Privilege and Ethical Issues in a Data Driven World

September 12, 2023

ACC Association of Corporate Counsel

BAKER BOTTS

Katherine Cooper

Managing Director & Deputy Head of Group Dispute Resolution, Litigation & Legal Investigations, Americas

BNP Paribas

Katie is a litigator with over 16 years of experience. She is currently a managing director and the deputy head of Group Dispute Resolution, Litigation and Legal Investigations, Americas, at BNP Paribas, where she is responsible for domestic and cross-border litigation and enforcement matters. She has been with the bank since 2014.

Katie began her career at Cleary Gottlieb Steen & Hamilton LLP. From 2008-09, she served as a law clerk to the Honorable Kevin Thomas Duffy of the U.S. District Court in the Southern District of New York.

Aditi Schretzman

Deputy General Counsel

IEX Trading

Aditi Schretzman is the Deputy General Counsel of IEX Group, Inc., which is best-known for operating IEX Exchange, the U.S. stock exchange designed to set new standards for investor protection and performance. As Deputy General Counsel, Ms. Schretzman manages a wide range of legal matters for IEX, including, among other things, corporate transactions, regulatory compliance, corporate governance, financial market data, privacy matters, intellectual property and general litigation.

Nicole A. Spence

Counsel, Data, and AI

IBM

Nicole A. Spence is a Brand Legal Counsel for IBM's Data and AI business unit, as well as one of IBM's AI and IP Policy attorneys for North America. She is also a certified information privacy professional in the US and the EU. Prior to IBM, Nicole practiced as a litigator for more than seven years, and she had her own practice for more than two years, where she advised start-ups in FinTech, music, fashion and software on IP and corporate matters. She earned her BA in Molecular Biology and History at Smith College, and her JD from New York Law School.

Margaret Welsh

Partner

Baker Botts

Maggie Welsh is an experienced patent attorney and helps companies solve complex technology issues. Drawing from her 10+ years of patent litigation, technology transactions, and patent prosecution, Maggie is able to quickly understand underlying issues and provide thoughtful and thorough advocacy for her clients. Whether she is litigating a patent or reviewing technology transaction agreements, Maggie sees the landscape of potential risks and provides her clients with tactics to address them.

Table of Contents

INTRODUCTION: DATA PROLIFERATION AND TECHNOLOGICAL CHANGE

BAKER BOTTS

Polling Question

Do you use cloud services or third-party data storage vendors in your work?

Attorneys and Data

- Proliferation of electronic data means there is more data to organize and control
- Growth of web-based software services ("cloud") can facilitate data management, but also introduces data security risks
  - Breach of confidentiality and endanger maintenance of applicable privileges
- Lawyers have a professional and ethical responsibility to ensure that data is securely protected
- Lawyers must also adapt their advice to clients on how to maintain confidentiality and privilege in a landscape of changing technology

ABA – 2022 Cloud Computing

- Cloud computing: "web-based software service or solutions," including Software as a Service (SaaS)
  - Software or services that can be accessed and used over the internet using a browser (or, commonly now, a mobile app), where the software itself is not installed locally on the computer being used by the lawyer accessing the service
  - Data is processed and stored on remote servers rather than on local computers and hard drives
- Cloud services might be hosted by a third party (Amazon Web Services or Microsoft Azure platforms) or, more commonly in the legal profession, by a provider running its services on Amazon, Microsoft, or another cloud platform
- The average number of cloud applications used by each employee in large business enterprises has been estimated at 36 apps each day

ABA – 2022 Cloud Computing

/ ABA Groups / Law Practice Division / Publications / TECHREPORT / ABA TechReport 2022

November 17, 2022 **TECHREPORT 2022**

2022 Cloud Computing

Dennis Kennedy

Despite the increase and escalation of cybersecurity threats, including cyberwarfare and ransomware, and clear warnings that law firms are targets, the poor cybersecurity approaches of lawyers were again the key take-away from this annual survey. It's difficult to reconcile the ethical duty of technology competence with the reported behaviors of lawyers in the 2022 Survey.

ABA – 2022 Cloud Computing

Survey Highlights

- Cybersecurity has passed the crisis point in lawyers' use of cloud services in our world of cybersecurity risks, ransomware, cyberwarfare, and more. The 2022 survey results showed only modest gains in the lax compliance of lawyers with even the most basic cybersecurity practices. Although lawyers say that confidentiality, security, data control and ownership, ethics, vendor reputation and longevity, and other concerns weigh heavily on their minds, their employment of precautionary security measures is quite low. No more than 40% of respondents were taking any of the specific standard cautionary cybersecurity measures listed in the 2022 Survey question on this topic. A stunning 16% of respondents (down slightly from 18% in 202) reported taking none of the security precautions of the types listed. Only 41% of respondents report that the adoption of cloud computing resulted in changes to internal technology or security policies. These are shocking numbers. Do you feel safe?

ABA – 2022 Cloud Computing

/ ABA Groups / Law Practice Division / Publications / TECHREPORT / ABA TechReport 2022

November 17, 2022 **TECHREPORT 2022**

2022 Cloud Computing

Dennis Kennedy

Takeaways and Action Steps

The 2022 Legal Technology Survey shows that, for a steadily increasing majority of lawyers and firms, cloud services are now part of the IT equation. Overall, reported growth in cloud use moved significantly in the past year, even though it is below what we might have expected with a pandemic and many lawyers working from home. However, the continuing lack of attention to confidentiality, security, and due diligence issues remains a serious and disturbing concern, especially with the growth ransomware and other cyberattacks. Clients will continue to be concerned about whether their law firms making adequate efforts on cybersecurity.

PROFESSIONAL AND ETHICAL OBLIGATIONS RELATING TO DATA SECURITY

BAKER BOTTS

Polling Question

Do you have information security teams or others involved in evaluating third-party data management/storage vendors?

Ethical Rules

- Lawyers have ethical obligations relevant to the management of data:

ABA Model Rules		
1.1: Duty of Competency	1.6: Duty of Confidentiality	5.1, 5.3: Duty to Supervise
1.4: Duty to Communicate		

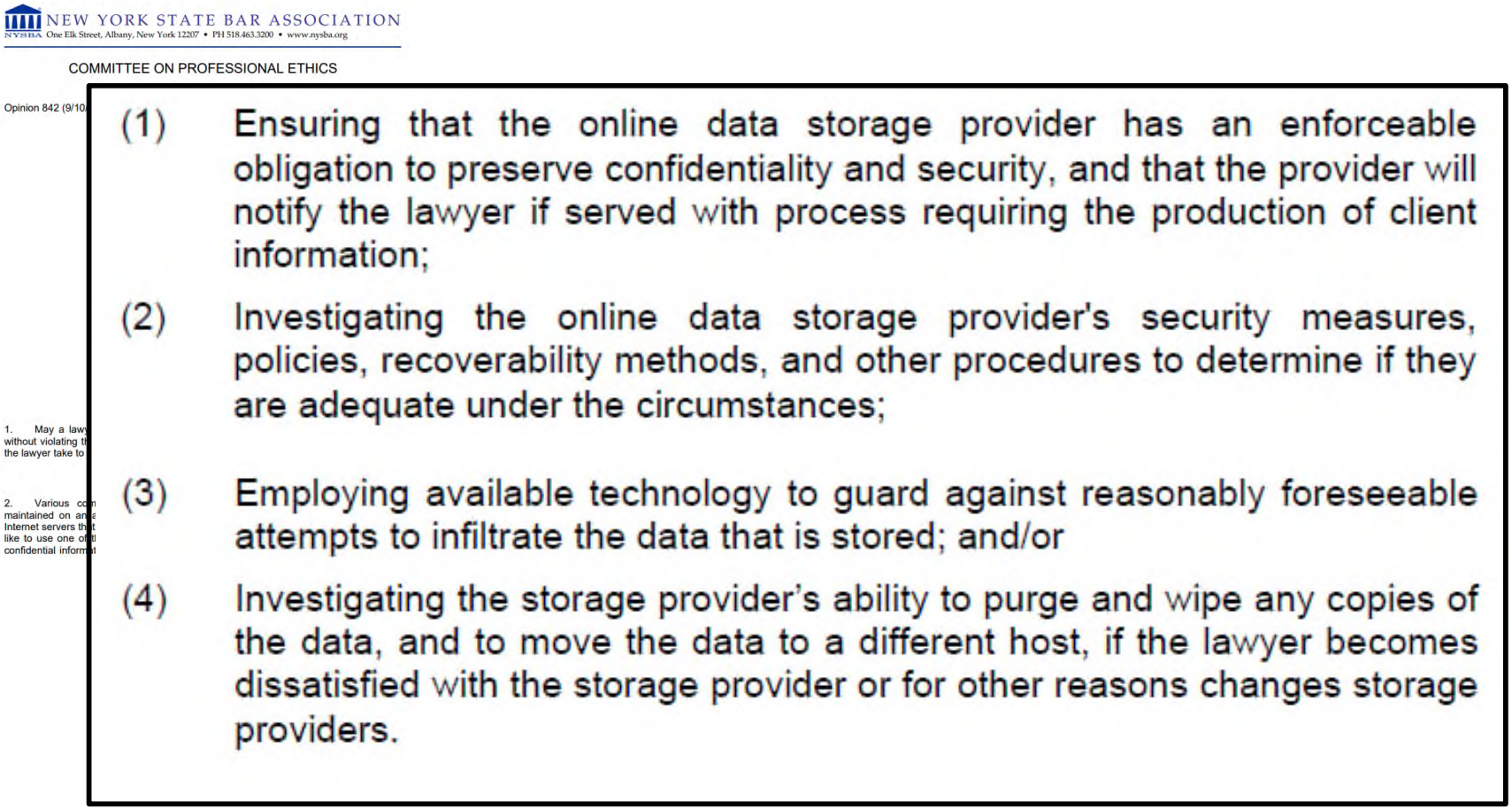
ABA Model Rule 1.1 (Competency)

"A lawyer shall provide **competent representation** to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Comment [8]: "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." (emphasis added).

Bar Association Advisory Opinion

NY State Bar Association's Committee on Professional Ethics Opinion No. 842.



NEW YORK STATE BAR ASSOCIATION
NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10

1. May a lawy
without violating th
the lawyer take to

2. Various com
maintained on an
Internet servers that
like to use one of t
confidential informa

(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;

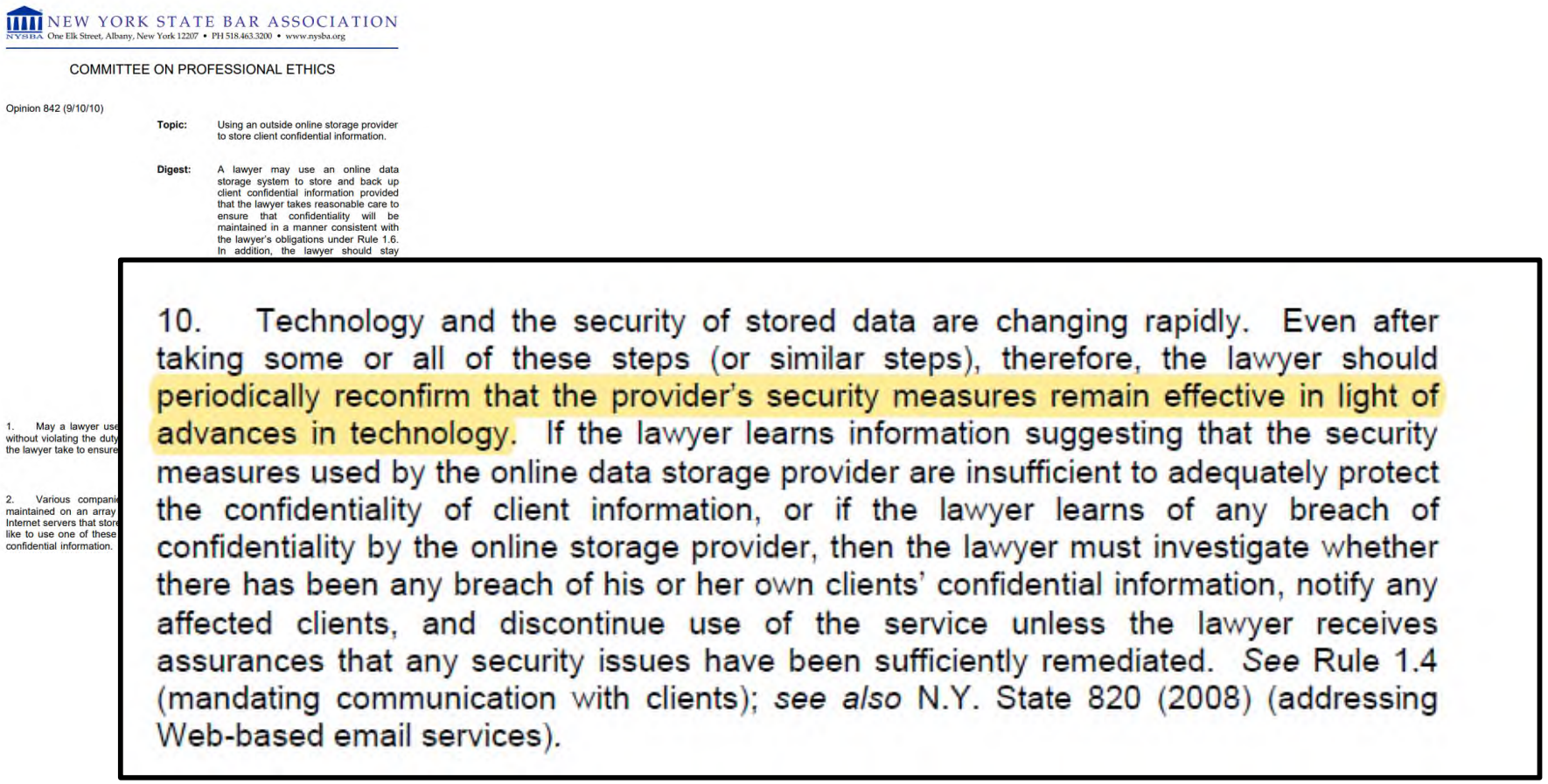
(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(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.

Bar Association Advisory Opinion

NY State Bar Association's Committee on Professional Ethics Opinion No. 842.



NEW YORK STATE BAR ASSOCIATION
NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay

1. May a lawyer use
without violating the duty
the lawyer take to ensure

2. Various companie
maintained on an array
Internet servers that store
like to use one of these
confidential information.

10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. *See* Rule 1.4 (mandating communication with clients); *see also* N.Y. State 820 (2008) (addressing Web-based email services).

ABA Model Rules 1.6 (Confidentiality); 5.1/5.3 (Duty to Supervise)

Make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client

A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer

Bar Association Advisory Opinion

A lawyer wants to use cloud-based services in her delivery of legal services by contracting with a third party provider. The cloud service will include storage, processing and transmission of information in a shared infrastructure and a shared application, multi-tenant environment. The data will include client personal identifiable information, opposing party documents, financial information, health information and any other confidential and public information relevant to the delivery of legal services. The lawyer plans to conduct due diligence when selecting a third party provider to ensure the controls are in place to maintain confidentiality of the client information and data.

QUESTION

May the lawyer use a third party provider for cloud-based services? If so, is the lawyer's due diligence at the time of entering into an agreement with the provider adequate to avoid an ethical violation if a breach of confidentiality should occur through a failure of the provider or through the action of hackers?

Bar Association Advisory Opinion

Illinois State Bar Association's Professional Conduct Advisory Opinion No. 16-06

ISBA Professional Conduct Advisory Opinion

Opin
Octo
Subje
Diges

Refer

1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;
3. Investigating the provider's reputation and history;
4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;
5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
6. Requiring that all data is appropriately backed up completely under the lawyer's control so that the lawyer will have a method for retrieval of the data;
7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.

Bar Association Advisory Opinion

Illinois State Bar Association's Professional Conduct Advisory Opinion No. 16-06

ISBA Professional Conduct Advisory Opinion

ILLINOIS STATE BAR ASSOCIATION

The inquiring lawyer also asks whether the lawyer's due diligence at the time of entering into an agreement with the provider will be adequate to avoid an ethical violation if a breach of confidentiality should occur through a failure of the provider or through the action of hackers. We do not believe that the lawyer's obligations end when the lawyer selects a reputable provider. Pursuant to Rules 1.6 and 5.3, a lawyer has ongoing obligations to protect the confidentiality of client information and data and to supervise non-lawyers. Future advances in technology may make a lawyer's current reasonable protective measures obsolete. Accordingly, a lawyer must conduct periodic reviews and regularly monitor existing practices to determine if the client information is adequately secured and protected. *See, e.g.,* Arizona Ethics Op. 09-04 (2009); Washington State Bar Association Advisory Op. 2215 (2012).

Washington State Bar Association Advisory Op. 2215 (2012)

Practical Tips to Comply with Ethical Rules

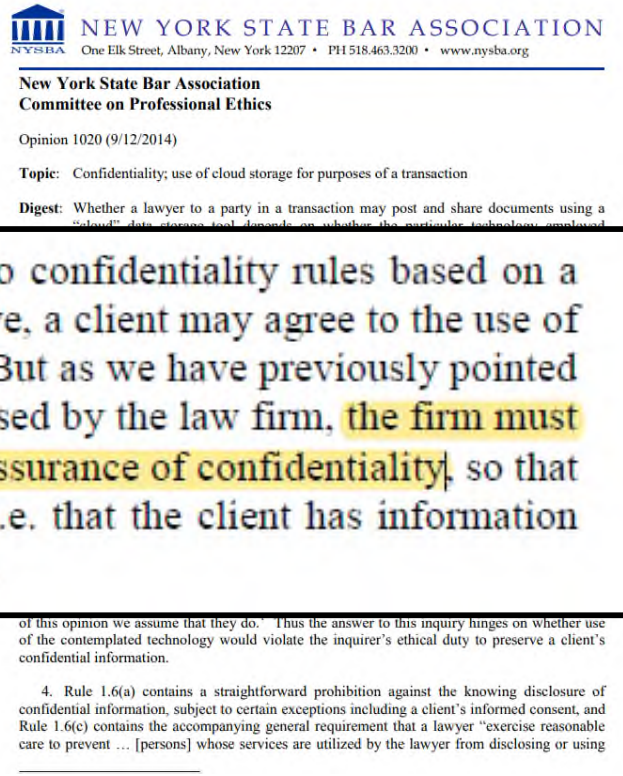
- The Bar Association's advisory opinions emphasize the need for lawyers to do some reasonable diligence regarding vendors and how they store data, not to simply rely on a vendor being reputable
- In practice this can be challenging given rapid changes in technology and data privacy laws
- Consider incorporating some or all of the following into your vendor onboarding process:
  - Have a clear idea from the business as to what data will be processed / stored / available to each vendor
  - Integrate your information security and technology specialists directly into your onboarding process
  - Ask questions! Have a questionnaire or similar diligence document that can be provided to each vendor and reviewed by your technology or other experts where needed
  - Make sure your agreement makes clear where liability falls and what remediation actions vendor would take in the event of a breach

ABA Model Rule 1.4 (Communications)

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

Bar Advisory Opinion

New York State Bar Association's Committee on Professional Ethics Opinion No. 1020



NEW YORK STATE BAR ASSOCIATION
NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

New York State Bar Association
Committee on Professional Ethics

Opinion 1020 (9/12/2014)

Topic: Confidentiality; use of cloud storage for purposes of a transaction

Digest: Whether a lawyer to a party in a transaction may post and share documents using a

9. Finally, we note that Rule 1.6 provides an exception to confidentiality rules based on a client's informed consent. Thus, as quoted in paragraph 5 above, a client may agree to the use of a technology that would otherwise be prohibited by the Rule. But as we have previously pointed out, "before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is 'informed' within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision." N.Y. State 1019 ¶11.

of this opinion we assume that they do." Thus the answer to this inquiry hinges on whether use of the contemplated technology would violate the inquirer's ethical duty to preserve a client's confidential information.

4. Rule 1.6(a) contains a straightforward prohibition against the knowing disclosure of confidential information, subject to certain exceptions including a client's informed consent, and Rule 1.6(c) contains the accompanying general requirement that a lawyer "exercise reasonable care to prevent … [persons] whose services are utilized by the lawyer from disclosing or using

High-Profile Data Breaches at Law Firms and Vendors and Follow-on Litigation

- Data breaches do not spare the legal industry and have routinely been in the news for:
  - Law firms
  - eDiscovery vendors
  - File transfer platforms

- High-profile follow-on litigations
  - Claims for negligence and/or breach of contract, including professional malpractice
  - Statutory violations: claims for failure to comply with specific state law requirements for storing and safeguarding private information

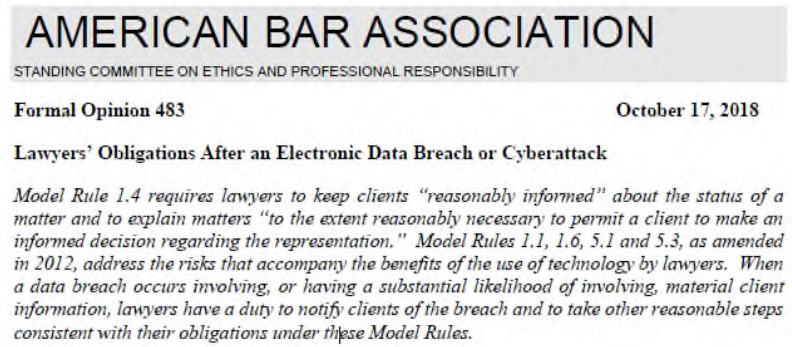
- Data breaches compromise confidentiality and could impair privilege

- Clients must be comfortable with the technological competence of their firms and their firms' vendors

ABA Opinion

ABA Formal 483 - Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,[13] whether further action is warranted,[14] whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.[17]



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Ethical Rules in Event of Data Breach

1. Obligation to Monitor for a Data Breach
2. Stopping the Breach and Restoring the System
3. Determining What Occurred
4. Provide Notice of Breach

CONFIDENTIALITY AND PRIVILEGE IN THE FACE OF TECHNOLOGICAL CHANGE

BAKER BOTTS

Definitions

- Attorney-Client Privilege
  - Protects communications between attorney and client for the purpose of securing legal advice
  - The "predominant purpose" of the communication must be to give or receive legal advice
  - Voluntary disclosure of privileged communications to a third-party results in waiver

- Work Product Privilege
  - Protects material prepared "because of" the prospect of litigation
  - Does *not* protect material prepared in the ordinary course of business or that would have been prepared irrespective of the possibility of litigation
  - Waiver occurs if disclosure has substantially increased the opportunities for potential adversaries to obtain the information

Privilege Guidance

- Principles
  - Comply with all instructions from Legal regarding maintaining confidentiality
  - Failure to maintain privilege can lead to the disclosure of sensitive information
  - Communications between non-lawyers generally are not privileged, unless initiated at the direction of counsel
- Ways to communicate and reinforce
  - Informal guidance
  - Training
  - Programs
    - "Communicate with Care"
- Risks to privilege
  - Inadequate guidance and training
  - Insufficient data security or management

Polling Question

Do you conduct training on privilege?

Programs to Help Clients Understand Privilege

- *United States of America, et al., v. Google LLC*
  - Google's "Communicate with Care" Program
  - DOJ's Motion for Sanctions and to Compel
    - Alleged that Google used the program to train employees to add an attorney, a privilege label, and a generic request for counsel's advice to shield sensitive business communications
    - Court declined to award sanctions

- Takeaways
  - Any policy or program seeking to protect the confidentiality of communications and maintain privilege where appropriate must be carefully vetted and overseen by lawyers
  - Policies should be appropriately tailored to privileged information
  - When in doubt, employees must know to seek situational, specific advice

Channel Proliferation

- Increasing number of channels for communication presents challenges
  - Examples of channels
    - Emails
    - Texting and texting apps
    - Slack
    - Video conferencing
    - Document sharing
- "Off-Channel" Communication Settlements
  - SEC and CFTC have conducted street-wide investigation into whether financial institution employees communicated on unauthorized channels such as WhatsApp and personal text in violation of recordkeeping rules;
  - Penalties to date have topped $2.5B

Press Release

SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures

Firms admit to wrongdoing and agree to pay penalties totaling $289 million

FOR IMMEDIATE RELEASE
2023-149

Washington D.C., Aug. 8, 2023 — The Securities and Exchange Commission today announced charges against 10 firms in their capacity as broker-dealers and one dually registered broker-dealer and investment adviser for widespread and

Managing Data Confidentiality

- Access to privileged information: "need to know" standard generally governs whether the privilege shields communications that are disseminated to corporate employees
  - *Garvey v. Hulu LLC*, No. 11-cv-03764-LB, 2015 U.S. Dist. LEXIS 7042 (N.D. Cal. Jan. 21, 2015)

- Collection of Data – Artificial Intelligence

Practical Tips for Helping Clients Maintain Confidentiality/Privilege

Discussion: How can in-house attorney maintain privilege over some many different channels of communication?

- Training
- Confidential communications should not include unnecessary individuals
  - If they do, it may be more difficult to demonstrate that privilege applies
- Information hygiene policies

AUSTIN

BRUSSELS

DALLAS

DUBAI

HOUSTON

LONDON

NEW YORK

PALO ALTO

RIYADH

SAN FRANCISCO

SINGAPORE

WASHINGTON

bakerbotts.com