LEGAL ETHICS OF EMAIL

National Business Institute
Holiday Inn South Plainfield-Piscataway
South Plainfield, New Jersey 07080
(908) 753-5500

December 14, 2016

By

Paul A. Carbon, Esq.
Jonathan P. Holtz, Esq.

I. Attorney Duties, Statutes and Case Law Regarding Email.

A. Must an Attorney Maintain an Active Email Account?

There is no affirmative duty for an attorney to have an active email account in New Jersey. However, practically speaking, an email account is essential for practice in the New Jersey federal court's e-filing system and the New Jersey state courts' eCourts electronic filing and document management system which is now in effect in some trial court divisions and are in the process of being implementing in the Law, Chancery and Landlord/Tenant Divisions. Further, while not required in New Jersey state court practice, the Rules of Professional Conduct can be read to suggest the use of email communication is encouraged. Indeed, the Advisory Committee on Professional Ethics has noted that use of email "promotes the values embraced in Rules of Professional Conduct ("RPC") 1.4".

Further, currently, many state and federal rules permit electronic communications and filing and provide for protection and production of electronic stored information. Thus, maintenance of an email account is now generally necessary from a practical standpoint.

New Jersey Court Rule 1:21-1(a), amended 1/17/13, effective 2/1/13 (dropped requirement for physical location "bona fide office rule")

R. 1:21-1 requires attorneys to assure "prompt and reliable communication". Further, it specifically mentions email serves as prompt and reliable communication.

> 1:21-1. Who May Practice; Appearance in Court
>
> (a) Qualifications. Except as provided below, no person shall practice law in this State unless that person is an attorney holding a plenary license to practice in this State, is in good standing, and complies with the following requirements:

(1) An attorney need not maintain a fixed physical location for the practice of law, but must structure his or her practice in such a manner as to assure, as set forth in RPC 1.4, **prompt and reliable communication with and accessibility by clients, other counsel, and judicial and administrative tribunals before which the attorney may practice**, provided that an attorney must designate one or more fixed physical locations where client files and the attorney's business and financial records may be inspected on short notice by duly authorized regulatory authorities, where mail or hand-deliveries may be made and promptly received, and where process may be served on the attorney for all actions, including disciplinary actions, that may arise out of the practice of law and activities related thereto.

...

(3) **The system of prompt and reliable communication required by this rule may be achieved through** maintenance of telephone service staffed by individuals with whom the attorney is in regular contact during normal business hours, through promptly returned voicemail or **electronic mail service**, or through any other means demonstrably likely to meet the standard enunciated in subsection (a)(1).

...

New Jersey Court Rule 1:4

New Jersey Court Rule 1:4-1 requires all papers submitted to contain the attorney's specific contact information and bar identification number. No email address is required.

RULE 1:4. Form And Execution Of Papers

1:4-1. Caption: Name and Addresses of Party and Attorney; Format

...

(b) Format; Addresses. At the top of the first page of each paper filed, a blank space of approximately 3 inches shall be reserved for notations of receipt and filing by the clerk. Above the caption at the left-hand margin of the first sheet of every paper to be filed there shall be printed or typed the name and the New Jersey attorney identification number of the attorney filing the paper, office address

> and telephone number or, if a party is appearing pro se, the name of such party, residence address and telephone number. No paper shall bear an attorney's post office box number in lieu of a street address. An attorney or pro se party shall advise the court and all other parties of a change of address or telephone number if such occurs during the pendency of an action.

New Jersey Rule of Professional Conduct 1.4

New Jersey Rule of Professional Conduct 1.4 does not require an attorney to maintain an email address; however, it does require an attorney to keep his client reasonably informed of, and promptly respond to, information requests. The Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage And Access of Client Files", notes that absent certain specific documents which must be maintained in paper form (such as wills), "there is nothing in the Rules of Professional Conduct that mandates a particular medium of archiving such documents". Further, the Advisory Committee notes that the use of electronic records and email "also has the potential of enhancing communications between lawyer and client, and promotes the values embraced in RPC 1.4".

> RPC 1.4. Communication
> (a) A lawyer shall fully inform a prospective client of how, when, and where the client may communicate with the lawyer.
> **(b) A lawyer shall keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information.**
> (c) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.
> (d) When a lawyer knows that a client expects assistance not permitted by the Rules of Professional Conduct or other law, the lawyer shall advise the client of the relevant limitations on the lawyer's conduct.

New Jersey Rule of Professional Conduct 3.2

New Jersey Rule of Professional Conduct 3.2 does not require an attorney to maintain an email address; however, it does require an attorney to make reasonable efforts to expedite litigation, which can be achieve, in part, through electronic mail service and communication.

> RPC 3.2. Expediting litigation
> A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client and shall treat with courtesy and consideration all persons involved in the legal process.

eCourts – New Jersey State Court Electronic Document Filing and Management System

eCourts is a web based application that is designed to allow attorneys, in good standing, to electronically file documents with the courts. The judiciary's plans for full implementation of eCourts in all trial court divisions is underway. The plan to modernize the Court's filing and document management systems focuses on electronic filing and information exchange between the court and attorneys, the creation of an electronic filing system, the establishment of an electronic case jacket, and the maintenance of an electronic records management system that provides both attorneys and the public with access to case information. An email account is essential for registering with and accessing eCourts.

Effective June 3, 2014, the Supreme Court has relaxed and supplemented the following Rules of Court pertaining to proof of service for documents electronically filed and served using a judiciary-authorized electronic filing system and applying the changes to the Judiciary's eCourts system:

- Rule 1:5-2 ("Manner of Service") – so as to permit service of process by electronic filing using an approved electronic filing system pursuant to Rule 1:32-2A(a), where that electronic filing system records that an automated notice of filing has been generated and transmitted.

- Rule 1:5-3 ("Proof of Service") – so as to suspend the requirement to file a separate proof of service document for those pleadings electronically filed using an approved electronic filing system pursuant to Rule 1:32-2A(a), provided that the electronic filing system records that an automated notice of filing has been generated and transmitted.

The electronic proof of service and the suspension of the requirement to file a separate proof of service document apply only to those parties who are registered as participants in the approved electronic filing system; for all other parties, the provisions of Rule 1:5-2 and 1:5-3 shall continue to apply.

Effective February 12, 2015, attorneys were able to file documents electronically with the Tax Court through the Judiciary's eCourts system and view electronic case jackets for all local property tax matters. In order to file documents electronically and view electronic case jackets attorneys must first register with the Administrative Office of the Courts. Instructions on registration and using eCourts are available at *njcourts.com/ecourts*.

Per the Supreme Court's January 21, 2015 Order, the following Rules were supplemented as they relate to the filing of any document through the electronic filing system for the Tax Court of New Jersey:

1. Rule 1:4-9 ("Size, Weight and Format of Filed Papers") so as to permit attorneys to file all Tax Court pleadings and other papers in an electronic format

prescribed by the Administrative Director of the Courts that will produce, as needed, printed paper copies that meet the requirements of the rule.

2. Rule 1:5-6(c) ("Filing – Nonconforming Papers") so as to permit the Tax Court Clerk to reject a document submitted for filing electronically if the document is not presented in accordance with the standards for filing prescribed by the Administrative Director of the Courts, and to permit the Tax Court Clerk to transmit information concerning that rejection for filing to the submitting attorney by electronic means.

3. Rule 1:6-2 ("Form of Motion; Hearing") so as to permit attorneys to file, in electronic form, proofs of service of notice of motion as well as any other motion information prescribed by the Administrative Director of the Courts when the moving papers are filed electronically.

4. Rule 1:13-4 ("Transfer of Actions") so as to provide that the papers filed in the incorrect forum and transferred to another court or agency may be printed paper copies of the documents that have been filed electronically.

5. Rule 1:37-2 ("Seal of Courts") so as to permit the printed reproduction of the Tax Court's seal on all papers required by the Rules of Court to contain a seal.

6. Rule 4:3-4 ("Transfer and Removal of Actions") so as to provide that the papers transferred to another court may be printed papers copies of the documents that have been filed electronically.

7. Rule 4:4-7 ("Return [of Service]") so as to permit attorneys to file proofs of service in electronic form.

8. Rule 4:42-1(e) ("Form; Settlement – Submission and Filing of Orders and Judgment") so as to permit judges to affix electronically a facsimile of the judge's signature to an order or judgment, to permit the submission of the form of order or judgment electronically by an attorney, and to require the submission of only the original of the form or order of judgment if it is filed electronically. This rule is further relaxed and supplemented so as to dispense with the requirement that a self-addressed, stamped envelope be submitted by the attorney or party submitting the form of order.

Further, consistent with the provisions of Rule 1:32-2A and in furtherance of the electronic filing system for the Tax Court of New Jersey, the Part VIII Rules were relaxed and supplemented as follows:

1. To permit the filing of all pleadings and other papers in an electronic format prescribed by the Administrative Director of the Courts.

2. To permit service of process in an electronic format using an approved electronic filing system pursuant to R. 1:32-2A(a) where that electronic filing system records that an automated notice of filing has been generated and transmitted.

3. That pursuant to R. 1:32-2A(c) an electronic signature shall have the same force and effect as an original handwritten signature.

4. To permit the Tax Court to issue notifications, orders, judgments and other documents in an electronic format using an approved electronic filing system pursuant to R. 1:32-2A(a).

On July 2, 2014, the Judiciary completed its statewide implementation of eCourts Criminal for use is the Criminal Division by prosecutors and public defenders. Thereafter, effective March 31, 2015, private attorneys submitting documents to the court for filing in Criminal Division cases were able to file those documents electronically through eCourts Criminal, with certain limited exceptions, and to view online the documents that are in the electronic Criminal case jackets.

The Judiciary Electronic Filing Imaging System ("JEFIS") was retired for Special Civil Part DC filings (those of $15,000 or less) as of September 30, 2016. The system was replaced by the new electronic filing application – eCourts Special Civil. The new efiling application allows attorneys to file documents online at any time and provides real-time remote access to electronic case files in the Special Civil Part ("DC") case type.

In anticipation of the retirement of JEFIS for Special Civil Part DC cases, as of August 12, 2016, the Judiciary was currently accepting electronic filing via eCourts Special Civil in the following counties: Bergen, Hunterdon, Mercer, Somerset, and Warren. Additional counties will be added on a rolling basis. Once JEFIS has been retired, use of eCourts Special Civil for Special Civil Part DC cases will be required. FAQ's and guides on the use of eCourts Special Civil, as well as a schedule of eCourts Special Civil availability in each county, are available at *njcourts.com/eCourts*. eCourts Special Civil Part and General Equity / Foreclosure began implementation in July 2016.

Finally, effective July 1, 2016, and as set forth in an April 12, 2016 Order of the Supreme Court, the Supreme Court has approved a two-phase approach for implementation of mandatory electronic filing of all Appellate Division appeals and other documents in appellate matters through the New Jersey Judiciary eDATA system (also referred to as eCourts-Appellate). In order to file documents electronically and view electronic case jackets, attorneys must first register with NJ eDATA and also have a collateral account with the Judiciary Account Charge System ("JACS"). Instructions on this registration process and for obtaining a JACS account and information on future CLE courses may be found at:
http://www.judiciary.state.nj.us/appdiv/eDATA/index.html.

Mandatory e-Filing – Phase I

1. All attorneys are required to file electronically in the following case types:

    a. Criminal appeals,
    b. Children in Court (FG and FN) appeals,
    c. Sexually Violent Predator (SVP) appeals,
    d. Civil Commitment Appeals.

2. Attorneys for respondents are required to register for NJ eDATA within seven (7) business days of the email notification of the filing of the notice of appeal.

3. Rule 1:5-6(c) is supplemented and relaxed such that attorneys in the case types identified in paragraph 1 above who file paper pleadings and documents that are required to be filed electronically will have those documents returned stamped "Received But Not Filed-Must be filed electronically." Those documents must be filed electronically within 15 days in order to preserve the original received date. Instructions on the filing requirements to preserve the time will be returned with the date stamped documents.

4. Attorneys may continue to voluntarily file electronic appeals in any case type where the responding party is represented by an attorney.

5. Exemptions to these requirements may be granted by leave of court if extraordinary circumstances prevent an attorney or law firm from utilizing NJ eDATA.

6. Except as otherwise specified in the April 12, 2016 Supreme Court Order, the provisions of the Rules of Court applicable to matters filed in the Appellate Division, and the January 21, 2015 rule relaxation Order (available on njcourts.com), shall remain in full force and effect.

Mandatory e-Filing – Phase II

1. Phase II will be implemented at a later date and will require all attorneys to electronically file appeals under all other case types.

District of New Jersey E-filing

The United States District Court for the District of New Jersey utilizes the Case Management Electronic Filing System (CM/ECF) for accepting court documents for filing. With minor exceptions, the DNJ requires all civil, criminal, miscellaneous cases and documents to be filed in the ECF System. An email address is essential for registering with CM/ECF.

PACER (Public Access to Court Electronic Records)

PACER is an electronic public access service that allows users to obtain case and docket information online from federal appellate, district, and bankruptcy courts, and the PACER Case Locator. PACER registration requires an email address.

Preserving Electronically Stored Information Under Amended Federal Rule of Civil Procedure 37(e)

In December 2015, there were several amendments to the Federal Rules of Civil Procedure. One of the most significant changes was to Rule 37(e), which concerns a party's failure to preserve electronically stored information ("ESI"). Rule 37(e) was amended because it did "not adequately address the serious problems resulting from the continued exponential growth [of ESI]" and because federal circuits established significantly different standard for imposing sanctions under Rule 37 that has "caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions." See Rule 37(e) advisory committee's notes to 2015 amendment.

Under amended Rule 37(e),

> if electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court: (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or (2) only upon the finding that the party acted with the intent to deprive another party of the information's use in the litigation may: (A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e)(1) and (2).

B. Duty of Confidentiality

Most state bar associations officially approved the use of email to communicate with clients in the late 1990s. Although there are no duties of confidentiality expressly addressing email, attorneys have general duties of confidentiality which would apply to email communications.

New Jersey Rule of Professional Conduct 1.6

RPC 1.6 is New Jersey's primary source of confidentiality over an attorney's representation

of a client:

> RPC 1.6. Confidentiality of Information
>
> (a) A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b), (c), and (d).
>
> ...

Note the difference in the ABA Model RPC 1.6, which specifically mentions taking reasonable efforts to prevent unauthorized disclosure (breach) of such information:

> (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 Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage And Access of Client Files", raised concerns with electronic records and RPC 1.6:

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

The Advisory Committee struggled regarding setting specific standards for safeguarding electronic records due to the rapid pace of technology, and noted "[w]e are reluctant to render a specific interpretation of RPC 1.6 or impose a requirement that is tied to a specific understanding of technology that may very well be obsolete tomorrow." Rather, the Committee concluded that "[t]he touchstone in using "reasonable care" against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security; and (2) use is made of available

technology to guard against reasonably foreseeable attempts to infiltrate the data." In response to the specific inquiry, the Advisory Committee stated that the attorney, when sending specific confidential material, should password protect the document "since it is not possible to secure the Internet itself against third party access." This quote is a somewhat outdated comment on current day email protections because most email communications are now essentially and universally encrypted.

New Jersey Rule of Professional Conduct 1.15

RPC 1.15, regarding safekeeping property, also applies to a client's files (which although not technically "property of the client", still give rise to duties to maintain such records, Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage And Access of Client Files"):

> RPC 1.15. Safekeeping property
>
> (a) 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 a financial institution in New Jersey. Funds of the lawyer that are reasonably sufficient to pay bank charges may, however, be deposited therein. 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 seven years after the event that they record.
> (b) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person. Except as stated in this Rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive.
> (c) When in the course of representation a lawyer is in possession of property in which both the lawyer and another person claim interests, the property shall be kept separate by the lawyer until there is an accounting and severance of their interests. If a dispute arises concerning their respective interests, the portion in dispute shall be kept separate by the lawyer until the dispute is resolved.
> (d) A lawyer shall comply with the provisions of R. 1:21-6 ("Recordkeeping") of the Court Rules.

C. Duty to Warn Client of Potential Breach of Confidentiality.

Breach by Attorney

New Jersey court rules do not contain express provisions imposing affirmative duties on attorneys to advise a client of a potential breach of confidentiality when the attorney's email has been hacked. However, arguably, a potential breach of attorney-client information would trigger RPC 1.4(b)'s duty to keep the client reasonably informed. Additionally, an attorney's duty to advise a client of a potential breach in confidentiality would appear inherent in the attorney client relationship.

Further, based on the type of information contained in the breach, the attorney (just like any other business entity) may be under various obligations to disclose or warn the client of a potential breach pursuant to state and federal consumer protection and breach notification laws applicable to personal information. See, e.g. The Health Insurance Portability and Accountability Act ("HIPAA"), 42 CFR § 164, 501, *et seq.*

New Jersey's Theft Prevention Act, N.J.S.A. 56:8-163 and 164, requires any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information to disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The statute requires disclosure to a customer or client to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c of the statute, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The statute further provides that disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years. N.J.S.A. 56:8-163(a). Further, section (b) of the statute provides that "any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person." The statute goes on to provide the methods, manner and timing of notification required. N.J.S.A. 56:8-163(c)-(8).

N.J.S.A. 56:8-164 prohibits the public posting or publically displaying an individual's social security number, or any four or more consecutive numbers taken from the individual's social security number, printing an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed, printing an individual's social security number on any card required for the individual to access products or services provided by the entity, intentionally communicating

or otherwise making available to the general public an individual's social security number, requiring an individual to transmit his social security number over the Internet, unless the connection is secure or the social security number is encrypted, or requiring an individual to use his social security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site.

"Spear phishing" is the mimicking of the real email addresses of buyers, sellers, counsel and real estate companies, and sending email directing individuals involved in real estate closings to transmit funds to bank accounts controlled by hackers.

The case of Millard v. Doran illustrates the potential liability to legal professionals resulting from spear phishing incidents. In that case, Robert and Bethany Millard hired real estate attorney Patricia Doran, Esq., in connection with their purchase of a $20M apartment in New York City. During contract, Doran's America On-Line (AOL) email account was hacked by cyber criminals. After review of communications about the purchase, the hackers sent emails to the Millards, posing as Doran, with wire transfer instructions to a bank that purportedly belonged to the seller. The Millards wired $1.938 million to the account. The hackers then sent Doran a confirmation email purportedly from the sellers' attorney (allegedly mis-spelling the attorney's name), which Doran forwarded to the Millards. The scheme was eventually uncovered, and the Millards were eventually able to recover all but $200,000 of the deposit. In April 2016, the Millards filed a legal malpractice claim against Doran in New York, citing her use of a "notoriously vulnerable" ISP email account (AOL), rather than an ISP email account with more current protections. Millard v. Doran, Supreme Court of New York, County of New York, Index No. 153262/2016.

Breach by Client

In Formal Opinion 11-459, by the American Bar Association Standing Committee on Ethics and Professional Responsibility, "Duty to Protect the Confidentiality of E-mail Communications with One's Client", August 4, 2011, the ABA noted that, in employment cases, attorneys have a duty to warn clients of the risk of discussing their employment case using employer-owned devices or accounts. The opinion more generally stated that attorneys have a duty to advise clients of the potential for any third-party to intercept or obtain electronic communications, including, but not limited to, spouses using their home computer to consult matrimonial attorneys, clients using public computers or public Wi-Fi, clients using devices (computers, tablets, and cell phones) which belong to others, or to which others have a right to inspect, and clients using devices which automatically back up to servers which belong to others, or to which others have a right to inspect. The opinion generally cites to duties of attorney-client confidentiality, which may be applied to the context of email to require the attorney to take reasonable steps to protect client communications and information. Although outdated, ABA Op. 99-413 (1999) ("Protecting the Confidentiality of Unencrypted E-Mail"), provides transmission of information to clients via unencrypted email is not a violation of the model rules; however, the more sensitive the information, the more protection should be employed. Encrypted email has become the standard, rather than the exception, and the field of email communication is

approaching universal end-to-end encryption, which would largely render opinions regarding unencrypted email moot.

D. Reasonable Expectation of Privacy

Privacy over emails in the possession of third party Internet Service Providers (ISPs) is primarily governed by two acts, Electronic Communications Privacy Act of 1986 and the Stored Communications Act. These Acts are based on an outdated understanding of emails and the internet; have been weakened by divergent and inconsistent federal court opinions; and have been criticized by Internet Service Providers, legal scholars, and privacy advocacy groups. There are currently bipartisan efforts to update and reform these Acts including the currently pending Email Privacy Act. Additionally, powerful Internet Service Providers are aggressively defending against information requests pursuant to these Acts, as well as affirmatively challenging the constitutional validity of these Acts. Accordingly, reform or repeal of these Acts appears to be imminent.

Electronic Communications Privacy Act of 1986 (Title I) and Stored Communications Act (Title II)

The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-22 (the "ECPA") was enacted to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer, and to limit access to stored electronic communications (the Stored Communications Act). It has since been updated by various legislation, including the Communications Assistance for Law Enforcement Act of 1994, USA PATRIOT Act, USA PATRIOT reauthorization acts, and the FISA Amendments Act. Title I protects electronic communications (including emails) during transit. It sets forth stringent search warrant requirements. Title II (the SCA) protects communications held in electronic storage (including emails), with similar, but weaker, protections. The ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which set limits for government wiretaps on "hard" telephone lines, but not computer or other digital communications.

Specifically, Title I, prohibits actual or attempted interception, use, disclosure or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515. It outlines the procedures for obtaining judicial authorization for intercepting such communications. 18 U.S.C. § 2516-18.

Title II protects stored electronic communications and transactional records held by third-party ISPs. The SCA imposes criminal penalties for unauthorized accessing or obtaining of electronic communications while in electronic storage. 18 U.S.C. § 2702. Under certain circumstances, ISPs can share "non-content" information, such as log data and the name and email address of the recipient with entities other than government entities. Also, private ISPs (businesses and universities) can freely disclose content and non-content information. For

unopened email stored for 180 days or less, the government must obtain a search warrant. For opened emails stored for 180 days or less, it is unclear.

	Voluntary Disclosure Allowed?	Voluntary Disclosure Allowed	Mechanisms to Compel Disclosure	Mechanisms to Compel Disclosure
	Public Provider	Non-Public Provider	Public Provider	Non-Public Provider
Unopened email (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Search Warrant [§ 2703(a)]	Search Warrant [§ 2703(a)]
Unopened email (in electronic storage more than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Subpoena with notice; § 2703(d) order with notice; or search warrant [§ 2703(a), (b)]	Subpoena with notice; § 2703(d) order with notice; or search warrant [§ 2703(a), (b)]
Opened e-mail, other content files being stored or processed	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702(a)(2)]	Subpoena with notice; § 2703(d) order with notice; or search warrant [§ 2703 (b)]	SCA does not apply [§ 2711(2)]
Non-content records	No, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	§ 2703(d) order; or search warrant [§ 2703(c)(1)]	§ 2703(d) order or search warrant [§ 2703(c)(1)]
Basic subscriber information, session logs, IP addresses (anything in § 2703(c)(2))	No, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	Subpoena; § 2703(d) order; or search warrant [§ 2703(c)(2)]	Subpoena; § 2703(d) order; or search warrant [§ 2703(c)(2)]

*Chart courtesy of Orin S. Kerr, A User's Guide to the Stored Communications Act, and a

Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1216 (2004).

Email Privacy Act

The Email Privacy Act (currently introduced as H.R. 66 in the 114th Congress (2015-2016)) is a bipartisan proposal designed to reform the ECPA. The EPA would extend the ECPA's protections to emails stored for over 180 days. The EPA would also essentially codify the holding of State v. Warshak, as discussed below. The EPA has not yet been passed.

E. Electronic Communications Privacy Act (ECPA) and United States v. Warshak

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) is a Sixth Circuit United States Court of Appeals case which held the government violated Warshak's Fourth Amendment rights by compelling his Internet Service Provider (ISP) to turn over Warshak's emails without a search warrant based on probable cause. Warshak is the first case to recognize a reasonable expectation of privacy, subject to Fourth Amendment protection, in a user's emails stored on third-party servers.

Factual Background

Starting in approximately 2001, Defendant Steven Warshak ("Warshak") was the owner of Berkeley Premium Nutraceuticals, Inc. ("Berkeley"), the distributor of popular male herbal sexual enhancement supplement "Enzyte". Id. at 274, 276. While made popular by the aggressive advertising campaign featuring "Smilin' Bob", Enzyte was largely marketed with the assistance of completely fabricated material, including "independent customer studies", customer satisfaction ratings, and medical endorsements. Id. at 277. Berkeley automatically enrolled customers in its "auto-ship" program, in which customers who received a free trial of a product were unwittingly subscribed to continue receiving the product and incur recurring charges on their credit card. Id. 277-78. Customers were required to affirmatively opt-out of the program to cancel; however, the customers were never advised they were enrolled in the program to begin. Id. at 277-78. Starting in approximately 2002, after voluminous complaints, Berkeley began to disingenuously and sporadically advise customers of the auto-ship program. Id. at 278. However, Warshak instructed that regardless of whether or not a customer agreed to the auto-ship program, the customer was to be enrolled in the auto-ship program. Id. at 279. By 2004, customer complaints had not slowed, and the President of the Better Business Bureau sent a letter to Warshak directly, advising of the specific issue with the auto-ship program. Ibid. Berkeley's merchant banks began terminating Berkley's merchant accounts due to the high percentage of charge-backs as a result of customers disputing the auto-ship creditcard charges. Id. at 279-280. Warshak began applying for new merchant accounts with false information. Id. at 280. Additionally, to lower the percentage of charge backs, Warshak instructed that single orders were to be charged in two or three transactions ("double-dinging" and "triple-dinging", respectively). Ibid. Thus, potentially resulting in a lower percentage of charges being disputed. Ibid. Further, Warshak had his employees charge Warshak's personal credit card for $1.00 charges up to the credit limit

to dilute the percentage of chargebacks on the merchant account. Id. at 280-81.

In approximately 2004, the government formally requested, pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq. ("SCA"), that Warshak's ISP prospectively preserve the contents of any emails to or from Warshak's email account (without notice to Warshak). Id. at 283. In January 2005, the government obtained a subpoena, pursuant to the SCA, and compelled the ISP to turn over the preserved emails. Ibid. In May 2005, the government served the ISP with a Court Order compelling it to surrender any additional emails in Warshak's account. Ibid.

On June 12, 2006, Warshak filed a claim against the United States seeking a declaratory judgment and injunctive relief claiming the compelled disclosure of his emails from his ISP violated his Fourth Amendment Rights. The district court filed a preliminary injunction, which was affirmed by the Sixth Circuit; however, the decision was vacated on ripeness grounds by an *en banc* panel of the Sixth Circuit.

In September 2006, a grand jury in the Southern District of Ohio returned a 112-count indictment charging Warshak and others (including his mother) with various crimes related to Berkeley's business sounding in money laundering, and mail, wire, and bank fraud. Id. at 281. Before trial, Warshak moved to exclude thousands of emails which the government had obtained from his ISP. Ibid. The motion was denied. Ibid. In January 2008, the case proceeded to a six-week trial wherein Warshak was convicted of the majority of the charges. Ibid. Warshak was sentenced to 25 years of imprisonment, fined over $100,000, and ordered to surrender over $90,000,000. Id. at 281-82. After a series of unsuccessful post-trial motions, Warshak appealed. Ibid.

Warshak argued that the government's warrantless, *ex parte* seizure of approximately 27,000 of his private emails constituted a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures. The government countered that, even if government agents violated the Fourth Amendment in obtaining the emails, they relied in good faith on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., a statute that allows the government to obtain certain electronic communications without producing a warrant. The government also argued that any hypothetical Fourth Amendment violation was harmless.

The Sixth Circuit found that the government did violate Warshak's Fourth Amendment rights by compelling his ISP to turn over the contents of his emails. However, the Court found that the agents relied on the SCA in good faith, and therefore held that reversal is unwarranted. Id. at 282.

The Stored Communications Act

The Sixth Circuit held that the Stored Communications Act permits a "governmental entity" to compel an ISP to disclose the contents of [electronic] communications in certain circumstances. The court explained that the SCA covers basic e-mail services. The court addressed the difference

between "electronic storage" which is "any temporary, intermediate storage of a wire or electronic communication . . . and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication" as opposed to "remote computing services" which provide "computer storage or processing services" designed for longer-term storage. The compelled-disclosure provisions give different levels of privacy protection based on whether the e-mail is held with an "electronic communication" service or a "remote computing service", as well as based on how long the e-mail has been in electronic storage. Overall, the government may obtain the contents of e-mails that are "in electronic storage" with an electronic communication service for 180 days or less "only pursuant to a warrant." The government has three options for obtaining communications stored with a remote computing service and communications that have been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d).

The Fourth Amendment

The Sixth Circuit held that the Fourth Amendment protects from unreasonable searches and seizures, and holds that no warrants shall be issued absent probable cause. U.S. Const. Amend. IV. The question for Fourth Amendment application is whether a "search" occurred, meaning whether the government infringed on a reasonable expectation of privacy. The analysis concerns (1) whether there was a subjective expectation of privacy, and (2) was that expectation reasonable.

The Court found Warshak "plainly" manifested an expectation of privacy in his emails, based on the extent to which his sensitive personal and business details (sometimes "damning") were laid out therein.

As to whether society is prepared to recognize an expectation of privacy in emails as reasonable, "the question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication." Id. at 284. The Court noted the extent to which modern day email users' entire activities can be disclosed via access to their email account. Ibid. The Court began by noting email (and the internet) are merely the new communication networks, and the Fourth Amendment has always been required to apply to new communication networks "or its guarantees will wither and perish." Id. at 285. Analogy was made to post office mail and the public telephone, from which an expectation of privacy is found, despite the fact the post office and telephone company have the ability to intercept the communication. Ibid. Accordingly, "[i]f we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment" because "the ISP is the functional equivalent of a post office or a telephone company." Id. at 286.

Although the Court acknowledged that some ISP's contractually reserve the right to access user emails, and "a subscriber agreement might, in some cases, be sweeping enough to defeat a

reasonable expectation of privacy in the contents of an emails account", such as when the ISP states an intention to "audit, inspect, and monitor" user emails, "we doubt that will be the case in most situations." Id. at 286-87. The Court rejected that the ability or right of a third-party intermediary to access communications does not defeat a reasonable expectation of privacy.

Accordingly, the Court held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP." Id. at 288. To the extent the SCA permits the government to compel an ISP to turn over a user's email without a warrant based on probable cause, the SCA is unconstitutional.

IV. Data Security and Cloud Storage - Does the Email You Delete Really Disappear?

Basics of Email Transfer and Storage

As a preliminary matter, a general discussion of the basics of email transfer and storage is required because of how courts address the application of the Fourth Amendment to email. Specifically, the Fourth Amendment provides:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Thus, whether the protections of the Fourth Amendment apply to an individual's emails, which are held by third-party Internet Service Providers, requires an understanding of how emails are transferred, and where/how emails are stored. This is because the Fourth Amendment generally does not offer protection to information shared with third-parties:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

United States v. Miller, 425 U.S. 435, 443 (1976).

Basics of Email Transfer

Every email requires the use of a sending server and a receiving server. Servers may be public, such as Google or Hotmail, or private, such as a private servers operated by a company, government agency, or educational facility.

Once you compose an email and hit send, your email is uploaded to your sending server.

Your sending server then communicates with other servers, and routes the email over the public internet to reach the recipient's server. If the recipient of the email has the same domain as the sender (e.g. a Gmail user sending an email to another Gmail user), the email is routed directly to the receiving server with less exposure over the public internet. Once an email reaches a recipient's server, it is stored until viewed.

Thus, as will be explained more fully below, an individual sending an email to another has arguably potentially shared this communication with both his third-party Internet Service Provider, as well as the recipient's third-party Internet Service Provider, raising issues of expectation of privacy. Additionally, limited information, such as the sender and recipient, has been potentially shared with a number of intermediary third-party servers which help route the email from the sending server to the receiving server, thus raising even greater issues of expectation of privacy as to that limited information.

Basics of Email Storage

POP v. IMAP v. MS Activesync

The user's method of email storage is also a critical consideration. A major difference in email accounts is the use of POP (Post Office Protocol), IMAP (Internet Message Access Protocol), or MS Activesync. Unfortunately, email storage has evolved so rapidly that discussions of these protocols in case law, and arguments of application to the governing statutes, is continually changing and becoming outdated.

POP is a protocol in which your email messages are saved on a remote server. Originally, when you access your email from a POP account, all emails were downloaded onto your computer, and no copy was saved on the server. This was largely due to the limited storage space allocated to email users. Thus, POP was an email equivalent to a Post Office, which collects and holds your physical mail until you pick it up, and thereafter cannot give you the mail a second time. If you subsequently checked your email from a different device, you would no longer be able to access any emails previously downloaded (and deleted). The fact that POP downloaded a user's emails to the user's computer and then deleted the emails from the third-party server had an impact on the court's analysis of who was in possession of the user's email. However, as technology advanced, POP accounts began offering options to hold on to copies of downloaded emails for a specified time period, thus allowing you to download them to multiple devices within that timeframe. Modern POP accounts usually allow options to hold copies of downloaded emails indefinitely. As POP accounts changed from temporary to more permanent storage, it arguably rendered moot the court's prior analysis of POP accounts.

IMAP is also a protocol in which your email messages are saved on a remote server. However, with IMAP, when you access your email account, you view the emails from the server without downloading and deleting the messages. Thus, the emails remain on your server, and you can access and synchronize all your emails on and across multiple devices (computers, phones, tablets, etc.)

MS Activesync is similar to IMAP; however, it also allows you to sync additional data such as your calendar and address book. MS Activesync also allows the server greater power to make changes to the user's account, such as allowing the server to remotely delete all data from a stolen device. MS Activesync is a preferred protocol by enterprises. Courts have struggled with whether the additional control afforded IMAP and MS Activesync protocols are merely the evolution of common email usage and storage, or an erosion of the user's expectation of privacy due to the increased control and transparency to the third-party Internet Service Provider.

For individuals whose emails are downloaded to their computer and deleted from the server, the issue of storage will be with the user's computer rather than cloud storage (i.e., the individual will be subpoenaed for access to their computer rather than a subpoena to the third-party Internet Service Provider for access to the user's email account).

It is also worth noting that every email will have both a sender and a recipient, thus, there will be two sets of records for any email sent. For example, to obtain an email between John Doe and Jane Doe, one can either subpoena Jon Doe's third-party ISP for access to Jon Doe's email account or subpoena Jane Doe's third-party ISP for access to Jane Doe's email account. If John Doe deletes an email sent to Jane Doe, it has no bearing on whether Jane Doe's copy of that email is deleted, and vice versa.

The distinctions between types of email accounts are directly relevant to judicial adjudication of email issues, as shown by the Sixth Circuit's comments in United States v. Warshak. Specifically, the Warshak Court noted the government requested Warshak's ISP prospectively preserve the contents of any existing or future emails to or from Warshak's email account. The ISP thereafter began preserving copies of Warshak's incoming and outgoing emails, which, because Warshak had a POP account, were copies that *would not have existed* absent the government's request:

> Warshak appears to have accessed emails from his NuVox account via POP, or "Post Office Protocol." When POP is utilized, emails are downloaded to the user's personal computer and generally deleted from the ISP's server.

United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010), and n. 14.

A. How Long do Emails Stay on Provider Servers?

There are a plethora of email providers with varying email policies. In 2016, Google announced Gmail has reached more than 1 billion active monthly users. Due to the popularity and prevalence of Gmail, we will focus our discussion on Google's Gmail policies as an example of the benchmark in America today. It is worth noting the level of technological protection offered by less popular email service providers may lag behind Gmail's email privacy

developments and capabilities. It is also worth noting that a number of specialty email providers with cutting-edge privacy-driven services well ahead of Gmail emerged following the concerns of the National Security Agency ("NSA") monitoring. These include Proton mail, which advertises itself as the 'Swiss Bank Account of Email', and houses its servers in a former military command center deep in the Swiss Alps, due to both the physical protection afforded by the location, as well as the legal protection afforded by Switzerland's privacy-friendly laws.

Pursuant to Gmail help topics, Google (Gmail) holds un-deleted email on their servers indefinitely. When an email is "deleted" the email is merely moved to the "Trash" subfolder, and can be fully recovered. Once in the "Trash" folder, the user can chose to further delete the email by choosing "delete forever". If the user deletes an email (moves it to Trash) and does nothing further (does not click "delete forever"), the email remains in the "Trash" subfolder for 30 days, and is thereafter permanently deleted. As to the completeness and permanency of a deleted email (either "deleted forever" or after 30 days in Trash) Google unofficially represents that those emails are actually completely and permanently removed from their system. However, Google admits it keeps offline back-up systems which may take an additional 60 days to catch up. Thus, for good or for bad, emails "permanently deleted" are not immediately permanently deleted.

Google's official policies are not explicit with any definite answers:

> Google keeps multiple backup copies of users' emails so that we can recover messages and restore accounts in case of errors or system failure, **for some limited periods of time**. Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our servers. Deleted messages may also remain on offline backup systems for some limited period of time. This is standard practice in the email industry, which Gmail and other major webmail services follow in order to provide a reliable service for users. We will make reasonable efforts to remove deleted information from offline backup systems as quickly as is practical.

After personally deleting a message (moving to trash) and then clicking "delete forever", Gmail produces a response that "your message has been deleted" with a hyperlink for "learn more". Under the "learn more" tab, Google advises:

> Delete or recover deleted Gmail messages - When you delete a message, it stays in your Trash for 30 days. After that time, it will be permanently deleted from your account and can't be recovered.

As set forth above, that is not exactly accurate because Google can recover the email for some time thereafter through its offline back-up system.

For a variety of reasons, intentional or not, some entity's email accounts have an "auto

delete" function where emails are automatically deleted after a set period of time, usually a function of storage limitations. Such "auto delete" functions must be addressed in consideration of document retention requirements and litigation hold requirements.

B. Are They encrypted? Who Has Access to Them?

What is encryption? In general, an unencrypted email is comparable to sending a postcard in the mail. The information is open to any individual who accesses the postcard during transit. Encryption (Transit Layer Security "TLS" and Pretty Good Privacy "PGP" are some forms of encryption) essentially puts the information in an 'envelope' of security which can only be opened by the recipient. Thus, even if accessed during transit, the content cannot be viewed.

According to the Google Transparency Report, Gmail is encrypted.

> Security is an ongoing challenge where no solution is perfect and progress is incremental. Encryption in transit makes it more difficult to snoop on email and universal encryption of email in transit would be a huge step forward for security and privacy online. But encryption doesn't make snooping impossible. Moreover, email is not only vulnerable in transit—it can also be snooped on after it's delivered. For example, unauthorized parties could still gain access to your email by installing malware on the computer you use to read it.

Encrypted emails require an encryption key. Some email providers advertise an extra layer of protection by not retaining a copy of the key, referred to as end-to-end encryption. Thus, an email is encrypted on a user's computer prior to being sent. The encrypted email passes through the provider's server to the recipient. The email is unencrypted on the recipient's computer. Thus, if for any reason the email provider were to turn over emails on its servers, they would all be encrypted and essentially still secure. The email provider could not be compelled to turn over an encryption key, because they do not possess one.

Pursuant to Google's terms of service, not only does Google have the encryption key, but Google scans emails with automated software to detect spam, as well as for advertising purposes:

> Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

C. Are They Discoverable?

Yes. Federal Rule of Civil Procedure 37 (e) and multiple New Jersey Court Rules address

the discoverability of electronically stored information.

Preserving Electronically Stored Information Under Amended Federal Rule of Civil Procedure 37(e)

As previously noted, in December 2015, Rule 37(e) was amended to address a party's failure to preserve electronically stored information ("ESI"). Rule 37(e) was amended because it did "not adequately address the serious problems resulting from the continued exponential growth [of ESI]" and because federal circuits established significantly different standard for imposing sanctions under Rule 37 that has "caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions." See Rule 37(e) advisory committee's notes to 2015 amendment. Under amended Rule 37(e),

> if electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court: (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or (2) only upon the finding that the party acted with the intent to deprive another arty of the information's use in the litigation may: (A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e)(1) and (2).

New Jersey Court Rule 1:9-2

R. 1:9-2 provides that emails (electronically stored information) are discoverable:

> 1:9-2. For Production of Documentary Evidence and Electronically Stored Information; Notice in Lieu of Subpoena
>
> A subpoena or, in a civil action, a notice in lieu of subpoena as authorized by R. 1:9-1 may require production of books, papers, documents, **electronically stored information**, or other objects designated therein. The court on motion made promptly may quash or modify the subpoena or notice if compliance would be unreasonable or oppressive and, in a civil action, may condition denial of the motion upon the advancement by the person in whose behalf the subpoena or notice is issued of the reasonable cost of producing the objects subpoenaed. The court may direct that the

> objects designated in the subpoena or notice be produced before the court at a time prior to the trial or prior to the time when they are to be offered in evidence and may upon their production permit them or portions of them to be inspected by the parties and their attorneys and, in matrimonial actions and juvenile proceedings, by a probation officer or other person designated by the court. Except for pretrial production directed by the court pursuant to this rule, subpoenas for pretrial production shall comply with the requirements of R. 4:14-7(c).

New Jersey Court Rule 4:23-6

However, R. 4:23-6 provides that Courts may normally not impose sanctions for failing to produce electronically stored information lost as part of routine system operation:

> 4:23-6. Electronically Stored Information. Absent exceptional circumstances, the court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system.

New Jersey Court Rule 4:17-4(d)

R. 4:17-4(d) provides that a party can produce, and refer to, their business records as a response to interrogatory responses requesting information contained in the business records. Thus, parties can produce their email records, and refer to same, in lieu of responding to interrogatories regarding such communications.

> (d) Option to Produce Business Records. When the answer to an interrogatory may be derived or ascertained from or requires annexation of copies of the business records of the party on whom the interrogatory has been served or from an examination, audit or inspection of such business records, or from a compilation abstract or summary based thereon, **or from electronically stored information**, and the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit or inspect such records and to make copies, compilations, abstracts or summaries. A specification shall be in sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained.

New Jersey Court Rule 4:5B-2

R. 4:5B-2 provides that a case management conference can be held to address issues with production of Electronically Stored Information, suggesting ESI may give rise to issues requiring judicial intervention best served by discussion with the Court rather than motion practice.

4:5B-2. Case Management Conferences

> In cases assigned to Tracks I, II, and III, the designated pretrial judge may sua sponte or on a party's request conduct a case management conference if it appears that such a conference will assist discovery, narrow or define the issues to be tried, **address issues relating to discovery of electronically stored information**, or otherwise promote the orderly and expeditious progress of the case... All decisions and directives issued at a case management conference shall be memorialized by order as required by R. 1:2-6. **The order may include provisions for disclosure of discovery of electronically stored information** and any agreements the parties reach for asserting claims of privilege or protection as trial preparation material after production.

New Jersey Court Rule 4:10-2

R. 4:10-2 provides that parties may obtain discovery regarding any relevant, non-privileged matter, including electronically stored information. Under subsection (f), a party need not produce ESI which would impose undue cost or burden. However, on a motion to compel, undue cost or burden will be overcome by a showing of good cause by the proponent.

> 4:10-2. Scope of Discovery
>
> Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:
>
> (a) In General. Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, **electronically stored information**, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. It is not ground for objection that the information sought will be

inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence; nor is it ground for objection that the examining party has knowledge of the matters as to which discovery is sought.

...

(c) Trial Preparation; Materials. Subject to the provisions of R. 4:10-2(d), a party may obtain discovery of documents, **electronically stored information**, and tangible things otherwise discoverable under R. 4:10-2(a) and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including an attorney, consultant, surety, indemnitor, insurer or agent) only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the case and is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation.

...

(f) Claims that Electronically Stored Information is not Reasonably Accessible. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On a motion to compel discovery or for a protective order, the party from whom discovery is sought shall demonstrate that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court nevertheless may order discovery from such sources if the requesting party establishes good cause, considering the limitations of R. 4:10-2(g). The court may specify conditions for the discovery.

New Jersey Court Rule 4:18-1

R. 4:18-1 - permits inspection of ESI. The Rule notes the requesting party may request the format for the ESI to be produced (R. 4:18-1(b)(1)), and if not specifically requested, the ESI will be produced in the form in which it is normally maintained or a reasonably usable form (R. 4:18-1(b)(2)(B)):

(a) Scope. Any party may serve on any other party a request (1) to

> produce and permit the party making the request, or someone acting on behalf of that party, to inspect, copy, test, or sample any designated documents (including writings, drawings, graphs, charts, photographs, sound recordings, images, **electronically stored information**, and any other data or data compilations stored in any medium from which information can be obtained and translated, if necessary, by the respondent into reasonably usable form), or to inspect, copy, test, or sample any designated tangible things that constitute or contain matters within the scope of R. 4:10-2 and that are in the possession, custody or control of the party on whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party on whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of R. 4:10-2.

See also applicable counterparts in the Federal Rules of Civil Procedure 26(a)(1)(A)(ii) (initial disclosures), 33 (interrogatory requests), 34 (document requests), 45(a)(1)(A)(iii) (non-party subpoenas), 30(b)(6) (deponents), and 37(e) (preservation failures).

D. Using Services That Default to Storing Emails and Other Data in the Cloud.

Since the advent of the Internet, the technology industry has been steadily moving away from local storage to remote, server-based storage and processing—what is known as *the cloud*. Look at music and movies: We used to play them from local media, but now they're streamed from servers. You can reap the same advantages of anywhere-access (and the productivity gains that can bring), as well as the reduction of local storage requirements by storing your own documents and media files in the cloud.

Cloud storage and syncing services provide seamless access to all your important data — Word docs, PDFs, spreadsheets, photos, any other digital assets from wherever you are. You no longer need to be sitting at your work PC to see your work files. With cloud syncing you can get to them from your smartphone on the train, from your tablet on your couch, and from the laptop in your hotel room or kitchen. Using cloud storage and syncing services means no more having to email files to yourself or plug and unplug USB thumb drives.

If you don't yet have a service for storing and syncing your data in the cloud, you need one. Which one you choose depends on the kinds of files you store, how much security you need, whether you plan to collaborate with other people, and which devices you use to edit and access your files. It may also depend on your comfort level with computers in general. Some services are extremely user-friendly, while others offer advanced customization for more experienced techies.

What Can Cloud Storage Do for You?

The very best cloud storage solutions play nicely with other apps and services, making the experience of viewing or editing your files feel natural. Especially in business settings, you want your other software and apps to be able to retrieve or access your files, so making sure you use a service that easily authenticates with the other tools you use is a big deal. Box is particularly strong in this regard.

The range of capabilities of cloud-based storage services is incredible. Many of them specialize in a specific area. For example, Dropbox and SugarSync focus on keeping a synced folder accessible everywhere. SpiderOak emphasizes security. Some cloud storage services, such as Apple iCloud, Google Drive and Microsoft OneDrive, are generalists, offering not only folder and file syncing, but also media-playing and device syncing. These products even double as collaboration software, offering real-time document coediting.

Distinct from but overlapping in some cases with cloud storage are online backup services. Some of these, such as Carbonite, are all about disaster recovery, while IDrive combines that goal with syncing and sharing capabilities. If you want to bypass the cloud for your backup, you can still go with local backup software, which saves you the time it takes to upload and download your data.

In fact, most cloud services offer some level of backup, almost as a consequence of their intended function. It follows logically that any files uploaded to a cloud service are also protected from disk failures, since there are copies of them in the cloud. But true online backup plays can back up all of your computer's files, not just those in a synced folder structure. Whereas syncing is about managing select files, backup tends to be a bulk, just-in-case play. With syncing, you pick the documents you might need and keep them in the cloud for easy access. With backup, you back up everything you think you might regret losing.

The Deal With the Cloud

Just to clear up any confusion, the cloud part of cloud-based storage services refers to storing your files somewhere other than your computer's hard drive, usually on the provider's servers. As one tech pundit put it: "There is no Cloud. It's just someone else's computer." Having data in the cloud refers to the ability to access those files through the Internet. Your data is usually encrypted before making the journey over the Internet to the providers' servers, and, while they live on those servers, they're also encrypted. The services don't upload entire files every time they change. They just upload the changes, saving your connection bandwidth.

You can access your cloud files through an app or software installed on your computer (once it's installed, it's usually pretty much invisible), though you need an

Internet connection for it to work. If you temporarily don't have an Internet connection, that's okay. The service will wait until the next time you do have a connection and take care of business then.

Free vs. Paid

Many cloud storage services have a free account that usually comes with some limitations, such as the amount of storage they provide or a size limit on files you can upload. You may prefer services that offer some level of free service (even if it's only 2GB) rather than a time-based trial, because that lets you fully integrate a service into your life for several weeks while you get a feel for how it works and what might go wrong with your particular setup.

What could possibly go wrong? Human error accounts for a good deal of cloud storage tragedies, but the dropped Internet connection is another common troublemaker. One of the benefits of paying for an account is that it usually comes with additional support from the provider, so if anything does go wrong, you can get someone on the phone to help you resolve the issue.

There are many other reasons to pay for cloud storage, from getting a lot more space (a terabyte really doesn't cost all that much anymore) to being able to upload really big files. Other perks of paying for your cloud storage often include increased access to file-version history (meaning you can restore an important business proposal to the version you had before your colleague made a bunch of erroneous changes), more security, or more features for collaboration and working with teams.

Cloud Storage Services

Below is a list of the better cloud storage services tested by PCMag, evaluated on their feature sets, ease of use, stability, and price:

- IDrive
  Very full-featured and versatile.

- SugarSync
  SugarSync is a highly intuitive file-syncing and online backup service, with simple installation and very good control over syncing. However, it is not cheap, it lacks collaboration and privacy features, and its backup performance can be slow.

- Microsoft OneDrive
  OneDrive, the default online storage and syncing service for Windows 10 and Office 365, offers a wealth of powerful features, as well as apps for many platforms.

- SpiderOakONE
  SpiderOakONE's strong focus on privacy is the biggest reason to choose it for online backup and file syncing. It is not great for novices, however, and its premium plans are expensive.

- CertainSafe Digital Safety Deposit Box
  When backing up your sensitive files to the cloud, Certain Safe Digital Safety Deposit Box emphasizes security over all else, but it does not sacrifice ease of use.

- Google Drive
  Part productivity suite and part syncing and online storage service, Google Drive also provides excellent collaborative office-suite functionality.

- Apple iCloud Drive
  Apple's iCloud Drive cloud file-syncing and storage service is a worthwhile service, especially if you're entrenched in Apple's ecosystem. It does not have as many features as the Google and Microsoft counterparts.

- Box (Personal)
  A syncing and storage tool, Box is easy to use and highly customizable, letting you integrate your account with a wide range of apps and services.

- Dropbox
  Dropbox is a simple, reliable, full-featured file-syncing and -storage service with support for real-time online document collaboration, but can be expensive.

E. How to Retain Emails Important to the Case.

If the concern is to retain emails, rather than concerns of hacking, cloud based email storage offers significant benefits. Cloud based email storage offers an attractive alternative to purchasing, maintaining, and upgrading a private server (and the associated IT professionals).

1. Do not delete your emails.

Simply put, to retain emails important to the case, do not delete them from the cloud based storage. For cloud based systems that only delete emails upon instruction, and retain emails indefinitely, simply do not delete the email. If using a POP system, adjust the retention settings to retain the email indefinitely. If emails have been downloaded from a POP system, consider a cloud-based backup system.

2. Download/Print and file.

If you want to retain important emails without leaving a copy on the cloud, download all emails to your local computer and delete the cloud copy. Alternatively, for paper filing only, print the email and delete the cloud copy. Each of these alternatives has its potential issues, as local computer storage is subject to hacking, malware, and physical deterioration/destruction. Similarly, paper filing is subject to theft, misplacement, and physical deterioration/destruction.

3. Web Based Client Portals

Web based client portals is a method of communicating and sharing information with clients, which offer slightly more protection than email. Web based client portals involve uploading communications or information to a third-party portal, which the client then accesses from their computer (or other device). A web based client portal would raise the same issues of third-party possession and storage as stored emails on ISPs; however, web based client portals would help alleviate some concerns of encryption and interception posed by emails. Based on the nature of their business, third-party providers of web based client portals normally have cutting edge security features.