefits) and in part "subjective", i.e. based on anticipated benefits that are difficult to measure, like increase in productivity, likelihood of occurrence of risk factors, and consequences to the firm and its clients if one of the identifiable risks materializes.[355]All this is particularly true for an ABIL.[356] We have also said that if the firm decides to use a particular service, but is unable to eliminate a risk, it would be prudent to insert client consent in the firm's engagement agreement and to deal with objections and to handle the data of objecting clients without using the cloud service if possible.[357] This is also one of CCBE's advices: "a lawyer might consider informing his future clients that the law firm uses cloud computing services. This could be achieved by inserting the information into the general conditions of any legal-service agreement, subject to changes as negotiated with individual clients."[358] The CCBE specifies that the disclosure to clients is particularly "advisable in cases when a law firm uses services of a cloud provider with servers located in a different jurisdiction. In such a case, a lawyer might need to obtain informed consent from his client to store confidential data on such servers."[359]

Can the analysis of an ABIL be simplified by following only one checklist? It is actually possible. If you compare the CCBE Guidelines[360] with the guidelines that we have suggested for American lawyers,[361] you might notice that the CCBE Guidelines appear to contain *all the elements* that we have made for American lawyers, *with the addition of privacy*. Indeed, the CCBE Guidelines identify three areas of concern:

---

352 In this respect American and European firms can each draw on the areas of emphasis that their nationalities indicate to be of greatest concern to develop a more comprehensive checklist for reviewing cloud computing services.
353 Part II(B).
354 Part IV(B)(4) (*"Contractual precautions")*
355 Part IV(A)(4).
356 An ABIL may need the flexibility and convenience of cloud computing even more considering that its offices are scattered across two continents.
357Part IV(A)(4).
358 CCBE's Guidelines at 9.
359 *Id.*
360 See our analysis in Part IV(B).
361 See Part IV(A).

(1) professional secrecy and data protection, (2) extraterritoriality, and (3) contracts with cloud computing service providers. In short, the CCBE Guidelines suggest that lawyers should consider the following aspects:

- Data protection laws and professional secrecy;
- Preliminary analysis of cloud computing services;
- Pre-evaluation of data sensitivity;
- Assessment of security measures;
- Comparing existing in-house IT infrastructure with cloud services;
- Assessment of ability to recovery data in the event of failure of the cloud service provider, failure of the law firm, or contractual dispute between provider and law firm;
- Contractual precautions;
- Contingencies;
- Transparency.

Given the detail and depth of the Guidelines, could an ABIL use the CCBE Guidelines and be confident that it is also complying with the American standard of reasonable care? Put in another way: is there any due diligence step required of an American firm that would not find a substantially similar equivalent in the CCBE Guidelines? After reviewing the CCBE Guidelines and comparing them with American standards, we think that in general ABIL would be on a solid ethical ground in following the CCBE Guidelines, with a caveat and a possible qualification.

The caveat to the use of the CCBE Guidelines is that there are quite a number of US ethics opinions dealing with cloud computing services. These opinions vary in details. Before relying on the CCBE Guidelines an ABIL should consult the relevant opinions to check if there are any requirements in those opinions that should be added or might qualify the CCBE Guidelines.

The qualification to the use of the Guidelines is the CCBE Guidelines do not mention internal risks in using cloud computing services, i.e., the risk that a firm might fail to adopt and implement policies and procedures to carry out its due diligence obligations.[362] We do not think that the drafters of the CCBE Guidelines ignored this issue; it was probably simply beyond the scope of the Guidelines. Nonetheless, ABIL cannot ignore the need to adopt appropriate internal policies and procedures for dealing with cloud services. Just by way of example, an ABIL must address issues such as use of personal devices to access the firm cloud services, types of devices that may be used, procedures in case devices are lost, and procedures for disposal of devices.

The conclusion of our analysis and of the CCBE's analysis are very similar, even if the order of discussion is different. Nonetheless, the details of the analysis matter and, for example, evaluation of internal risks should not be omitted if an ABIL decides to follow the CCBE Guidelines. International firms

[362] See Part I(B)(A).

can and should learn from the standards developed in different jurisdictions to create a merged standard that incorporates the best of all.

The process should be similar to what happens when an international group make business in several jurisdictions – it must comply with the privacy requirements of the several jurisdictions but at the same time may wish to follow a unified policy all over the world. In this situation, which privacy law should the group follow? The natural answer is: the most restrictive. However, this is not the correct answer. What the group actually should do is to acquire a deeper knowledge of the law requirements of the several countries and to integrate them as much as possible (and only when not possible following the most restrictive). The bonus of this approach is that a comparative analysis of several laws often triggers ideas for improvement in procedures. We recommend that ABILs follow this approach, which is also the methodology that an all-American law firm using the cloud should do considering the rapid evolution of technology, as we discussed in Part IV(A)(5).

2. Two problems peculiar to ABIL: the respect of privacy laws and the secrecy obligation

While the checklists of a purely domestic law firm and an ABIL are very similar, two issues have a purely European component to which an ABIL must pay attention: (i) the steps necessary for the firm to comply with European data privacy law in using cloud services[363]and (ii)the application of secrecy obligation to members of the ABIL.

It is worth remembering that the CCBE cautions lawyers to comply both with privacy law and with their secrecy obligation when adopting a cloud service. The CCBE provides some indications on how to deal with these concerns,[364]which the CCBE recommends to tackle as initial steps of the analysis meaning probably that if lawyers' use of the cloud cannot comply with these aspects, any additional discussion is useless:

> As a general rule, data protection laws and professional secrecy principles should be taken into account by lawyers as a *primary step* when considering using cloud computing services.[365]

Professional secrecy is not governed by a unified EU law – it is rather governed by the several domestic laws of the jurisdiction in which lawyers are admitted to practice.[366]Professional secrecy is

[363] In our paper we are only dealing with American firms practicing in Europe, therefore we speak here only of EU privacy laws. Obviously an American based international firm doing business in other parts of the world should make a similar analysis with reference to privacy law where applicable (for example, if the firm operates in Argentina, it must comply with the Personal Data Protection Law No. 25,326, as restated by the Regulatory Decree No. 1558/2001). A similar analysis would be needed for other countries where the firm operates, but that is beyond the scope of this paper.

[364] See above Part IV(B)(1).

[365] CCBE Guidelines, above at note 328. Emphasis added.

[366] For a discussion of professional secrecy in Europe, *see* Nathan M. Crystal & Francesca Giannoni-Crystal, *Understanding Akzo Nobel: A Comparison of the Status of In-House Counsel, the Scope of the Attorney-Client Privilege, and Discovery in the U.S. and Europe*, Global Jurist: Vol. 11: Iss. 1 (Topics) (2011), Article 1, available at http://www.bepress.com/gj/vol11/iss1/1

somewhat different from the confidentiality obligation of American lawyers because the first is often coupled with a crime or a tort in the several European countries.[367] In addition, unlike in the U.S., lawyers' duty of secrecy generally cannot be waived by the client. Usually the duty of secrecy is coupled with the "professional privilege," which grants lawyers the right to refuse to testify or deliver documents to authorities concerning legal advice. (Often the term "professional privilege" is used to refer to both the privilege and the duty of secrecy.)[368] Even if the privilege is not identical to the duty of confidentiality in the US, the privilege does not render the use of the cloud more difficult for European lawyers than for the American.

We cannot analyze the details of the secrecy obligation here. Enough to say that, as for content, the secrecy obligation is similar to the American duty of confidentiality, but the exception do not seem to be

---

You can also read for example with reference to France, Emmanuèle Lutfalla Pierre-Paul Saulou, France in International Association of Defense Counsel: available at http://www.iadclaw.org/UserFiles/file/17_11_FRANCE.pdf:

> Under French law, "professional secrecy" is a principle of public policy included in the Criminal Code. According to this principle, certain professionals such as priests, lawyers or doctors may obtain confidential information from their congregation members, clients, or patients, which the law considers necessary for the exercise of their profession. In return, the law imposes on such professionals an unconditional and unqualified obligation not to disclose confidential information.
>
> Legal "professional secrecy" is a general and absolute principle that has no limitation in time. In contrast with the situation in many other countries, in France there are no exceptions whatsoever to this principle. Lawyers cannot breach their obligation of "professional secrecy" to either clients, authorities of any kind, or, more generally, to any person whomsoever.

[367] *See, e.g.,* Article 622 of Italian Criminal Code, Article 226-13 of French Criminal Code, Article 203 of German Criminal Code, and Article 199 of Spanish Code.

e.g.

> Article 226-13 of the French Code: "The disclosure of secret information by a person entrusted with such a secret, either because of his position or profession, or because of a temporary function or mission, is punished by one year's imprisonment and a fine of €15,000."
>
> Article 226-14 of the German Civil Code, Section 203 Violation of Private Secrets - (1) Whoever, without authorization, discloses a the secret of another, in particular, a secret which belongs to the realm of personal privacy or a business or trade secret, which was confided to, or otherwise made known to him in his capacity as a: . . . lawyer . . . shall be punished with imprisonment for not more than one year or a fine.

[368] See for example for Italy: In the Code of Criminal Procedure article 200 (list of professionals who can sue the privilege), article 256 (right to object to deliver of documents to public authorities), article 362 (right to object to answer to the Attorney general's office). In the Criminal Code: article 622 (revelation of secrecy). In the Code of Civil procedure: Article 249 (right to refuse to give testimony). For a more detailed discussion, see Mario Napoli, *Il Segreto Professionale dell'Avvocato in Italia: disciplina normative ed aspetti deontologici* (The professional secrecy of the Italian Lawyer: rules and ethics) available in Italian at http://www.ordineavvocatitorino.it/sites/default/files/documents/deontologia_segreto_professionale_avvocato_italia.pdf.

well defined and almost certainly not as extensive[369] as exceptions to the American duty (see Model Rule 1.6(b) and other exceptions in the Rules).[370]

The European Code of Conduct provides

> 2.3. Confidentiality
> 2.3.1.It is of the essence of a lawyer's function that the lawyer should be told by his or her client things which the client would not tell to others, and that the lawyer should be the recipient of other information on a basis of confidence. Without the certainty of confidentiality there cannot be trust. Confidentiality is therefore a primary and fundamental right and duty of the lawyer.
>
> The lawyer's obligation of confidentiality serves the interest of the administration of justice as well as the interest of the client. It is therefore entitled to special protection by the State.
>
> 2.3.2. A lawyer shall respect the confidentiality of all information that becomes known to the lawyer in the course of his or her professional activity.
>
> 2.3.3. The obligation of confidentiality is not limited in time.

Our discussion in Part I (B)(2) on cloud risks for confidentiality and in Part IV(A) on precautions can be useful also to comply with the duty of secrecy. The CCBE Guidelines also give practical advice to lawyers on how to deal with these risks.[371] As for the criminal aspect of violation of the duty of secrecy, because the crime of revelation of secrecy isin our best knowledge always *intentional,* it cannot be committed simply by negligent entrustment of data to a cloud provider if there is a security breach[372] or if a statute requires the provider to reveal the data.[373]

While the duty of secrecy should not concern an ABIL more than the American duty of confidentiality, privacy should. If an ABIL has offices in the EU, then it has an establishment in the EU[374] and must comply with EU privacy law (unless it does not process any data from the European office,

---

369 For Italy, see Pierluigi Perri, Riservatezza e Deontologia Professionale, available at http://www.ilcivilista.giuffre.it/psixsite/Ultimo%20fascicolo/2007/Dicembre%202007/SCENARI/Perri-2007_03_6.pdf
For France, notice that the duty of secrecy is defined as "absolute" and "of public order":

> Une obligation absolue et d'ordre public L'avocat doit garder confidentiel le contenu de ses discussions, de ses courriers avec ses clients ainsi que les informations dont il a eu connaissance au cours de ses échanges avec l'avocat de l'adversaire. Le secret couvre toutes les confidences que l'avocat a pu recevoir à raison de son état ou de sa profession dans le domaine du conseil ou de la défense devant les juridictions et ce quels qu'en soient les supports, matériels ou immatériels (papier, télécopie, voie électronique). Les correspondances entre avocats sont par nature confidentielles. Enfin, obligation absolue, le justiciable ne peut délivrer l'avocat du respect du secret professionnel. Déontologie de l'avocat, Ordre des Avocats de Paris, at http://avocatparis.org/votre-avocat/deontologie-de-lavocat.html

370 See, e.g., ABA Model Rule 3.3.
371 Part IV(B) (4)
372 For example, Article 622 of the Italian Criminal Code punished the "revelation" without cause of the professional secrecy or the use of it to the lawyer's own benefit. The violation must be intentional. Just for completeness, we add that no damage is required for the crime to occur.
373 For example, the French Civil Code Article 226-13 is not applicable to the cases where the law imposes or authorises the disclosure of the secret.
374 See Article 4 of the Data Protection Directive. See for a wider discussion above in Part III(B)(1).

which is unrealistic).[375]Even in the absence of a European office, the ABIL is still subject to privacy law if it processes data through equipment located in Europe,[376] Even minimal use of equipment counts (e.g., use of cookies in firm's website to monitor users' behavior). This is true under the current Data Protection Directive but will change under the proposed Data Protection Regulation.[377] Once the Regulation is passed, the ABIL will be subject to European privacy "if the processing activities are related to: (a) the offering of services to data subjects in the EU; or (b) the monitoring of their behavior."[378] The existence of a European office or the location of equipment in Europe will not be necessary: if an American firm targets the European market, it will be subject to EU privacy law. Until the Data Protection Regulation is passed, an ABIL must evaluate the data privacy laws enacted of the several EU countries in which the firm has an office or in which it uses instrumentalities to process data.[379]Passage of the Regulation should make application of EU privacy law to ABILs clearer. ABILs will be subject to the Directive if they have European clients. In addition, the Regulation will provide a uniform set of rules across the EU.

Does the location of the provider matter? We have already discussed this in Part III(B)(3) but it is worth repeating it here. If a EU based law firm or an ABIL hires a EU based provider, then EU privacy law clearly applies. The Article 29 Working Party in Opinion 05/2012 stated:

> Article 4.1.c)[Directive on data Protection] refers to how data protection legislation applies to controllers who are not established in the EEA but use automated or non-automated equipment located in the territory of the Member State, except where these are used only for purposes of transit. This means that if a cloud client is established outside the EEA, but commissions a cloud provider located in the EEA, then the provider exports the data protection legislation to the client.[380]

But suppose a EU based law firm or a ABIL hires a US based cloud provider. Does the EU privacy law apply?

The CCBE has cautioned EU based firms against using cloud providers located outside the EU:

> Particularly, lawyers should verify whether they are allowed under the rules of their home state bar or law society to store data outside their law firm and, if so, ensure that the cloud computing service provider is not subject to a jurisdiction with long-arm legislation obliging them to hand over European lawyers' data stored on a cloud server to, as the case might be, non-EU national authorities. Lawyers may wish to consider whether, in view of these concerns, it might not in any given case, *be more appropriate to use a cloud service provider established within the EEA* and (wherever situated) so far as practicable not subject to such long-arm jurisdiction.[381]

---

375 The firm, for its European offices, will be subject to the European privacy laws of the various countries in which it has offices.
376 See Article 4 of the of Data Protection Directive Part III(B)(1)
377 Article 3 of Data Protection Regulation Proposal, above at Part III(A)
378 *Id.*
379 For discussion of the benefits of the adoption of a EU regulation see Part III(A).
380 Opinion 05/2012 at 7.
381 For a discussion, see CCBE, above at note 328 (emphasis added).

While the CCBE does *not* state that the use of a non-EU based cloud is unethical for a law firm, it warns lawyers that they need to respect privacy obligations. Some commentators have opined, however, that using non-EU clouds is inconsistent with privacy obligations unless the cloud commits to use the *same* level of protection of the several European countries.[382]

Presumably all the above would be true also for a ABIL that collects data from European clients and store in a US cloud. The argument for application of EU privacy law would be strengthened, probably close to the level of certainty, if the cloud provider has some EU based servers.

One issue remain to be discussed: suppose a US based cloud provider agrees to comply with the Safe Harbor scheme.[383] May a EU based law firm or an ABIL that controls European citizens' data use such a provider? In Opinion 05/2012, the Article 29 Working Party stated that there is "uncertainty with regard to the admissibility of the transfer of personal data to cloud providers established outside of the EEA"[384] and that "the controller must choose a cloud provider that guarantees compliance with data protection legislation."[385] Among the specific cloud computing risks considered in the opinion is "Lack of information on processing (transparency)":

> Some potential threats may arise from the controller not knowing that:
> …
> Personal data is transferred to third countries outside the EEA. Third countries may not provide an adequate level of data protection and transfers may not be safeguarded by appropriate measures (e.g., standard contractual clauses or binding corporate rules) and thus may be illegal.[386]

---

[382] *See, e.g.*, *Are "Clouds" Located Outside The European Union Unlawful?*, available at http://blog.security-breaches.com/2010/07/16/are_clouds_located_outside_the_european_union_unlawful/:

> This is at least what Dr. Thilo Weichert argues. He is the head of the Independent Center for Privacy Protection of the State of Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, or "ULD"), and one of Germany's top privacy experts. In a ***June 18, 2010 opinion***, he wrote on the subject of cloud computing. . . . .
> According to the German expert, the client is still the data controller, which is defined by *Section 3 (8) of Germany's Federal Data Protection Act*. . . .
> Pursuant to *Section 11 of the BDSG*, which regulates the commissioned processing or use of personal data,
> *"Where other bodies are commissioned to process or use personal data, responsibility for compliance with the provisions of this Act and with other data protection provisions shall rest with the principal."*
> Dr. Weichert's opinion is that section 11 does apply, not only to data controllers when the data transfer is inside the European Union, but also when such transfer is outside the European Union. Dr. Weichert's opinion reminds users of their responsibility: "[T]he customer remains responsible for ensuring the confidentiality and integrity of the data" (*"Der Auftraggeber bleibt für die Sicherstellung der Vertraulichkeit und Integrität der Daten verantwortlich*") (at 6.1). He notes that **cloud computing clients are not able to fulfill their responsibilities if the cloud service provider does not provide them with information on how and where their data is stored.** By using cloud services the client will necessarily give up some of its control over the data. **In order to fulfill his responsibility as a data controller, there must a clear agreement between him and the cloud computing service provider. The client must therefore be certain that** *"the technical and organizational measures, such as the contractor's substantive data protection requirements in German law, are respected."*

[383] Opinion 05/2012, above at note 7.
[384] Opinion 05/2012, above at note 7, at 2.
[385] *Id.* at 8.
[386] *Id.* at 6.

In a controversial aspect of the opinion, the Article 29 Working Party advised that the adoption of the Safe Harbor scheme by a cloud provider in itself would *not* be sufficient to comply with EU privacy law:

> [I]n the view of the Working Party, sole self-certification with Safe Harbor *may* not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment.[387]
>
> ….
>
> For these reasons it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.[388]
>
> When the cloud provider does not give same guarantees required by national law, cloud users are "encouraged to use other legal instruments available, such as [EU] standard contractual clauses"[389]

Based on this opinion, it is uncertain whether the use of a US based provider (even if Safe Harbor certified) is lawful for an ABIL. Opinion 05/2012 does not say expressly -- but seems to suggest -- that it is only possible to use a US based cloud <u>if the cloud in question complies with European privacy</u> in whole. No shortcut of Safe Harbor would be sufficient.

Opinion 05/2012 triggered a reaction in the U.S. The U.S. Department of Commerce's International Trade Administration (ITA) issued a document "to clarify that Safe Harbor continues to offer eligible U.S. organizations, regardless of whether or not they are operating in the cloud environment, an officially recognized means of complying with the Directive's "adequacy" requirement.[390] On the question on whether "the U.S.-EU Safe Harbor [is] applicable to cloud service provider agreements", the ITA clearly answered

---

[387] Opinion 05/2012, note 7 above, at 17, emphasis added.

> In addition, Article 17 of the EU directive requires a contract to be signed from a controller to a processor for processing purposes . . . Such contract specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure. . . .
>
> The Working Party also considers that cloud client must verify if the standard contracts composed by cloud providers are compliant with national requirements regarding contractual data processing. National legislation may require sub-processing to be defined in the contract. . .. Normally the cloud providers do not offer the client such information – their commitment to the Safe Harbor cannot substitute for the lack of the above guarantees when required by the national legislation. In such cases the exporter is encouraged to use other legal instruments available, such as standard contractual clauses or BCR.
>
> Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC35. *Id.* 17-18.

[388] *Id.* at 18.

[389] *Id.*

[390] U.S. Department of Commerce's International Trade Administration (ITA), *Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing* at 8, available at http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf ("*ITA's Clarifications on Safe Harbor*").

> Yes, Safe Harbor and the Commission's "adequacy" decision apply to such agreements that involve the transfer of *personal data* from the EU to organizations established in the United States.

However, the ITA specified that "a cloud service provider [is] required to enter into a contract even if it is Safe Harbor-compliant and is receiving personal data merely for processing" because

> the Directive explicitly requires that all data controllers in the EU (1) confirm that the data processor– irrespective of where it is located – provides sufficient data protection guarantees (i.e. technical security and organizational measures) and (2) conclude a contract providing that the data processor shall act only on behalf of and pursuant to the instructions from the data controller and in compliance with all data security requirements that apply to the data controller.
>
> Safe Harbor fully acknowledges this requirement, explaining that the purpose of the contract is to protect the interests of the data controller who retains full responsibility for the data vis-a-vis the data subject(s) concerned.[391]

But

> One of the principal advantages of Safe Harbor certification is that: "contracts with Safe Harbor participants for mere processing" (i.e., contracts between EU data controllers and U.S. data processors) do not require prior authorization or such authorization will be granted automatically by the Member States, whereas contracts with recipients not participating in the Safe Harbor or otherwise not providing "adequate" protection may require prior authorization by relevant data protection authorities. [392]

The ITA reminded that the Commission [has not] issued any new requirements regarding Safe Harbor that "would reduce the value of certification to cloud service providers" and that the Article 29 Working Party's Opinion is "non binding."[393] The ITA also noted that no "[m]ember State data protection authorities [can] unilaterally refuse to recognize Safe Harbor certification . . . [because] the Commission's Safe Harbor adequacy decision is binding on all EU Member States and by extension all EEA Member States."[394]

We agree with the ITA's conclusions. A European law firm and a ABIL subject to EU privacy can safely used a US-based cloud provider that is Safe Harbor certified. If the cloud is not Safe Harbor certified, "may require prior authorization by relevant data protection authorities."[395]

Besides being consistent with the Safe Harbor scheme, this approach is also consistent with modern technology. Any position that would limit the use of non-EU based clouds *per se* might be difficult to

391 *Id.* at 3.
392 *Id.* at 4.
393 *Id.*
394 *Id.* at 6.
395 *Id.* at 4.

maintain in face of the worldwide development of technology and the amount of data being transferred to the cloud.

Taking Google as an example, if you have a look at its website, it states that its servers are located in Iowa, Oregon, Belgium, Georgia, North Carolina, Finland, Ireland, South Carolina, Oklahoma, Hong Kong (China), Singapore, and Taiwan;[396] Google indicates that this list is not complete.

The cloud is an unstoppable factor in modern life because of the volume of Internet traffic and data. In 2012Internet users sent 204 million messages per minute. Google received over 2 million search queries.[397]Amazon EC2, the Amazon web service[398]-- which is probably the biggest cloud -- has been projected "to be worth $50 billion by 2015."[399]

[396] See http://www.google.com/about/datacenters/inside/locations/index.html

[397] How much data is consumer every minute, available at http://www.zdnet.com/blog/btl/how-much-data-is-consumed-every-minute/80666

[398] Nominated the top cloud computing provider for three years in a row (see http://searchcloudcomputing.techtarget.com/photostory/2240149049/Top-10-cloud-providers-of-2012/11/1-Amazon-Web-Services#contentCompress)

[399] Matt Asay, *Amazon Web Services Worth $50 Billion By 2015, And That May Be Too Low*, available at http://readwrite.com/2013/11/20/amazon-web-services-business-worth-50-billion-by-2015-analyst-projects#awesm=~oo2pQOiSOWXbNK (November 20, 2013)