International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 02 February 2022

DOI: 10.47191/ijsshr/v5-i2-14, Impact factor-5.586

Page No: 493-501

How Should an Attorney Deal with High Technology in Their Law Practice?

Donald L. Buresh, Ph.D., J.D., LL.M.
Morgan State University

ABSTRACT: In this essay, the modifications of the American Bar Association Model Rules are discussed with regards to an attorney's responsibilities when dealing with technology. In particular, an attorney is accountable for having a reasonable appreciation of technology functions, mainly when protecting client data or the data entrusted to their care. The paper briefly describes the common law and regulatory law associated with safeguarding data. Compliance with existing ABA Rules and federal and state statutes is paramount. Finally, the article discusses that attorney responsibilities regarding electronic discovery, automated document assembly. Electronic court filing, how a client employs technology, the presenting of digital evidence in a courtroom, and open-source Internet investigations and research tools. The paper concludes that constant vigilance is the order of the day.

KEYWORDS: ABA Model Rules, Automated document assembly, E-discovery, Electronic court filing, Open-source investigations, Presenting digital evidence

Abbreviations:
The following abbreviations are used in this manuscript:

Abbreviation	Description
ABA	American Bar Association
BIPA	Illinois Biometric Information Privacy Act
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
CPA	Colorado Privacy Act
Commission	ABA Commission on Ethics 20/20
CRSLF	ABA Cybersecurity Legal Task Force's Cybersecurity Resources for Small Law Firms
e-filing	Electronic Court Filing
e-discovery	Electronic Discovery
ESI	Electronically Stored Information
FRCP	Federal Rules of Civil Procedure
FTC	Federal Trade Commission
NIST	National Institute for Standards and Technology
OSINT	Open-Source Intelligence
VCDPA	Virginia Consumer Data Privacy Act

INTRODUCTION

In today's society, information technology dominates the communications between individuals, particularly between attorneys and their clients. Computers and mobile devices have connected people, making information a valuable commodity, one that was rarely conceived of a few decades ago. The result of transmitting and storing electronic data is that some individuals attempt to exploit its use, if only because of its ubiquitous presence and ease of access. As a profession, attorneys are required to safeguard the information given to them by their clients. Historically, these acts of protecting client information took the form of keeping client secrets, whether those secrets were verbally or expressly communicated. In particular, in representing their clients, attorneys are charged with maintaining the sanctity of their work product so that they adequately and fairly represent the best interests of their clients.

Modifications to the American Bar Association Model Rules

With the omnipresence of technology, unscrupulous individuals have dedicated their lives to attacking businesses and organizations, including law firms. The reasons for their cyber-attacks are as varied as the individuals themselves. Some people

attack for financial profit, some for revenge regarding a purported hard, some for the belief that secret information should be available to all, and some just for the joy of satisfying their ego that they can break into a system. The greatest threats include spear phishing, ransom ware, compromising emails, or disrupting the flow of goods and services through supply chains.[1] Here, spear phishing is a "method that targets specific individuals or groups within an organization. [Spear phishing] is a potent variant of phishing, a malicious tactic which uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions that cause network compromise, data loss, or financial loss."[2] Second, ransom ware is a "type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid."[3] A supply chain attack, also known as a value-chain or third-party attack, occurs "when someone infiltrates your system through an outside partner or provider with access to your systems and data."[4]

According to the American Bar Association (ABA) Model Rules, attorneys are charged with protecting client data.[5] Model Rule 1.1 addresses the competence of an attorney, Model Rule 1.4 deals with the communications between attorneys and clients, Model Rule 1.6 is concerned with the confidentiality of information, Model Rules 5.1, 5.2, and 5.3 tackle the supervision of attorneys and non-attorneys, and Model Rule 1.15 speaks to safeguarding client property, both tangible and intangible.[6] In the 2012 ABA Annual Meeting, the ABA adopted the recommendations of the ABA Commission on Ethics 20/20 (Commission) regarding technology and confidentiality. The Commission proposed that Comment [8] to Model Rule 1.1 be amended so that attorneys are required to know and keep current with the benefits and risks associated with technology that is relevant to their legal practices.[7] The Commission also suggested that section (c) of Model Rule 1.6 be changed, demanding that attorneys make reasonable efforts to ensure unauthorized disclosure or client information access.[8] Finally, the Commission offered that Comment [18] of Model Rule 1.6 be modified so that attorneys must ensure that attorneys again make reasonable efforts to analyze the risk associated with the client data in their possession.[9]

Model Rule 1.4 addresses client communications and an attorney's use of technology. Model Rule 1.4 obliges attorneys to communicate with clients how their goals and objectives will be achieved, particularly technology employment. Clients must be informed that an attorney's use of technology may demand the client's informed consent. If there is a material breach of client information, Model Rule 1.4 insists that a client be given notice.[10]

Model Rule 5.1 and 5.2 describe the responsibilities of partners, managers, and supervisory lawyers and the responsibilities of attorneys being supervised concerning the duties of competence and confidentiality. Model Rule 5.3 was changed to nonlawyer assistants. The term "assistants" in Model Rule 5.3 was expanded to the assistance of all outsourced staff levels and services, including copying and legal services.[11] Under the revised ABA Model Rules, attorneys must engage in reasonable safeguards such as due diligence, contractual requirements, supervision, and monitoring of lawyers and nonlawyers alike both inside and outside a law firm to deliver their services.[12]

Model Rule 1.5 demands that attorneys safeguard clients' money, property, and third parties entrusted to attorneys. Rule 1.15 was extended to apply to attorneys' electronic data held in trust.[13] According to ABA Formal Opinion 483 dated October 17, 2018, safeguarding client information in paper and electronic form is paramount. These duties include:

- The responsibility to monitor a breach;
- The requirement to stop a breach and restore system integrity; and
- A commitment to determine why the breach occurred.

When applying Model Rule 1.9(c) to Model Rule 1.4, the Commission that an attorney is required to notify a client of a breach as a matter of ethics.[14] Opinion 483 included an examination of the duties of a lawyer about

---

[1] David G. Reis, *Cybersecurity for Attorneys: The Ethics of Securing Your Virtual Practice*, LAW PRACTICE TODAY (Oct. 15, 2021), *available at* https://www.lawpracticetoday.org/article/cybersecurity-for-attorneys-the-ethics-of-securing-your-virtual-practice/.
[2] *Spear Phishing*, TREND MICRO (n.d.), *available at* https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing.
[3] *Ransomware, TREND MICRO (n.d.), available* at https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
[4] Maria Korolov, *Supply Chain Attacks Show Why You Should Be Wary of Third-Party Providers*, CSO UNITED STATES (Dec. 27, 2021), *available at* https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.
[5] David G. Reis, *supra*, note 1.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*

How Should an Attorney Deal with High Technology in Their Law Practice?

- Hardware and software systems;
- Accessing the data and files of a client;
- Using virtual meeting software including video conferencing;
- Employing virtual document and data exchange platforms; and
- Intelligent speakers, virtual assistants, and other electronic listening devices.[15]

The Opinion concluded by attorneys that employ electronic technologies should understand their advantages and disadvantages, including their limitations and the likelihood of a breach.

Common-Law and Regulatory Law

Common law and contractual duties are defined and explained in the case law. These duties encompass competence, communication, and confidentiality, where a breach of these duties can result in a malpractice suit. Finally, federal and state statutes may specify how attorneys and law firms should protect client data, particularly for financial and health industries and other industries.[16] State laws include the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA),[17] [18] the Virginia Consumer Data Privacy Act (VCDPA),[19] the Colorado Privacy Act (CPA),[20] as well as the Nevada[21] and Maine[22] privacy laws. Buresh described these state laws in greater detail.[23] Currently, there is no comprehensive federal privacy law.[24] Attorneys may also be responsible for the privacy and security of personal information, including incident responses and notice of incident responses.[25] The safeguarding of data includes clients, employees, customers, opposing parties and their employees, and sometimes even witnesses.[26]

Complying with the Duties

This section of this essay aims to discuss cybersecurity issues and the safeguarding of a virtual practice.

Cybersecurity Issues

Cybersecurity is the "application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks."[27] Cybersecurity attempts to reduce and mitigate the risks of cyber-attacks by protecting against the unauthorized use and exploitation of systems, networks, and technologies. According to Reis, cybersecurity should identify, protect, detect, respond, and recover from a cyber-attack.[28] In other words, cybersecurity is dedicated to safeguarding the confidentiality, integrity, and availability of data.[29] Reis further opined that recently the emphasis is on detection, response, and recovery.[30]

Security begins at home. First, a law firm should inventory its information assets to determine what data should be protected and what information is likely to target a breach.[31] Once the information to be protected is known, steps should be taken to implement and maintain a comprehensive cybersecurity program that employs electronic safeguards and physical restraints against unauthorized access and use.[32] The program should include an incident response plan that describes what a law firm should do in

---

[15] *Id.*
[16] Donald L. Buresh, *Legal, Marketing, and Advertising Issues with Big Data*, 1 JOURNAL OF BIG DATA RESEARCH 2, 38-52 (Jan. 2022), available at DOI: 10.14302/issn.2768-0207.jbr-21-4048.
[17] Donald L. Buresh, *A Comparison between the European and American Approaches to Privacy*, 6 INDONESIAN J. OF INT. AND COMP. L. 253, (2019), https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=.
[18] *California Privacy Rights Act of 2020*, PROP. 24, *available at* https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.
[19] *Virginia Consumer Data Protection Act of 2021*, SB1392, *available at* https://legiscan.com/VA/text/SB1392/id/2328317.
[20] *Colorado Privacy Act of 2021*, SB21-190, *available at* https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf.
[21] *Nevada Privacy Law*, NRS 603A.300 – 603A.360 AS AMENDED BY SB 220, *available at* https://www.leg.state.nv.us/nrs/nrs-603a.html.
[22] *An Act To Protect the Privacy of Online Customer Information*, LD 946, *available at* https://www.mainelegislature.org/legis/bills/bills_129th/billtexts/SP027501.asp.
[23] Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECH. L. J. 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
[24] *Id.*
[25] Donald L. Buresh, *supra*, note 16.
[26] David G. Reis, *supra*, note 1.
[27] IT Governance Staff, *What is Cyber Security? Definition and Best Practices*, IT GOVERNANCE (n.d.), *available at* https://www.itgovernance.co.uk/what-is-cybersecurity.
[28] David G. Reis, *supra*, note 1.
[29] Bill Bernard, *What Is CIA (in Cybersecurity)?*, DEEPWATCH (Dec. 21, 2020), *available at* https://www.deepwatch.com/blog/cia-in-cybersecurity/.
[30] David G. Reis, *supra*, note 1.
[31] Donald L. Buresh, *supra*, note 16.
[32] *Id.*

the presence of a breach. Other issues that should be part of a comprehensive cybersecurity plan are the conditions when protected data is disclosed to third parties and at the appropriate time when data should be destroyed.[33] The National Institute for Standards and Technology (NIST), the ABA Cybersecurity Legal Task Force's Cybersecurity Resources for Small Law Firms (CRSLF), and the Federal Trade Commission (FTC) website are sources that can be employed in generating a comprehensive cybersecurity plan.[34] The advantage of using the CRSLF is that it contains references to ABA, government, and industry resources.[35] Microsoft Office, Google Workspace, and cloud management platforms also possess a high level of data security that may be particularly advantageous for small to medium law firms. When selecting cloud services, attorneys should review the safety features of the cloud to ensure that they comply with the ABA Model Rules, the common law, and federal and state statutes.[36]

Safeguarding a Virtual Practice

An attorney can employ various practical steps to protect client data. Lawrence observed that when contracting with a client, an attorney should:

- Make sure that the contract is in writing;
- Keep the agreement simple to understand;
- When agreeing, deal with the person who has the authority to contract;
- Correctly identify each party in the contract;
- State specifically all of the details of the bargain;
- Stipulate the payment obligations for all parties;
- Agree on the circumstance where the contract may be terminated;
- Decide on a way or method to resolve disputes;
- Select the state law that will govern the contract; and
- Keep the contract confidential.[37]

These ten steps are relevant when dealing with cybersecurity issues that affect client data. It is essential that attorneys adhere to the ABA Model Rules, the common law, and federal and state statutes and that the client and relevant third parties understand their duties and obligations from a cybersecurity perspective.[38]

According to Reis, practical cybersecurity demands a continuing focus on a periodic review of the cybersecurity plans and measures adopted and taken by a law firm.[39] This includes:

- Managing and minimizing the data collected, used, stored, disseminated, and destroyed;
- Employing reasonable and industry-standard configurations for servers, laptops, and mobile devices;
- Limiting and controlling the use of administrative privileges;
- Using strong passwords and a password manager;
- Using multifactor authentication, particularly for administrative accounts and remote access to systems; and
- Limiting and segmenting access to sensitive client data.[40]

Other cybersecurity measures are:

- Patching operating systems, firmware, applications, and plug-ins;
- Providing secure electronic communication such as employing encrypted email when appropriate;
- Filtering websites for spam;
- Employing strong encryption for computers and mobile devices;
- Requiring that attorneys, assistants, nonlegal staff, and third-parties use secure wireless networks by employing virtual private networks (VPNs);
- Keeping security application and software current or up to date; and
- Periodically conducting cybersecurity assessments and remediation.[41]

[33] *Id.*
[34] David G. Reis, *supra*, note 1.
[35] *Id.*
[36] *Id.*
[37] Bethany K. Laurence, *Ten Tips for Making Solid Business Agreements and Contracts*, NOLO (n.d.), *available at* https://www.nolo.com/ legal-encyclopedia/make-business-contract-agreement-30313.html.
[38] *Id.*
[39] David G. Reis, *supra*, note 1.
[40] *Id.*
[41] *Id.*

Specific Cybersecurity Practices

There are several specific cybersecurity practices that a law firm may need to address, depending on the type of legal practice. These include electronic discovery and its issues, automated document assembly, electronic court scheduling and file-sharing technologies, understanding how a client uses technology, presenting evidence using digital information in a courtroom, and open-source Internet investigations and research tools.

Electronic Discovery

Electronic discovery (e-discovery) is the "electronic aspect of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a law suit or investigation."[42] In terms of e-discovery, ESI includes emails, documents, presentations, databases, voicemail, audio and video files, social media, and websites.[43] In other words, ESI is any information stored on electronic media and is available electronically.

For attorneys engaged in litigation, the problem with e-discovery is that what may be found in the process is not necessarily known. If specific information were known in litigation, it would be an easy task to protect that information. An issue with e-discovery is that information about some facts of a case may not be known by the plaintiff or the defendant. Also, given the onslaught of technology, the sheer volume of information can be staggering. Hundreds of thousands or more emails and other electronic documents may be unearthed during an e-discovery process. The result is that attorneys must be diligent in protecting electronic data because someone may inadvertently disclose personal information unrelated to the case or data protected by the attorney-client privilege.

The Federal Rules of Civil Procedure (FRCP) 26(b) (2)(C) states that when required: "[o]n motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

i. the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
ii. the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
iii. the proposed discovery is outside the scope permitted by Rule 26(b)(1)."[44]

Even if the court limits e-discovery based on FRCP 26(b)(2)(C), the amount of information collected and digested by a litigant may be massive. Because of the risk that information not related to a case or protected attorney-client information will be disclosed, it is essential that electronic information be safeguarded by all reasonable means.

Automated Document Assembly

Automated documentation or automated document assembly is the "process of using automation to decrease the amount of human intervention required to create, maintain, and share software documentation, cutting down costs, improving quality and freeing humans from tedious, error-prone work."[45] There are three reasons why attorneys may favor automated documentation, including:

- Manual documentation writing is slow, error-prone, and time-consuming;
- Documentation can quickly become outdated;
- The cost and time of manually creating and maintaining documentation could be better spent on other activities.[46]

The advantages of automating documentation generation are manifold, including integrating documentation with the documentation of third parties, the ability to employ reusable templates, workflows that can be intelligible, and compliance with federal and state laws and regulations that may prevent inadvertent violations.[47] Other advantages of automated document assembly for a law firm include savings of time and resources, increased control over a case, fast and secure digital sharing, and an improved client experience.[48] Document automation may also provide mobile access to e-discovery data, the ability to manage the data discovered electronically intelligently, and integration with an existing legal software.[49]

There are several disadvantages of automated documentation stemming from the volumes of documents being automated. During litigation, hundreds of thousands of documents are likely to be the object of the automated effort. In other words, automated document assembly shares many of the risks of an e-discovery. Also, incorrect documentation may be generated and propagated to

[42] CDS Staff, *The Basics: What is e-Discovery?*, COMPLETE DISCOVERY SOURCE (n.d.), *available at* https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/.
[43] *Id.*
[44] Legal Information Institute Staff, *Rule 26. Duty to Disclose: General Provisions Governing Discover*, LEGAL INFORMATION INSTITUTE (n.d.), *available at* https://www.law.cornell.edu/rules/frcp/rule_26.
[45] Carlos Schults, *Automated Documentation: What It Means and 3 Tools to Help*, SUBMAIN (Jul. 23, 2019), *available at* https://blog.submain.com/automated-documentation-3-tools/.
[46] *Id.*
[47] Bigtincan Staff, *What is Document Automation?*, BIGTINCAN, CORP. (n.d.), *available at* https://www.bigtincan.com/company/.
[48] *Id.*
[49] *Id.*

third parties with automated documentation. In this instance, there is the possibility that a miscarriage of justice could occur, particularly when the plaintiff or the defendant does not uncover then incorrect documentation.

Another issue with automated documentation includes overestimating the power of document automation software.[50] Second, a law firm may only try one automated documentation software package rather than evaluate multiple packages.[51] Third, a law firm may expect too little from its automated documentation software. Fourth, automated documentation software may be selected based on the action of a demo and not the actual software. Finally, a law firm may pick software that locks the organization into a particular software application.[52] In particular, Model Rule 1.5 demands that attorneys safeguard clients' money, property, and third parties entrusted to attorneys.[53] ABA Formal Opinion 483 requires that an attorney promptly inform a client of a breach.[54] The automated documentation software must adhere to the stringent requirements specified by the ABA Model Rules and federal and state law statutory requirements.

Electronic Court Filing

Electronic court filing (e-filing) is the automated transmission of legal documents from a party to the court, court to a party, or party to another party or individual.[55] Because court documents are being filed electronically, they are being communicated over the Internet. In other words, a given document may be momentarily received and transmitted over five or more servers. Once a court document resides on a server if only for a moment, a cybercriminal can attack the server and gather the document. Thus, it is essential that documents received and transmitted over the Internet be encrypted to preserve the confidentiality and integrity of the information. If this is not accomplished, a law firm may be liable for violating Model Rules 1.5 and 1.6, where attorneys must safeguard client information and property. Law firms could also be liable for violating federal and state privacy laws. Thus, securing documents received and transmitted over the Internet is paramount.

How a Client Employs Technology

There is a variety of software applications that clients may employ. Many of these applications have been breached. For example, consider the SolarWinds supply chain attack on September 12, 2019.[56] A supply chain attack is a hacking technique where an adversary inserts malicious code or components into a trusted software application.[57] The idea of the attack was to compromise a single supplier so that hackers may hijack its distribution system, converting any application sold, including hardware and software, into Trojan horses.[58] Because of the high-profile nature of SolarWinds software, Congressional hearings were held to determine the extent of the breach. On February 26, 2021, the House committees on Homeland Security and Oversight and Report conducted a joint hearing regarding the SolarWinds security breach.[59] On March 10, 2021, the House Committee on Appropriations and the Homeland Security Subcommittee discussed upgrading federal cybersecurity software.[60] On March 18, 2021, the Senate Homeland Security and Governmental Affairs Committee held a similar hearing on determining how to respond to the attack.[61]

The SolarWinds attack had far-reaching implications. Multiple billion-dollar companies used the SolarWinds software. Law firms that represented these companies may have inadvertently exposed themselves to the breach. The ABA Model Rule 1.4 explicitly addresses client communications and an attorney's use of technology.[62] Model Rule 1.5 demands that attorneys protect the money and property of clients and third parties.[63] Formal Opinion 483 specifies that attorneys must monitor a breach, stop a

---

[50] Epsillion Staff, *Five Common Mistakes Professionals Make When Choosing Document Automation Software*, EPSILLION SOFTWARE, LTD. (Jul. 26, 2020), *available at* https://www.epsillion.com/blog/commonMistakesChooseDocumentAutomationSoftware.php.
[51] *Id.*
[52] *Id.*
[53] David G. Reis, *supra*, note 1.
[54] *Id.*
[55] *See generally*, JAMES E. MCMILLAN, J. DOUGLAS WALKER, & LAWRENCE B. WEBSTER, A GUIDEBOOK FOR ELECTRONIC COURT FILING (West Group, Inc. 1998), *available at* https://www.srln.org/system/files/attachments/A_Guidebook_for_Electronic_Court_Filing.pdf.
[56] Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Attack*, NATIONAL PUBLIC RADIO (NPR) (Apr. 16, 2021), *available at* https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
[57] Andy Greenberg, *Hacker Lexicon: What Is a Supply Chain Attack?*, WIRED (May 31, 2021), *available at* https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.
[58] *Id.*
[59] Vijay A. D'Souza, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, WATCHBLOG (Apr. 22, 2021), *available at* https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
[60] *Id.*
[61] *Id.*
[62] David G. Reis, *supra*, note 1.
[63] *Id.*

breach and restore system integrity, and determine why a breach occurred.[64] If a client of a law firm experiences a breach, a law firm has access to its client's system. The law firm's computer systems may also be breached, and the law firm's other clients may be affected by the breach because a cyber-attacker may have access to their data. This is an untenable situation for a law firm. Thus, a law firm must monitor the cyber activities of its clients to ensure that its other clients are not affected by a cyber breach experienced by a specific client.

Presenting Digital Evidence in a Courtroom

When a party presents digital evidence in a courtroom, the evidence must be accurate and firmly established its chain of custody.[65] The evidence presented in court must be formatted so that the court systems can accept the data and accurately display it.[66] ABA Model Rule 1.4, mainly if the court employs document and data exchange applications. Although, in general, the party's attorneys are not responsible for court systems, they are accountable for ensuring that the court systems display their evidence accurately and precisely, thereby ensuring the integrity of the data.

Open-Source Internet Investigations and Research Tools

Open-source Internet investigations gather data that is freely available on the Internet. Examples include:

- Public records databases;
- Government reports, documents, and websites;
- The Internet;
- Newspapers, TV, radio, magazines, and websites;
- Social networks, social media sites, user account profiles, posts, and tags;
- Maps and commercial imagery;
- Photos, images, videos; and
- The dark web.[67]

In collecting data from an open-source intelligence (OSINT) source, an attorney must ensure that the source contains accurate information. Data integrity can be achieved by various means, including cross-checking the data. Once the data has been collected, establishing the chain of custody is paramount. If there are breaks in the chain of custody, this fact casts dispersions on the data quality. Senior attorneys should supervise the collection, storage, use, dissemination, and destruction of OSINT to ensure compliance with Model Rules 5.1, 5.2, and 5.3.[68]

There are various OSINT tools that are readily available. For example, the OSINT framework focuses on gathering information from free Internet tools or resources.[69] The idea behind the framework is to help people discover free OSINT resources.[70] Information that may be obtained using the OSINT Framework include username, email address, domain name, IP address, social networks, instant messaging, people search engines, business records, the dark web, malicious file analysis, and a host of other functions.[71] As previously observed, an attorney should be careful when employing any of these OSINT tools because the quality of the data obtained is directly proportional to the reliability of the tool employed.

CONCLUSION

In conclusion, the responsibilities of attorneys regarding the receiving and transmitting of electronic data are manifold. The ABA Model Rules seemingly require that attorneys safeguard the confidentiality, integrity, availability, and security of client data and the data of third parties that are inadvertently collected. Senior attorneys are responsible for supervising junior attorneys and nonlawyer assistants and all outsourced staff levels and services, including copying and legal services.[72] It is a difficult task, but one that must be accomplished if personal information is to remain protected. Nothing short of constant vigilance will suffice.

---

[64] *Id.*
[65] Digital Evidence in the Courtroom: A Guide For Law Enforcement and Prosecutors, U.S. Department of Justice (Jan. 2007), available at https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors.
[66] *Id.*
[67] Michael Kissiah, *Open Source Intelligence Tools (OSINT)*, EINVESTIGATOR.COM (Jan. 14, 2022), *available at* https://www.einvestigator.com/open-source-intelligence-tools/.
[68] David G. Reis, *supra*, note 1.
[69] *OSINT Framework*, GITHUB.COM (n.d.), *available at* https://osintframework.com/.
[70] *Id.*
[71] *Id.*
[72] *Id.*

REFERENCES

1) David G. Reis, Cybersecurity for Attorneys: The Ethics of Securing Your Virtual Practice, LAW PRACTICE TODAY (Oct. 15, 2021), available at https://www.lawpracticetoday.org/article/cybersecurity-for-attorneys-the-ethics-of-securing-your-virtual-practice/.
2) Spear Phishing, TREND MICRO (n.d.), available at https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing.
3) Ransomware, TREND MICRO (n.d.), available at https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
4) Maria Korolov, Supply Chain Attacks Show Why You Should Be Wary of Third-Party Providers, CSO UNITED STATES (Dec. 27, 2021), available at https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.
5) Donald L. Buresh, Legal, Marketing, and Advertising Issues with Big Data, 1 JOURNAL OF BIG DATA RESEARCH 2, 38-52 (Jan. 2022), available at DOI: 10.14302/issn.2768-0207.jbr-21-4048.
6) Donald L. Buresh, A Comparison between the European and American Approaches to Privacy, 6 INDONESIAN J. OF INT. AND COMP. L. 253, (2019), https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=.
7) California Privacy Rights Act of 2020, PROP. 24, available at https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.
8) Virginia Consumer Data Protection Act of 2021, SB1392, available at https://legiscan.com/VA/text/SB1392/id/2328317.
9) Colorado Privacy Act of 2021, SB21-190, available at https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf.
10) Nevada Privacy Law, NRS 603A.300 – 603A.360 AS AMENDED BY SB 220, available at https://www.leg.state.nv.us/nrs/nrs-603a.html.
11) An Act To Protect the Privacy of Online Customer Information, LD 946, available at https://www.mainelegislature.org/legis/bills/bills_129th/billtexts/SP027501.asp.
12) Donald L. Buresh, Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?, 38 SANTA CLARA HIGH TECH. L. J. 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
13) Donald L. Buresh, supra, note 16.
14) David G. Reis, supra, note 1.
15) IT Governance Staff, What is Cyber Security? Definition and Best Practices, IT GOVERNANCE (n.d.), available at https://www.itgovernance.co.uk/what-is-cybersecurity.
16) Bill Bernard, What Is CIA (in Cybersecurity)?, DEEPWATCH (Dec. 21, 2020), available at https://www.deepwatch.com/blog/cia-in-cybersecurity/.
17) Donald L. Buresh, supra, note 16.
18) Bethany K. Laurence, Ten Tips for Making Solid Business Agreements and Contracts, NOLO (n.d.), available at https://www.nolo.com/ legal-encyclopedia/make-business-contract-agreement-30313.html.
19) CDS Staff, The Basics: What is e-Discovery?, COMPLETE DISCOVERY SOURCE (n.d.), available at https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/.
20) Legal Information Institute Staff, Rule 26. Duty to Disclose: General Provisions Governing Discover, LEGAL INFORMATION INSTITUTE (n.d.), available at https://www.law.cornell.edu/rules/frcp/rule_26.
21) Carlos Schults, Automated Documentation: What It Means and 3 Tools to Help, SUBMAIN (Jul. 23, 2019), available at https://blog.submain.com/automated-documentation-3-tools/.
22) Bigtincan Staff, What is Document Automation?, BIGTINCAN, CORP. (n.d.), available at https://www.bigtincan.com/company/.
23) Epsillion Staff, Five Common Mistakes Professionals Make When Choosing Document Automation Software, EPSILLION SOFTWARE, LTD. (Jul. 26, 2020), available at https://www.epsillion.com/blog/commonMistakesChooseDocumentAutomationSoftware.php.
24) See generally, JAMES E. MCMILLAN, J. DOUGLAS WALKER, & LAWRENCE B. WEBSTER, A GUIDEBOOK FOR ELECTRONIC COURT FILING (West Group, Inc. 1998), available at https://www.srln.org/system/files/attachments/A_Guidebook_for_Electronic_Court_Filing.pdf.
25) Dina Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Attack, NATIONAL PUBLIC RADIO (NPR) (Apr. 16, 2021), available at https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
26) Andy Greenberg, Hacker Lexicon: What Is a Supply Chain Attack?, WIRED (May 31, 2021), available at https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.

27) Vijay A. D'Souza, SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic), WATCHBLOG (Apr. 22, 2021), available at https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
28) Digital Evidence in the Courtroom: A Guide For Law Enforcement and Prosecutors, U.S. Department of Justice (Jan. 2007), available at https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors.
29) Michael Kissiah, Open Source Intelligence Tools (OSINT), EINVESTIGATOR.COM (Jan. 14, 2022), available at https://www.einvestigator.com/open-source-intelligence-tools/.
30) OSINT Framework, GITHUB.COM (n.d.), available at https://osintframework.com/.