Texas A&M Journal of Property Law

Volume 4
Number 5 *Symposium Edition - Artificial Intelligence and the Legal Profession*

Article 1

2018

# Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers

Jan L. Jacobowitz
*University of Miami School of Law*, jjacobowitz@law.miami.edu

## Recommended Citation

Jan L. Jacobowitz, *Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers*, 4 Tex. A&M J. Prop. L. 407 (2018).
Available at: https://doi.org/10.37419/JPL.V4.I5.1

# Happy Birthday Siri!
# Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers

*By Jan L. Jacobowitz and Justin Ortiz*[†]

> *"We're working on having lawyers teach the computer to think like a lawyer. That would be a huge step for humanity. With legal tech, there will be new jobs, and we can embrace a very happy future in the law. This is a new frontier."*
>
> —Andrew Arruda[1]

> *"There is no threshold that makes us greater than the sum of our parts, no inflection point at which we become fully alive. We can't define consciousness because consciousness does not exist. Humans fancy that there's something special about the way we perceive the world, and yet we live in loops as tight and as closed as the [AI] hosts do, seldom questioning our choices, content, for the most part, to be told what to do next."*
>
> —Dr. Robert Ford, Westworld[2]

> "*I am very honored and proud of this unique distinction. This is historical to be the first robot in the world to be recognized with a citizenship.*"
>
> —Sophia, the first robot to be granted citizenship in Saudi Arabia[3]

Table of Contents

[†] Jan L. Jacobowitz is a Lecturer in Law and Director of the Professional Responsibility & Ethics Program (PREP) at the University of Miami School of Law. Justin Ortiz is a Miami Law and PREP alumnus who is currently practicing law in Kansas City, Missouri. The authors are tremendously grateful to PREP Fellow and research assistant extraordinaire, Nicole Chipi, for her valuable input and assistance with the writing of this article.

[1] Julie Sobowale, *How Artificial Intelligence is Transforming the Legal Profession,* ABA J. (Apr. 2016), http://www.abajournal.com/magazine/article/how_artificial_intelligence_is_transforming_the_legal_profession [https://perma.cc/97JD-H8N3].

[2] *Dr. Robert Ford*, Quote Catalog, https://quotecatalog.com/communicator/dr-robert-ford/ [https://perma.cc/P9GG-GRX8] (last visited Feb. 25, 2018).

[3] Anthony Cuthbertson, *Tokyo: Artificial Intelligence 'Boy' Shibuya Mirai Becomes World's First AI Bot to Be Granted Residency*, Newsweek (Nov. 6, 2017, 4:52 AM), http://www.newsweek.com/tokyo-residency-artificial-intelligence-boy-shibuya-mirai-702382 [https://perma.cc/Q5L2-GTQM].

DOI: https://doi.org/10.37419/JPL.V4.I5.1

## I. INTRODUCTION

If we ask six-year-old Siri[4] to create a guest list for a party to celebrate the tenth anniversary of the iPhone,[5] Siri might include invites (or e-vites) for Alexa, Bixby, Cortana, and Google's Assistant. Whether the guests would be able to "mingle" with one another is unclear, but human invitees could communicate with each of Siri's "smart" technology guests.[6]

Smart devices and Artificial Intelligence ("AI") programs have altered the way we live—both in our personal and professional lives. Through these platforms, we can communicate simultaneously with a large number of people located at multiple locations throughout the world.[7] We can access both our personal and business emails and files from almost anywhere on the planet.[8] Free public WiFi hot-spots are

[4] *How Apple's Siri Got Her Name*, WEEK (Mar. 29, 2012), http://theweek.com/articles/476851/how-apples-siri-got-name (Siri is a Norwegian name which translates to "beautiful woman who leads us to victory." Siri, Inc. was founded in 2007, and the Siri app launched in 2010. Apple, Inc. purchased Siri, Inc., and shortly thereafter, Apple introduced Siri with the iPhone 4s on October 4, 2011.); *see also* Luke Dormehl, *Today in Apple History: Siri Debuts on iPhone 4s*, CULT MAC (Oct. 4, 2017, 5:00 AM), https://www.cultofmac.com/447783/today-in-apple-history-siri-makes-its-public-debut-on-iphone-4s/ [https://perma.cc/7PRT-NHF9].

[5] Dan Grabham & Robert Jones, *History of the iPhone 2007–2017: The Journey to iPhone X: A Decade Is a Long Time in Smartphones*, T3 (Jan. 10, 2018), https://www.t3.com/features/a-brief-history-of-the-iphone [https://perma.cc/M6ZM-Q35N].

[6] Scott Rosenberg, *Voice Assistants Aren't So Easy to Fire*, WIRED (Oct. 11, 2017, 6:40 AM), https://www.wired.com/story/voice-assistants-arent-so-easy-to-fire/ [https://perma.cc/YXS4-B628].

[7] *See* Audrey Willis, *6 Ways Social Media Changed the Way We Communicate*, HIGHER ED MKTG. J. (Aug. 15, 2017), https://perma.cc/H78D-SD2N.

[8] *See* Michael Muchmore & Jill Duffy, *The Best Cloud Storage and File-Sharing Services of 2017*, PC MAG (Jan. 23, 2018, 1:03 PM), https://www.pcmag.com/roundup/306323/the-best-cloud-storage-providers-and-file-syncing-services [https://perma.cc/95E5-J34D].

as numerous as the apps that are available for our smartphones.[9] We can communicate with technological assistants that perform our tasks and answer our questions.[10] In fact, technology makes it possible for us to conveniently use the same device for personal and professional purposes. But the increased sophistication and convenience of these technologies have also created vulnerabilities for users who fail to learn how the technology functions and to employ reasonable precautions. These vulnerabilities become especially problematic in the practice of law.[11]

The legal community has confronted the challenge of adapting to technological innovation throughout its history (albeit, generally somewhat behind the technological curve),[12] but artificial intelligence and its use in the legal profession is relatively new. While many lawyers use smartphones and virtual assistants, the arrival of new "smart machines" has baffled many in the legal profession.[13]

ROSS, sometimes referred to as the "robot" lawyer, was merely a glint in his developers' eye when Apple gave birth to the iPhone.[14] Today, ROSS Intelligence offers AI driven research to legal practitioners.[15] A slew of other AI vendors also provide attorneys with legal support services including legal research, contract review, litigation strategy, litigation funding decisions, e-discovery, and jury selection. The use of services provided by these vendors are slowly gaining acceptance in the legal community.[16] AI promises increased efficiencies, but strikes fear into those who worry about robot lawyers replacing humans. In fact, automated "bots" like DoNotPay, a bot developed by

[9] Mari Silbey, *US Cable WiFi Hotspots Near 17 Million*, LIGHT READING (July 6, 2016), http://www.lightreading.com/cable/cable-wi-fi/us-cable-wifi-hotspots-near-17-million/d/d-id/724584 [https://perma.cc/FKR5-HK6V].

[10] *See generally* Sharon D. Nelson & John W. Simek, *Are Alexa and Her Friends Safe to Use in Your Law Office? The Pros and Cons of Personal Assistants*, SENSEI ENTERS., INC. (2017), https://senseient.com/wp-content/uploads/Alexa-and-other-PDAs.pdf [https://perma.cc/75LC-4AJB].

[11] *See id.*

[12] *See* Jan L. Jacobowitz & Danielle Singer, *The Social Media Frontier: Exploring a New Mandate for Competence in the Practice of Law*, 68 U. MIAMI L. REV. 445, 447–54 (2014); *see also* Jane Croft, *Artificial Intelligence Disrupting The Business Of Law,* FIN. TIMES (Oct. 5, 2016), https://www.ft.com/content/5d96dd72-83eb-11e6-8897-2359a58ac7a5 [https://perma.cc/5XD6-RPRX] ("Its traditional aversion to risk has meant the legal profession has not been in the vanguard of new technology.").

[13] Robert Ambrogi, *Fear Not, Lawyers, AI Is Not Your Enemy*, ABOVE THE L. (Oct. 30, 2017, 3:00 PM), https://abovethelaw.com/2017/10/fear-not-lawyers-ai-is-not-your-enemy/ [https://perma.cc/E7TA-EZCN].

[14] *ROSS Intelligence Gains $8.7m in Major Series A Funding*, ARTIFICIAL LAW (Oct. 11, 2017), https://www.artificiallawyer.com/2017/10/11/ross-intelligence-gains-8-7m-in-major-series-a-funding/ [https://perma.cc/N82D-7YLZ].

[15] *Id.*

[16] *See* Matthew L. Willens, *How Artificial Intelligence Is and Will Change the Practice of Law*, 21ST CENTURY TECH (May 2, 2017), http://www.21stcentech.com/artificial-intelligence-change-practice-law/ [https://perma.cc/FS3J-2CW3]; *see also* Sobowale, *supra* note 1.

a British teenager that has "represented" thousands of individuals who have successfully contested their traffic tickets, demonstrate that some of these fears are not unfounded.[17]

Regardless of whether AI is embraced or feared, the use of AI implicates the Rules of Professional Conduct and a lawyer's corresponding ethical duties to his client. Whether a lawyer's use of AI will become tantamount to competent representation remains to be seen, but there is no doubt that the current use of AI has already raised the specter of legal ethics landmines, with issues such as client consent, confidentiality, and supervision already in play.[18] Moreover, a debate has ensued as to whether the use of an AI machine or "bot" constitutes the unauthorized practice of law.

This Article explores the history of AI and the advantages and potential dangers of using AI to assist with legal research, administrative functions, contract drafting, case evaluation, and litigation strategy. This Article also provides an overview of security vulnerabilities attorneys should be aware of and the precautions that they should employ when using their smartphones (in both their personal and professional lives) in order to adequately protect confidential information.[19] Finally, this Article concludes that lawyers who fail to explore the ethical use of AI in their practices may find themselves at a professional disadvantage and in dire ethical straits.[20]

The first part of this Article defines the brave new world of AI and how it both directly and indirectly impacts the practice of law. The second part of this Article explores legal ethics considerations when selecting and using AI vendors and virtual assistants. The third part outlines technology risks and potential solutions for lawyers who seek to embrace smartphone technology while complying with legal ethics obligations. The Article concludes with an optimistic eye toward the future of the legal profession.

[17] Alvaro Dominguez, *Rise of the Robolawyers: How Legal Representation Could Come to Resemble Turbotax*, THE ATLANTIC (Apr. 2017), https://www.theatlantic.com/magazine/archive/2017/04/rise-of-the-robolawyers/517794/ [https://perma.cc/MMU7-XKYY].

[18] *See* Wendy Wen Yu Chang, *Competence: What Are the Ethical Implications of Artificial Intelligence Use in Legal Practice?,* 33 LAW. MAN. PROF. CONDUCT 284 (May 17, 2017), https://aprl.net/wp-content/uploads/2016/09/3.-Ethical-Implications-of-AI.pdf [https://perma.cc/RXM3-D4U6] [hereinafter *Ethical Implications*].

[19] Throughout the article, various companies and programs are referenced as examples of available technology. These companies are mentioned solely to provide a reflection of the types of technology available at the time of the writing of this article. The authors' mention of a company is in no way an endorsement of that company or a particular type of technology.

[20] *See* Nicole Black, *Artificial Intelligence Is Already Impacting Legal Practice*, LEGAL IT PROFS. (May 26, 2017), https://www.legalitprofessionals.com/legal-it-columns/118-niki-black/9769-artificial-intelligence-is-already-impacting-legal-practice [https://perma.cc/96W6-PB5E] ("Mark my words: AI will undoubtedly change the legal profession. You can either resist its impact to your detriment, or take steps to acclimate and use it to your advantage. The choice is yours.").

## II. ARTIFICIAL INTELLIGENCE DEFINED

In 1956, James McCarthy, an assistant professor of mathematics at Dartmouth, coined the term "artificial intelligence" when he established a summer symposium dedicated to the burgeoning field.[21] When applying for funding for the symposium, he described artificial intelligence in the following manner:

> The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves.[22]

The kind of learning described by McCarthy requires more than just logical reasoning—experience, training, and practice comprise necessary variables.[23] Smart machines employ AI programming to extract patterns from data rather than simply storing and accessing data. While most thought leaders agree that the term AI connotes a machine that can "learn" (i.e., Watson's famous jeopardy triumph),[24] it is worth noting that scientists, philosophers, futurists, and others disagree as to the definition of intelligence, the definition of consciousness, the speed at which technology may deliver super intelligent machines, and whether those machines will be the next species to rule the planet.[25]

In fact, there are widespread ethical concerns about the development of artificial intelligence that have little to do with legal ethics.[26] Renowned Swedish-American cosmologist Max Tegmark refers to the artificial intelligence debate as "the most important conversation of our lifetime."[27] Tegmark writes that "[t]he questions raised by the success of AI aren't merely intellectually fascinating; they are morally crucial, because our choices can potentially affect the entire future of life."[28]

[21] *See* JERRY KAPLAN, ARTIFICIAL INTELLIGENCE: WHAT EVERYONE NEEDS TO KNOW 13 (2016).

[22] *Id.*

[23] *Id.* at 27.

[24] *See* Engadget, *IBM's Watson Supercomputer Destroys Humans in Jeopardy*, YOUTUBE (Jan. 13, 2011), https://www.youtube.com/watch?v=WFR3lOm_xhE; *see also* Lauren J. Young, *What Has IBM Watson Been Up to Since Winning Jeopardy 5 Years Ago?*, INVERSE (Apr. 5, 2016), https://www.inverse.com/article/13630-what-has-ibm-watson-been-up-to-since-winning-jeopardy-5-years-ago [https://perma.cc/6LNK-QU8J].

[25] MAX TEGMARK, LIFE 3.0: BEING HUMAN IN THE AGE OF ARTIFICIAL INTELLIGENCE 44, 49–50, 282–83 (2017); *see also* KAPLAN, *supra* note 21, at 67–86.

[26] *See* TEGMARK, *supra* note 25, at 261–62.

[27] *Id.* at 37.

[28] *Id.* at 36.

Some of the issues arising from the "greatest conversation" necessarily implicate the legal profession because of the pervasive role of the law in society. Among the more nuanced questions raised are whether machines should have legal rights and liabilities similar to those of corporations,[29] whether an AI program can commit a crime, whether "robo-judges" would render more objective rulings and therefore create greater equality in society, whether AI could more efficiently create legislation, and whether updates to the law could be streamed immediately to relevant machines (i.e., automatically updating speed limits and other traffic laws to a self-driving car.)[30] While these issues are no doubt on the horizon,[31] today's lawyers need to confront the "beginning" of artificial intelligence's "invasion"[32] by considering the ethical issues raised by the AI programs currently available to the legal profession.[33]

Analysis of the current legal ethics considerations requires a working definition of AI. Wendy Wen Yu Chang's definition lays a solid foundation:

> Broadly, AI is the ability of a machine to perform what normally can be done by the human mind. AI seeks to use an automated computer-based means to process and analyze large amounts of

[29] *See* Cuthbertson, *supra* note 3 (discussing Sophia, a robot that was recently granted citizenship in Saudi Arabia, and Mirai, a seven-year-old bot that was given residency in Japan).

[30] *See* KAPLAN, *supra* note 21, at 89–105.

[31] *See* Black, *supra* note 20 (One Deloitte Study includes not only projections of the automation of legal sector jobs over the next 20 years, but also Richard Troman's fictional description of the life of future lawyers, which begins with "an attorney arriving to work in a driverless vehicle and being granted access to his firm's building after facial recognition technology is employed. Next, he enters a mostly empty office, since most employees work remotely from home.").

[32] *See* Nadaline Webster, *How Many Lawyers Are Using Artificial Intelligence Right Now?*, TRADEMARKNOW (June 9, 2017), https://www.trademarknow.com/blog/lawyers-artificial-intelligence [https://perma.cc/CBP2-Z3TW] (The article discusses the results of management consultant firm Altman Weil's 9th annual report titled "Law Firms in Transition." Of 386 participating law firms "7.5% said that they were already using tools involving AI. Another 28.8% are researching options and 37.8% are familiar with the area but haven't yet taken any steps. Perhaps the most surprising finding is that just over one quarter of firms (25.9%) were not familiar with any developments in this area.").

[33] Though beyond the scope of this article, one such ethical dilemma is raised by the use of AI to assist judges in setting bail and deciding whether to grant parole. *See* Dominguez, *supra* note 17. As reported by Dominguez, COMPAS, the software used to assist with these calculations, uses responses to over 100 survey style questions (addressing biographical data such as the defendant's gender, age, criminal history, and personal relationships) to predict whether or not he or she likely to re-offend or is a flight risk. *Id.* Northpointe, the company that created the software, has refused to make its algorithm public, effectively preventing defense attorneys from being able to bring informed challenges to judges' decisions. *Id.* More troubling still is the fact that a study by ProPublica found that the software appears to employ a bias against black defendants. *Id.*

> data and reach rational conclusions–the same way the human mind does.[34]

No doubt, James McCarthy would appreciate the evolution of his 1956 definition that expressed AI as a possibility to the current definition that describes AI as a statement of fact. As noted by Chang, AI is more than data processing; it is the ability of a machine to learn from recognizing patterns in the data. Andrew Arruda, the CEO of ROSS Intelligence, defines AI using four categories: machine learning, natural language processing, vision, and speech.[35] His descriptions provide further insight:

> **Machine learning** describes a system that can take data points, process them to improve performance at completing a task, and then loop that process to continue doing the task while continuously improving.
>
> **Natural language processing** is when a computer can understand human language. The computer can interpret what a human actually means—deciphering intent and therefore providing more accurate and relevant answers and search results.
>
> **Vision** is the computer having the ability to interpret images, identify them and describe them, which is a task humans perform automatically.
>
> **Speech** is a system like Siri that can speak and interpret oral language, so you can have a back-and-forth interaction.[36]

These definitions provide context through which one can better understand the current offerings of AI legal service providers. For example, ROSS, referred to as IBM's Watson's "son" by legal tech experts Sharon Nelson and John Simek, is a legal research service.[37] ROSS's full name is ROSS Intelligence.[38] The program continues to advance its legal research and writing skills in the areas of bankruptcy and intellectual property law.[39] ROSS understands natural language, so it can be asked a question using normal speech.[40] At the time of this writing, at least ten large law firms have invested in ROSS.[41] One attorney has gone so far as to proclaim ROSS's legal skills to be indecipherable from those of a young associate.[42]

[34] *See Ethical Implications*, *supra* note 18; *see also* Sobowale, *supra* note 1.

[35] *See* Andrew Arruda, *Artificial Intelligence Systems and the Law*, PEER TO PEER (Summer 2016), http://www.hsc.edu/Documents/alumni/hscbar/ArrudaROSSIntelligenceAISystemsAndLaw.pdf [https://perma.cc/KP8E-DMBD].

[36] *Id.*

[37] *See* Nelson & Simek, *supra* note 10.

[38] *Id.*

[39] *Id.*

[40] *See* Sobowale, *supra* note 1.

[41] *Id.*

[42] Gina Passarella, *Salazar Jackson Enters World of AI With ROSS Intelligence*, DAILY BUS. REV. (Nov. 4, 2016), http://www.law.com/dailybusinessreview/almID/1202771616534/ [https://perma.cc/EN32-GUH6].

Beyond ROSS, there are AI vendors available to assist in drafting patent applications,[43] performing due diligence, and analyzing contracts.[44] Other AI systems offer assistance with case strategy.[45] Lex Machina spots trends in judges' rulings, identifies legal strategies of opposing counsel, and notes winning arguments.[46] It uses natural language processing to evaluate millions of court decisions to find patterns or trends and refers to its product as "moneyball lawyering."[47] Still other AI systems predict the winner of a case based upon statistical analysis of verdicts in similar cases.[48] One AI company, aptly named Premonition, boasts, "We Know Which Lawyers, Win Which Cases, In Front of Which Judges."[49] In fact, litigation funding companies are looking to AI before they "bet" on the outcome of a lawsuit.[50] Silicon Valley's Legalist invests in a case after its algorithm concludes that a lawyer has high odds of winning the lawsuit.[51]

Handling a murder trial and need assistance developing a legal strategy? Visit the Jury Lab: a program that scans the faces of mock jurors, providing a lawyer with feedback as to how the jurors "feel"—consciously or otherwise—about a lawyer's arguments.[52] And for the lawyer who is already in the courtroom, the tech company Voltaire recently launched an AI jury selection program.[53]

There are also companies attempting to automate daily administrative functions such as seamlessly recording billing hours and producing client invoices.[54] William Davis asks lawyers to consider the following possibilities:

> 1. **Focus:** A partner about to enter a client meeting verbally asks the computer to bring up the last few invoices. The verbal interface saves the attorney what would normally require several, rather dis-

[43] David Hricik, *Machine Aided Patent Drafting: A Second Look*, PATENTLYO (Aug. 25, 2017), https://patentlyo.com/hricik/2017/08/machine-patent-drafting.html [https://perma.cc/9328-6BY5].

[44] *See* KIRA, https://kirasystems.com [https://perma.cc/JS78-B423] (last visited Mar. 14, 2018).

[45] *See, e.g.,* LEX MACHINA, https://lexmachina.com [https://perma.cc/MQ3R-4BNE] (last visited Mar. 14, 2018).

[46] *Id.*

[47] *Id.*

[48] *See* PREMONITION, https://premonition.ai [https://perma.cc/KMJ8-VRA5] (last visited Mar. 14, 2018).

[49] *Id.*

[50] *See* Cromwell Schubarth, *Y Combinator Startup Uses Big Data to Invest in Civil Lawsuits*, SILICON VALLEY BUS. J. (Aug. 24, 2016, 7:25 AM), https://www.bizjournals.com/sanjose/blog/techflash/2016/08/y-combinator-startup-uses-big-data-to-invest-in.html [https://perma.cc/3UL8-AZKM].

[51] *See id.*

[52] *The Jury Lab, LLC Brings the Legal Community Game-Changing Technology*, NEWSWIRE (Apr. 6, 2017), https://www.newswire.com/news/the-jury-lab-llc-has-partnered-with-affectiva-emotion-ai-to-bring-the-19157468 [https://perma.cc/9TB9-WAQW].

[53] Willens, *supra* note 16.

[54] *See id.*

> tracting, navigational clicks. He or she is now *focused* on what needs to be done rather than *searching* for what needs to be done.
>
> 2. **Expenses:** As a lawyer closes the door to an Uber ride that dropped him or her off at the client site, an AI application scans the attorney's inbox for the receipt and automatically enters it as a line item expense.
>
> 3. **Calendaring:** Near the end of an hour-long client meeting, the attorney and client agree to a follow-up meeting the next week. An AI application has been passively listening to the conversation—with legal consent—in the background and automatically reviews each party's calendar and proposes a new meeting time that's mutually beneficial.
>
> 4. **Intake:** During new client intake, an AI application is listening in the background and automatically begins searching for potential conflicts. In the meantime, another algorithm continuously narrows down sources of legal research relevant to the legal matter at hand, as the intake form is completed or files are added to the case.
>
> 5. **Predictive analysis:** An AI application combs through the massive data set in a law firm's case management and practice management system—and compares that data to public sources such as newsfeeds and stock exchange data to make a prediction: In the next 12 months, this practice area, or this type of company, represents a growth opportunity for the firm; look for new lateral hires with this expertise.[55]

There are many other AI applications currently impacting the legal profession, including bots like DoNotPay, an AI program that directly handles traffic citations for live clients.[56] DoNotPay is expanding to assist tenants challenging eviction notices and consumers contesting fraudulent charges on credit cards.[57] These bots give rise to a challenging legal ethics question explored by Ronald D. Rontunda: *"Can Robots Practice Law?"*[58]

[55] William Davis, *How AI's Opportunities Will Augment Rather than Replace Lawyers*, Legaltech News (Oct. 5, 2017), https://www.law.com/legaltechnews/almID/1202799657613/ [https://perma.cc/4GQJ-5WYM].

[56] John Mannes, *DoNotPay launches 1,000 new bots to help you with your legal problems*, TECHCRUNCH (July 12, 2017), https://techcrunch.com/2017/07/12/donotpay-launches-1000-new-bots-to-help-you-with-your-legal-problems/ [https://perma.cc/8ZAT-4TMB].

[57] *See generally id.* (explaining that DoNotPay can help people with landlord contract violations).

[58] Ronald D. Rotunda, *Can Robots Practice Law*?, VERDICT (Sept. 11, 2017), https://verdict.justia.com/2017/09/11/can-robots-practice-law [https://perma.cc/3R36-RRWA].

## III. THE INTERPLAY OF ARTIFICIAL INTELLIGENCE AND LEGAL ETHICS

### A. *Vendors and Devices*

The legal ethics concerns raised by the use of AI vary based on context. For example, the ethical duties of competence and confidentiality pertain to the analysis of both the use of AI programs offered by third-party vendors and the use of personally and professionally owned smart devices; however, a lawyer's relationship to a vendor is distinct from his possession and control of a smart device.[59] The distinction exists because lawyers must actively protect the confidential data stored and transmitted on their individual devices. While lawyers do not necessarily need to understand the technical underpinnings of AI algorithms, they should understand basic smart device technology. This Section explores the legal ethics rules in connection with retaining an AI vendor. The Section that follows discusses competence, confidentiality, and the legal ethics obligations attendant to smart devices.

### B. *ROSS and His Colleagues (The Vendors)*

The use of AI programs in the legal profession presents a few threshold questions: Will there be a profession-wide mandate for lawyers to employ AI in order to remain competent? In other words, if AI increases efficiency and enhances effectiveness, does a lawyer risk being subjected to a disciplinary complaint or a malpractice claim for failing to use an applicable AI program? If an AI system works more efficiently, and thereby reduces a client's bill, is a lawyer who fails to employ AI charging unreasonable fees?

Sound preposterous? It was not that long ago that some in the legal field suggested that a lawyer's failure to consider social media in preparing a case would soon be deemed incompetence.[60] This suggestion was initially met with skepticism, but today social media has been codified as a component of competence in various ethics opinions and court cases.[61]

Regardless of whether the use of AI becomes a fundamental component of competence, there is nonetheless a competent manner in which to retain an AI vendor. Generally, retention of an AI vendor falls within the context of the established legal ethics guidelines for

[59] The legal profession's consideration of bots that function without any lawyer interacting with the client is another category, the comprehensive analysis of which is beyond the scope of this article.

[60] JAN L. JACOBOWITZ & JOHN G. BROWNING, LEGAL ETHICS AND SOCIAL MEDIA: A PRACTITIONER'S HANDBOOK 6 (2017); *see* Jacobowitz & Singer, *supra* note 12.

[61] Jan L. Jacobowitz, *Lawyers Beware: You Are What You Post: The Case for Integrating Cultural Competence, Legal, Ethics, and Social Media*, 17 SMU SCI. & TECH. L. REV. 541, 553 (2014).

outsourcing legal services.[62] The American Bar Association ("ABA") and several states issued ethics advisory opinions between 2006 and 2012 that provide guidance to lawyers who outsource legal research, document review, and the drafting of pleadings to both domestic and international third-party vendors.[63] New York also released an advisory opinion that addresses outsourcing a law firm's administrative functions.[64]

The outsourcing opinions primarily discuss outsourcing legal work to other human beings and generally agree that outsourcing is permissible if done in compliance with the rules of professional conduct.[65] The rules implicated comprise the fundamental components of the effective, ethical practice of law—competence, diligence, communication, confidentiality, and the supervision of non-lawyer assistance.[66] In fact, the ABA recognized the increasing use of outsourcing in 2012, when it enacted amendments to the comments to Rule 1.1 Competence and Rule 5.3 Responsibilities Regarding Nonlawyer Assistants.[67] The comments dovetail with various state ethics opinions that generally advise lawyers to obtain client consent before using outsourcing in a client's case.[68]

Of course, in order to obtain valid client consent, both the lawyer and the client must understand the nature and purpose of the outsourcing.[69] AI outsourcing may necessitate a more detailed explana-

[62] *See* ABA Comm. on Ethics & Prof'l Resp., Formal Op. 08-451 (2008); State Bar of Cal. Comm. on Prof'l Resp. & Conduct, Formal Op. 2004-165 (2004); Colo. Bar Ass'n, Formal Op. 121 (2009); Fla. State Bar Prof'l Ethics Comm., Ethics Op. 07-2 (2008); N.C. State Bar, Formal Op. 2007-12 (2008); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Ethics Op. 762 (2003); N.Y.C. Bar Ass'n Comm. on Prof'l & Jud. Ethics, Formal Op. 2006-3 (2006); Ohio Supreme Court Bd. Of Comm'rs on Grievances & Discipline, Advisory Op. 2009-06 (2009); San Diego Cty. Bar Ass'n, Ethics Op. 2007-1 (2007); L.A. Cty. Bar Ass'n Prof'l Resp. & Ethics Comm., Op. No. 518 (2006); D.C. Bar, Ethics Op. 362 (2012); *see also* N.Y.C. Bar Ass'n Comm. on Prof'l Resp., *The Outsourcing of Legal Services Overseas*, NYC BAR (2007), http://www.nycbar.org/pdf/report/uploads/20071813-ReportontheOutsourcingofLegalServicesOverseas.pdf [https://perma.cc/EZ8W-5M8W].

[63] *See supra* note 62.

[64] N.Y. City Bar Ass'n Comm. on Prof'l & Judicial Ethics, Formal Op. 2015-1 (2015).

[65] *See* JACOBOWITZ & BROWNING, *supra* note 60.

[66] *See id.*

[67] MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 6 (AM. BAR ASS'N 2016); MODEL RULES OF PROF'L CONDUCT r. 5.3 cmt. 3–4 (AM. BAR ASS'N 2016).

[68] *See supra* note 62; *see* MODEL RULES OF PROF'L CONDUCT r. 1.2 (AM. BAR ASS'N 2016); MODEL RULES OF PROF'L CONDUCT r. 1.4 (AM. BAR ASS'N 2016).

[69] Mark Williamson, co-founder and chief technology officer for Hanzo Archives Ltd. in London, suggests, "AI can't be defended unless it's possible to explain why and how the AI system or tool reached the conclusion it reached. For example, a law firm would need to find out which analytics and variables programmed into the technology sparked the conclusion that particular facts about a case are relevant." Mark Williamson, *Getting Real About Artificial Intelligence at Law Firms*, LAW360 (Nov. 3, 2017), https://www.law360.com/articles/976805/getting-real-about-artificial-intelligence-at-law-firms [https://perma.cc/9UEQ-KRW8]. Williamson also suggests that a

tion than the outsourcing of legal research or document review to other humans. Clients who are unfamiliar with AI may ask not only how AI performs legal work, but also why a lawyer has opted to use AI and what the relative cost will be for the client. In fact, the outsourcing opinions explain that, in most circumstances, and unless otherwise agreed upon, a lawyer should bill the client only the net costs of outsourcing, with a possible additional fee for the lawyer's time to supervise and review the work product.[70]

Regardless of how much detail the client seeks, lawyers must thoroughly vet an outsourcing company as to how and where the work will be performed, the qualifications of its employees (and bots), what type of security measures are used to protect data, and the relevant privacy laws in an outsourcing vendor's jurisdiction.[71] Additionally, where appropriate, lawyers should ensure that a conflict-checking mechanism exists, so that opposing parties in a case or both parties in a transactional matter do not retain the same vendor.[72] Another fundamental concern is confidentiality—a confidentiality agreement that binds both the vendor and its employees must be executed or integrated into the terms of service documents provided by the vendor.[73] The strength of a confidentiality agreement depends partially upon the vendor's data security protocol.

Recently, intellectual property attorney and law professor David Hricik explored AI in the context of patent law.[74] He contracted with a company that employs AI to draft a patent application. Hricik reviewed the biographies of the founders of the company and found a wide spectrum of knowledge—a lawyer, a linguistic expert, and a venture capitalist among them.[75] Next, he delved into the terms of service and the privacy statement.[76] Although complex, the documents re-

"framework" of input variables should be known to assist in understanding the basis for an AI conclusion. *Id.* Williamson concludes that law firms must "[t]reat AI solutions exactly like new hires—even high-powered attorneys or employees who have just joined a law firm's or client's staff. When new hires come on board, law firms and their clients don't usually assume that all will be fine and leave these individuals to their work. Instead, they explain company policies and practices—and the reasons for them." *Id.*

[70] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 1.5 (AM. BAR ASS'N 2016).

[71] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 1.3 (AM. BAR ASS'N 2016); *see also* Williamson, *supra* note 69 (quoting "[t]he 'Wild West' days when little attention was paid to [personally identifiable information] was handled or protected, if at all, are over").

[72] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 1.7 (AM. BAR ASS'N 2016).

[73] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 2016).

[74] *See* Hricik, *supra* note 43.

[75] David Hricik, *Augmented Patent Drafting and Ethics*, PATENTLYO (June 8, 2017), https://patentlyo.com/hricik/page/2 [https://perma.cc/ZF22-USR2].

[76] *Id.*

vealed that the company had thoughtfully covered many of the legal ethics issues concerning confidentiality.[77] Specifically, the company's terms of service explain that the program encrypts data and does not retain confidential information.[78] The terms also indicate that any retained information is converted into a language consisting of symbols that is incomprehensible to the untrained eye.[79]

Perhaps most compelling is Hricik's test run with the company.[80] Hricik submitted a patent claim and received a remarkable set of specifications and drawings almost instantaneously.[81] While presenting on the ethical implications of AI at the Texas A&M AI Symposium, Hricik explained that the patent documents he received would have taken a patent lawyer between ten and fifteen hours to draft.[82] Instead, the patent preparation required two hours of lawyer time and $2,500 (the cost of using the AI company).[83] Thus, in terms of work efficiency for the lawyer and cost efficiency for the client, the AI machine appeared to prevail.

However, Hricik does raise additional questions about whether the corporation's patent preparation constitutes the practice of law or whether payment may be considered the sharing of attorney fees.[84] Moreover, Hricik emphasizes the need for due diligence as these companies tend to disclaim any liability.[85] The patent example exemplifies the general rule that a lawyer must thoroughly vet and supervise any non-lawyer assistance such that regardless of whether an in-house paralegal or a high-tech AI vendor provides the assistance, the conduct aligns with the lawyer's responsibilities under the legal ethics rules.[86]

Of course, there are other macro legal ethics concerns in relation to using an AI vendor such as the rules that require a lawyer to maintain

[77] Note that the terms of service are generally those documents that individuals tend to scroll past in search of the box to check "agree."

[78] *See* Hricik, *supra* note 43.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *See also Artificial Intelligence and the Legal Profession*, TEX. A&M J. PROP. L. (Oct. 20, 2017), http://law.tamu.edu/current-students/academics/law-journals/journal-of-property-law/ai-symposium [https://perma.cc/WQ4X-E8XS].

[83] *See* Hricik, *supra* note 43; *see Artificial Intelligence and the Legal Profession*, TEX. A&M J. PROP. L. (Oct. 20, 2017), http://law.tamu.edu/current-students/academics/law-journals/journal-of-property-law/ai-symposium [https://perma.cc/WQ4X-E8XS]; *see* Jason Tashea, *Artificial Intelligence Software Outperforms Lawyers (Without Subject Matter Expertise) In Matchup*, ABA J. (Nov. 3, 2017, 8:00 AM), http://www.abajournal.com/news/article/artificial_intelligence_software_outperforms_lawyers_without_subject_matter [https://perma.cc/ZL75-EXST].

[84] *See* Hricik, *supra* note 43.

[85] *Id.*

[86] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 5.3 (AM. BAR ASS'N 2016).

independent professional judgment[87] and to avoid the encouragement of, or participation in, the unauthorized practice of law.[88] In the outsourcing context, these concerns generally translate into a question of whether a lawyer carefully reviews the vendor's work so that the lawyer provides the ultimate analysis of the legal work and its use in the case.[89] In other words, a lawyer could not permit an AI machine to research, write, and file a pleading without the lawyer's review of the research and the pleading. It may be a brave new world, but no lawyer should be so "brave" as to blindly rely on a bot's legal work.

### C. *Siri and her "Invitees" (The Devices)*

Although there may be some technical debate as to whether Apple's Siri,[90] Google's Assistant, Samsung's Bixby[91] and Amazon's Alexa should be considered real artificial intelligence,[92] that debate is not the central focus for lawyers concerned with their ethical responsibilities to their clients. Instead, lawyers must understand how their interaction with these electronic assistants might impact confidential client information.[93] Siri and the Google Assistant, the two most widely used forms of AI in the mobile market, along with Amazon's Alexa, provide insight into the confidentiality concern.

Although Apple has been a prominent privacy advocate, it has also been fairly straightforward about its pervasive collection of data, particularly as to Siri voice data.[94] However, Apple has recently adopted a less detailed privacy statement, which gives Apple far more leeway in data collection.[95]

[87] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 5.4 (AM. BAR ASS'N 2016).

[88] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 5.3 (AM. BAR ASS'N 2016).

[89] *See supra* note 62; MODEL RULES OF PROF'L CONDUCT r. 5.3 (AM. BAR ASS'N 2016).

[90] *See* William Herkewitz, *Why Watson and Siri Are Note Real AI*, POPULAR MECHS. (Feb. 10, 2014), http://www.popularmechanics.com/science/a3278/why-watson-and-siri-are-not-real-ai-16477207/ [https://perma.cc/H896-PJY8].

[91] Bixby, SAMSUNG, http://www.samsung.com/us/explore/bixby/overview/ [https://perma.cc/M9ZH-BZL6] (last visited Feb. 26, 2018).

[92] *See* JR Raphael, *'Artificial Intelligence' has Become Meaningless Marketing Jargon*, COMPUTERWORLD (Mar. 21, 2017, 9:43 AM), http://www.computerworld.com/article/3183140/android/samsung-bixby-artificial-intelligence.html [https://perma.cc/62EP-C2SH].

[93] *See* Haley Sweetland Edwards, *Alexa Takes the Stand: Listening Devices Raise Privacy Issues,* TIME (May 4, 2017), http://time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues/ [https://perma.cc/J6WV-WKSE].

[94] iOS Software License Agreement, APPLE (JULY 27, 2014), https://ssl.apple.com/legal/sla/docs/iOS8.pdf [https://perma.cc/D2J2-FWGV] [hereinafter iOS8 Privacy].

[95] iOS Software License Agreement, APPLE (JULY 14, 2016), https://ssl.apple.com/legal/sla/docs/iOS10.pdf [https://perma.cc/5DEL-V2T9].

Apple records, transmits, and transcribes an individual's voice commands to Siri along with other information including names, nicknames, relationships, and contacts' addresses.[96] The individual's location is logged and attached to every Siri request.[97] Apple also requires a person to provide his consent to provide his information to third parties.[98] In fact, IBM's privacy concerns about Siri caused it to ban the use of Siri on IBM campuses.[99]

Nonetheless, Apple implements two methods to secure and anonymize the information shared with Siri; both methods were confirmed at the 2017 World Wide Developer's Conference and will apply to Apple's various platforms, including HomePod.[100] First, Apple plans to implement end-to-end encryption for Siri data that is transmitted and synced between all iCloud-connected Apple devices.[101] Second, Apple will use a combination of what it calls an anonymous Siri Identification Number[102] and Differential Privacy.[103]

Differential Privacy is a design that employs mathematical certainty to remove the possibility that a cyber-attack will obtain an individual's anonymized data (known as a linkage attack) by attributing the data to a group rather than an individual.[104] Netflix's system has been used to illustrate how a linkage-attack might occur.[105] Netflix publishes anonymized user viewing histories, but researchers at University of Texas Austin proved that the release of the so-called anonymous data was not actually anonymous.[106] According to the researchers, the anonymous information released by Netflix can be used to find personally identifiable information and create an identity linkage (or cross reference) between sensitive "anonymized" data and public data.[107] The researchers linked the "anonymous" data provided by Netflix with the names of individuals who publicly posted movie and

[96] *See* iOS8 Privacy, *supra* note 94, at 4(c).

[97] *Id.*

[98] *Id.*

[99] Robert McMillan, *IBM Outlaws Siri, Worried She Has Loose Lips*, WIRED (May 22, 2012, 7:01 PM), https://www.wired.com/2012/05/ibm-bans-siri/ [https://perma.cc/KD8Y-YT9F].

[100] *Apple Special Event: June 5, 2017*, APPLE, https://www.apple.com/apple-events/june-2017/ [https://perma.cc/CYT6-JB9C] (last visited Feb. 24, 2018).

[101] *Id.*

[102] *Id.*

[103] Andy Greenberg, *Apple's 'Differential Privacy' is About Collecting Your Data – But Not* Your *Data*, WIRED (June 13, 2016, 7:02 PM), https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/ [https://perma.cc/2URQ-H67T].

[104] *See* Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy*, FOUND. & TRENDS THEORETICAL COMPUT. SCI. 3 (2014), https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf [https://perma.cc/2Z98-W89Q].

[105] *Id.* at 7.

[106] Bruce Schneier, *Why 'Anonymous' Data Sometimes Isn't*, WIRED (Dec. 12, 2017), https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/ [https://perma.cc/ZG4V-B46J].

[107] Dwork & Roth, *supra* note 104, at 7.

television reviews on IMDB, thereby assigning names to the anonymous data provided by Netflix.[108]

Like Siri, Google's Assistant also records, transmits, and transcribes the same information that Apple maintains.[109] The key difference, as of the writing of this Article, is that Google does not employ privacy protecting algorithms such as Differential Privacy.[110] Furthermore, every voice command entered into an Android device (or Google Home) is logged and stored in connection with the person's Google account.[111] Using Google Voice & Audio, users can listen to their own vocal commands, which are directly linked to their Google account, which also contains personal information such as name, geo-location, YouTube viewing history, and search history.[112]

If you are using an Amazon Echo, then you should be aware that Amazon maintains a voice recording—on Amazon's servers—of all Alexa commands.[113] Amazon also saves a "fraction of a second" of audio recorded before the command word is uttered.[114] One journalist, writing about virtual assistants, shared her personal discovery: "I was surprised when I checked my Amazon Echo recordings. In one recording, I was explaining why I wasn't taking a deal on a commercial building that I had for sale."[115] The journalist advised Amazon Echo users to check their recordings.[116]

While it can be shocking to see just how much personal information is stored by these virtual assistants, lawyers are not necessarily re-

[108] *See id.* Linkage attacks have existed at least since 2006 when AOL released browsing history information that was anonymized through numeric ID. Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?mcubz=1 [https://perma.cc/GSF9-9NB5]. The New York Times quickly demonstrated the vulnerability of numeric ID, when it used this data, with the consent of the individual, to identify several personal IDs. *Id.* This attack vector is the crux of the concern for the recent legislation that repealed the privacy rules that were designed to prevent ISPs from selling users Internet browsing history; these types of sensitive data sets are vulnerable to linkage-attacks. *Id.*

[109] Privacy, GOOGLE, https://privacy.google.com/intl/en [https://perma.cc/Z4DQ-PNKS] (last visited Feb. 24, 2018).

[110] *See id.*

[111] Jocelyn Baird, *Smart Speakers and Voice Recognition: Is Your Privacy at Risk?*, NEXTADVISOR BLOG (Apr. 4, 2017), https://www.nextadvisor.com/blog/2017/04/04/smart-speakers-and-voice-recognition-is-your-privacy-at-risk/ [https://perma.cc/2C74-3XG9].

[112] *See* Alex Hern, *How to Listen to (and Delete) Everything You've Ever Said to Google*, GUARDIAN WEEKLY (Oct. 13, 2015, 10:07 AM), https://www.theguardian.com/technology/2015/oct/13/google-voice-activity-listen-delete-recordings [https://perma.cc/DJF4-EMRF].

[113] *See* Kim Komando, *How to Stop Your Devices From Listening to (and Saving) What You Say*, USA TODAY (Sept. 29, 2017 10:14 AM), https://www.usatoday.com/story/tech/columnist/komando/2017/09/29/how-stop-your-devices-listening-and-saving-what-you-say/715129001/ [https://perma.cc/P8SX-ZYBF].

[114] *Id.*

[115] *Id.*

[116] *Id.*

quired to be knowledgeable about the specifics of how Apple, Google, or Amazon stores information, but rather whether any information stored on their personal accounts reveals information about a client.[117] Query: how does a lawyer serve his client effectively by incorporating technology into his practice, while also avoiding the ethical landmines that may be lurking within a smart device? For example, if a lawyer used Google Assistant to research a topic or do a quick search on a client, that information is stored and indexed, easily searched on the lawyer's account by anyone who gains access to it. If that account is compromised, a malicious actor may be able to find exactly where that attorney is located, precisely what the attorney was searching, and may even discover any contacts stored in the attorney's account, including confidential client information.

Thus, careful consideration must be given to whether the AI features on a smartphone or virtual assistant are appropriate for a lawyer's particular work environment. Siri's differential privacy appears to have the edge on security, but Siri does not have all of Google Assistant's searching capacity or Alexa's varied features. A lawyer must first become aware of the risks involved in the use of virtual assistants. Then he may decide whether the benefits outweigh the risks. Finally, if using a virtual assistant, a lawyer must learn to manage the features of a virtual assistant to minimize a breach of confidentiality.[118] Sharon Nelson and John Simeck, prolific writers and law firm tech advisors, note:

> We have found that lawyers rarely think about keeping data confidential with respect to their personal assistants, which tend to be compellingly addictive. Just as it took a while to get used to the notion that we need to be serious about protecting confidential data on our computers and phones, it will likely take a while for the legal profession to wrap its head around the dangers of personal assistants – and the rich lode of potential evidence that may be found in the clouds that store questions or commands addressed to personal assistants.[119]

Unlike virtual assistants, lawyers' use of smartphones have become ubiquitous. Since the inception of the smartphone in 2007, there has been considerable analysis in the context of legal ethics—both tech and ethics guidelines exist to assist lawyers in the effective, ethical use of a smartphone.[120] Because all smartphones contain AI and are also

[117] *Id.*; *see generally* Lisa Vaas, *Alexa is Listening to What You Say – and Might Share That With Developers*, NAKED SECURITY (July 7, 2017), https://nakedsecurity.sophos.com/2017/07/17/alexa-is-listening-to-what-you-say-and-might-share-that-with-developers/ [https://perma.cc/ZJ72-X323].

[118] *See* Komando, *supra* note 113; *see also* Vaas, *supra* note 117.

[119] *See* Nelson & Simek, *supra* note 10.

[120] *See, e.g.,* Peter Geraghty, *ABA Formal Opinion 477R: Securing Communication of Protected Client Information*, ABA (June 2017), https://www.americanbar.org/publications/youraba/2017/june-2017/aba-formal-opinion-477r—securing-communica-

used to communicate with both clients and AI vendors, lawyers must consider the "reasonable efforts" required to maintain client confidentiality when using a smartphone.

### D. *Smartphones, Legal Ethics, and "Reasonable Efforts"*

Much has changed about how the world does business since the iPhone's debut; in fact, we have witnessed not only the introduction of mobile devices, but also the "smartening" of mobile phones such that they have become an integral part of many everyday business operations. It is important to explore where the legal field is heading in regard to information security ("InfoSec"), and to focus on the somewhat overlooked security risks of the use of mobile devices such as the iPhone and Android smartphones, which often employ AI assistants and are used to communicate with AI vendors and clients. Regardless of whether the AI component of the smartphone is in use, if the smartphone is employed in any aspect of a lawyer's practice, the ethical implications must be addressed.

In fact, given the constantly changing technological landscape, the ABA recently released and revised Formal Opinion 477.[121] Importantly, it updates the ABA's 1999 Opinion[122] regarding securing communications to protect client information.[123] And despite the ABA's awareness of the increasing dangers resulting from the ubiquity of technology in legal practice, mobile devices are only mentioned once in passing.[124] However, mobile devices must be explicitly included in the guidance for maintaining the security of confidential information if lawyers are to "keep abreast of changes in the law and its practice, including the benefits and risks of technology."[125]

The ABA opinion offers seven guiding considerations to assist in determining whether a lawyer's efforts are *reasonable in the circumstances* and therefore in compliance with Rules 1.1 Competence, 1.6 Confidentiality, 4.4 Respect for Rights of Others, 5.1 Supervisory Lawyer, and 5.3 Supervision of Nonlawyers.[126] The seven considerations are the following: (1) the nature of the threat; (2) how client confidential information is transmitted and stored; (3) the use of reasonable electronic security measures; (4) how electronic communications should be protected; (5) the need to label client information as privileged and confidential; (6) the need to train lawyers and nonlawyer assistants in technology and cybersecurity; and (7) the need to

tion-of-protected-cli.html [https://perma.cc/VL5P-C3JG] [hereinafter *Securing Communication*].

[121] *See id.*

[122] *See id.*

[123] *Id.*

[124] *See id.*

[125] MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. (AM. BAR ASS'N 2016).

[126] *See Securing Communication*, *supra* note 120.

conduct due diligence on vendors who provide technology services.[127] The analysis that follows will pertain to smartphones, which may be used with an AI assistant or to communicate with an AI vendor who has presumably been vetted appropriately.

The ABA's Opinion 477[128] emphasizes reasonable efforts, beginning with a significant emphasis on InfoSec and Operational Security ("OpSec"), essentially suggesting that lawyers perform a threat model evaluation, often referred to as "threat modeling."[129] Threat modeling is the structured process of evaluating what information needs to be protected, from whom it needs protection, and the relative importance of protecting the information.[130] The unfortunate part of threat modeling for an average technology user is that the user may be unaware of both the various threats that confront the user and the prevalence of these threats; thus, understanding "the nature of the threat" is paramount to the analysis.[131]

Removing some of the threat modeling guesswork for the legal community begins with a consideration of the duties of competence, diligence, communication, and confidentiality across at least six aspects of using a mobile device. In fact, regardless of whether a lawyer embraces AI on his smartphone, the following factors should be considered: (1) whether the device should be used for both personal and professional purposes; (2) passwords and password management; (3) encryption of data at rest and encryption of data in transit; and (4) non-email messaging.[132]

It is often said that by failing to prepare, one prepares to fail, and similarly, failing to competently consider the following known risks and reasonable solutions for everyday digital life will leave lawyers vulnerable and open to failing to protect clients' confidential information.

### 1. Using a Single Device for both Personal and Professional Purposes

Although it may be an accepted practice, using a single device (mobile or otherwise) for both personal and professional purposes

[127] *Id.*

[128] *Id.*

[129] *Assessing Your Risks*, ELEC. FRONTIER FOUND., https://ssd.eff.org/en/module/introduction-threat-modeling [https://perma.cc/X4UE-2GL3] (last visited Sept. 7, 2018).

[130] Lorenzo Franceschi-Bicchierai, *What Is Threat Modeling?*, VICE (Nov. 21, 2017, 8:00 AM), https://motherboard.vice.com/en_us/article/a37p94/what-is-threat-modeling [https://perma.cc/P5G6-8BV3].

[131] *See id.*

[132] It is important to employ multiple layers of security to any system, mobile or otherwise. Securing information is an imperfect practice, and new vulnerabilities and flaws are constantly revealed for almost every platform. When those flaws compromise a system, multiple layers of security will prevent access to confidential and sensitive information, regardless of the nature of the failure.

("mixed-use") creates vulnerabilities. In fact, many firms and corporations now issue laptops and smartphones for business use only. However, the rules of professional conduct do not prohibit a lawyer from using a smartphone as a mixed-use device and many lawyers use their devices in a mixed-use capacity. Therefore, it is important to understand the risks so that a lawyer may make reasonable efforts to protect his professional, confidential information.

### *a. The Risks*

The largest attack vectors for mixed-use devices are called doxxing and phishing.[133] These two attack vectors allow a malicious actor to gain access to all accounts on a device, often unbeknownst to the owner of those accounts. Doxxing is a practice whereby a malicious actor researches freely available information on the Internet and uses it to either release that information in a more public manner or to gain access to an individual's accounts. Sometimes the malicious actor poses as a close friend or relative to gain access to accounts.[134] More often, malicious actors couple the information that they collect on the person, or "target," to create a phishing attack, thereby increasing their likelihood of success.[135] For example, a malicious actor who has learned information about a target may know the target's purchasing habits and send that person a false shipping tracking email where the link in that email leads the person to a cloned site that could steal that person's credentials.

Spear Phishing[136] is a practice whereby a malicious actor poses as a mutual acquaintance or as a company that a person uses (e.g. Google) in order to induce that person to click a malicious link, enter credentials, or download a malicious file.[137] Once the person, or "target," complies with the malicious actor's instructions, the malicious actor steals the target's credentials and tests the information on other accounts owned by the target.[138]

[133] *See What Doxxing is, and Why It Matters*, ECONOMIST (Mar. 10, 2014), http://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9 [https://perma.cc/DHS9-LAD6]; *see also How to recognize phishing email messages, links, or phone calls,* MICROSOFT, https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx [https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx] (last visited Feb. 24, 2018).

[134] *See* Fusion, *Real Future: What Happens When You Dare Expert Hackers to Hack You (Episode 8)*, YOUTUBE (Feb. 24, 2016), https://youtu.be/bjYhmX_OUQQ?t=1m25s [https://perma.cc/U6PG-TBCQ].

[135] *See id.*

[136] Spear phishing is distinguished from a dragnet style phishing attack in that the hacker gathers information about the target that is intended to increase the likelihood that the target will activate the attack. *See* Kim Zetter, *Hacker Lexicon: What is Phishing?*, WIRED (Apr. 7, 2015, 6:09 PM), https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ [https://perma.cc/S8W9-QTDZ].

[137] *Id.*

[138] *See id.*

Some of the most famous examples of spear phishing are the recent leaks relating to John Podesta, Colin Powell, and the Democratic National Committee.[139] However, these types of attacks occur regardless of status or notoriety. Verizon's 2017 Data Breach Investigations Report indicates that "7.3% of users across multiple data contributors were successfully phished—whether via a link or an opened attachment."[140] In other words, an untold number of an attorney's co-workers are likely to open up a phishing email that may compromise their entire system, unless, of course, they are educated and informed on best practices.[141]

### *b. The Solutions*

The key vulnerability in using a smart device for both personal and professional matters is that if one account is compromised, both are compromised. Lawyers who use mixed-use mobile devices expose themselves to a greater probability of having their professional accounts compromised through doxxing, spear phishing, or malware.[142] Thus, a lawyer must employ the same security measures to protect his casual, personal exchanges as are required to insulate his sensitive work accounts. Two-factor authentication, strong and unique passwords, and encryption, discussed below, are some of the tools that enhance security. Awareness of the mixed-use issue is paramount; a lawyer must determine a best practice strategy based on both his area of practice and how he uses his device. Bottom line: a practicing attorney who is not using separate devices for personal and professional purposes should consider securing their device and their personal data to the same degree as their professional confidential data.

## 2. Passwords and Password Management

### *a. The Risks*

Passwords are no longer just single words coupled with a number or two—or at least, they should not be. In 2013, Ars Technica[143] wrote an

[139] *See* Eric Lipton, David E. Sanger, & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0 [https://perma.cc/LRE4-F2XV].

[140] *Verizon's 2017 Data Breach Investigations Report*, VERIZON, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf [https://perma.cc/WG8X-QXLP] (last visited Feb. 24, 2018).

[141] *See id.*

[142] *See generally* Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, & Arturo Ribagorda, *Evolution, Detection and Analysis of Malware for Smart Devices*, IEEE (Nov. 7, 2013), http://www.seg.inf.uc3m.es/~guillermo-suarez-tangil/papers/2013cst-ieee.pdf [https://perma.cc/RK7S-MY7F].

[143] Dan Goodin, *Anatomy of a Hack: How Crackers Ransack Passwords Like "qeadzcwrsfxv1331"*, ARSTECHNICA (May 27, 2013, 8:00 PM), https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/ [https://perma.cc/7HG2-6KMJ].

article illustrating that old computer passwords with six or fewer characters could be cracked in a matter of no more than a few hours.[144] Other institutions have arrived at similar conclusions, but with scalable results.[145]

In the years since Ars Technica conducted its study, computing power has dramatically increased on all devices, including mobile devices. According to Dashlane, one of the leading password management companies, eight alpha-numeric characters are necessary in order to extend the time it would take to crack a password from a few seconds to five hours. However, if you create a twelve character password then, with current technology, it could take a hacker up to 200 years to break the password.[146] Thus, by the addition of four characters, the time to crack that password increases from hours to centuries.[147]

Compounding the problem, most brute-force cracking dictionaries cover permutations and misspellings that are often employed as simple passwords (e.g., p@ssword).[148] Furthermore, in cases where an individual "target" has been doxxed, the attacker is likely to add words and numbers to the cracking dictionary that the attacker believes are most likely to be used (e.g., birth dates, middle names, pet names, etc.), speeding up the cracking process exponentially.[149] Additionally, users who adopt the same password for multiple (or all) accounts are extremely vulnerable; a malicious actor may steal one set of credentials, which then enables them to compromise and usurp all of the users' accounts.

A frequently overlooked threat vector for passwords involves a former employee's access to a system. For example, if a recently terminated employee had access to confidential or sensitive information password deletion and access denial must be initiated, or two problematic scenarios may occur. First, the employee may continue to access the information after termination. Second, the employee and the employer may have failed to maintain security measures or updates to the account, leaving the account susceptible to malicious actors.

[144] Nate Anderson, *How I became a password cracker*, ARS TECHNICA (Mar. 24, 2013, 7:55 PM), https://arstechnica.com/information-technology/2013/03/how-i-became-a-password-cracker/2/ [https://perma.cc/3P4P-2WJ5].

[145] Rick Robinson, *Teraflop Troubles: The Power of Graphics Processing Units May Threaten the World's Password Security System*, GEORGIA TECH (Aug. 7, 2010), http://www.rh.gatech.edu/news/341201/teraflop-troubles-power-graphics-processing-units-may-threaten-worlds-password-securit-0 [https://perma.cc/Y4KR-ZPAU].

[146] *Estimating Password-Cracking Times*, BETTER BUYS, https://www.betterbuys.com/estimating-password-cracking-times/ [https://perma.cc/7L4C-NA83] (last visited Mar. 11, 2018).

[147] *Id.*

[148] Pavitra Shankdhar, *Popular Tools for Brute-force Attacks*, INFOSEC INST. (May 29, 2017), http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref [https://perma.cc/X73W-YDT3].

[149] *See id.*

### *b. The Solutions*

#### i. Strong and Unique Passwords

Simply stated, in order to be properly secured online, an individual should have a different password for each log-in and each of the passwords should be sufficiently long and varied (by including symbols and a mix of upper-case and lower-case letters) in order to render the password more difficult to crack. This solution is based on password entropy, which considers the length and character set of a password to determine the maximum amount of guesses necessary to crack a password.[150] However, creating a password with various symbols and letters may not protect a user from a simple dictionary attack that employs permutations of words (e.g. P@55word); these passwords may be broken almost instantaneously despite a technically high entropy.[151]

Strong passwords may be created using two methods: (1) solely relying on a password manager to generate passwords and (2) creating memorable and strong pass-phrases. For example, thinking of an offbeat sentence or phrase may be a key to creating a memorable pass-phrase that will not be easily doxxed using your personal information. Law students and practicing lawyers may appreciate this example: RAP=100%confusing. The RAP password meets the requirements of long, complex, and memorable. However, this phrase has just become public information, so an astute hacker will add this phrase to his attack dictionary. Bottom line: a password manager may be used to create unique and complex passwords of at least fourteen characters for each account, and one (or more) memorable and strong pass-phrases may be used as the password manager's master password.

#### ii. Secure Password Managers

It is important to note that any system that creates convenience almost always creates security flaws in the system. Thus, lawyers should select companies with solutions that not only solve the problem of creating strong and unique passwords, but also require users to adhere to well-established secure policies.

For example, LastPass allows a system administrator to both seamlessly add and delete users and to implement stringent password stan-

[150] Colin Weaver, *A Somewhat Brief Explanation of Password Entropy*, ITDOJO (Jan. 19, 2016), http://www.itdojo.com/a-somewhat-brief-explanation-of-password-entropy/ [https://perma.cc/JQ5U-XSKT].

[151] A dictionary attack is "a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document." Margaret Rouse & John Ostrowick, *Definition: dictionary attack*, TECHTARGET, http://searchsecurity.techtarget.com/definition/dictionary-attack [https://perma.cc/QJ2X-GD6B] (last visited Mar. 10, 2018).

dards, including disabling auto-fill.[152] On LastPass, lawyers may share logins without revealing their passwords, which provides flexible and secure access to sensitive accounts.[153]

Although LastPass has been the target of hacking, its AES-256-bit encryption with PBKDF2, SHA-256, and salted hashes has prevented the disclosure of the credentials stored on its servers.[154] LastPass, Dashlane, and other password managers cannot guarantee absolute security; however, both of these companies appear to be transparent about security breaches, an important consideration when vetting a password manager.[155] The companies alert users to change their passwords in the event of a breach. Moreover, LastPass and Dashlane both offer the implementation of software- and hardware-based Two-Factor Authentication ("2FA") to gain access to a user's password vault, further securing against malicious agents.[156]

#### iii. Two-Factor Authentication

Two-factor authentication is a method by which to confirm identity.[157] The first factor is a user name and password combination.[158] The second is (usually) a digital, one-time password that is sent through an application or to a physical device.[159]

Two-factor authentication is nearly ubiquitous, although users are not always aware of it. One of the most popular examples is a bank security token.[160] For example, many businesses use a security token to prevent employees from taking unauthorized petty cash.[161]

[152] *See* LASTPASS, https://www.lastpass.com/en/enterprise [https://perma.cc/XPY6-EWYQ] (last visited Feb. 24, 2018).

[153] *See id.*

[154] Ian Paul, *The LastPass Security Breach: What You Need to Know, Do, and Watch Out For*, PCWORLD (June 16, 2015, 11:26 AM), http://www.pcworld.com/article/2936621/the-lastpass-security-breach-what-you-need-to-know-do-and-watch-out-for.html [https://perma.cc/SD2H-ZLH5].

[155] Emmanuel Schalit, *Dashlane Security Updates*, DASHLANE (Sept. 6, 2016), https://blog.dashlane.com/dashlane-update-1/ [https://perma.cc/SA2B-ETA3].

[156] *Id.*

[157] Seth Rosenblatt & Jason Cipriani, *Two-factor Authentication: What You Need to Know (FAQ)*, CNET (June 15, 2015, 1:39 PM), https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ [https://perma.cc/GN36-889Y].

[158] *Id.*

[159] *Id.*

[160] *Security Token*, TECHOPEDIA, https://www.techopedia.com/definition/16148/security-token [https://perma.cc/DU2B-4CQ2] (last visited Feb. 24, 2018); *see also Security Token*, Citi, https://www.privatebank.citibank.com/our_services/online/digital_key.htm [https://perma.cc/W3EM-WCDW] (last visited Feb. 24, 2018) (explaining how bank customers can use a token as an additional security measure against unauthorized access to account information).

[161] *See Tokens,* FREEMONT BANK, www.freemontbank.com/business/business-banking/online-banking/tokens [https://perma.cc/73AU-UDGU] (last visited Feb. 24, 2018).

Mobile Two-Factor Authentication is primarily limited to software-based solutions.[162] There are three main software-based solutions—Google Authenticator, Authy, and FreeOTP. The use of 2FA for both personal and professional accounts may be considered a best practice. For professional accounts, 2FA should be established on any account or login that contains clients' information; ideally that includes access to files, emails, and other communication platforms used by a lawyer and his firm or legal organization. For personal accounts, implementation is recommended to reduce the ability of malicious actors to compromise professional accounts by gaining access to personal accounts and the information they contain.

### 3. Encryption

### *a. The Risks*

### i. Data at Rest

A course in cryptography would likely be necessary to provide a complete understanding of encryption. However, a basic understanding and the routine use of encryption should fulfill a lawyer's duty of competence and confidentiality to his clients. Encryption is the method by which data is scrambled so that only authorized users can understand that data.[163] An unauthorized party can determine that the data exists, but in its encrypted form, an unauthorized party sees only a string of unintelligible letters, numbers, and symbols.[164]

Encryption has been analogized to sending information in a sealed envelope instead of on a postcard. A postcard allows anyone to read the information, whereas a sealed envelope hides the information from plain view—only the person to whom the envelope is addressed may view its contents.[165] Encryption is platform agnostic, meaning that the cryptographic protocols (i.e., encryption protocols) are based on sequences and algorithms that function the same way regardless of the user's system.[166] One example is the Advanced Encryption Standard (AES), which was adopted by the U.S. National Institute of

[162] Rakesh Thatha, *Limitations of Two Factor Authentication (2FA) Technology,* COMPUT. WKLY. (Sept. 2012), http://www.computerweekly.com/tip/Limitations-of-two-factor-authentication-2FA-technology [https://perma.cc/KJ6F-QKN6]. An exploration of Near Field Communication (NFC) solutions is beyond the scope of this article and are unavailable on iOS and Android.

[163] *Encryption*, TECHOPEDIA, https://www.techopedia.com/definition/5507/encryption [https://perma.cc/7R2B-FQW8] (last visited Feb. 24, 2018).

[164] *See id.*

[165] *See* David G. Reis, *Safeguarding Confidential Information Attorneys' Ethical and Legal Obligations*, ABA (Apr. 2016), https://www.americanbar.org/content/dam/aba/events/law_practice_management/2016/SpringMeeting/CybersecurityLPSpring Meeting2106.authcheckdam.pdf [https://perma.cc/RG87-65N5].

[166] *See id.*

Standards and Technology (NIST) in 2001[167] and later made a standard for encryption of all state secrets.[168] AES has different key sizes: 128-, 192-, and 256-bit keys. The difference in key sizes determines how many times a particular set of data goes through encryption rounds.[169] Simply stated, the larger the key, the stronger the encryption; the stronger the encryption, the harder it is to breach.

Three types of data that may be encrypted: data at rest, data in use, and data in transit. Data at rest is data that is stored on a device but is not being accessed or processed by the device (e.g., data that resides on a laptop or mobile device).[170] The good news for lawyers is that encryption of data at rest (or when the phone is locked and not in use) is enabled by default for both iOS[171] and Android[172] devices. It is important to note that techniques do exist to breach the encryption of data at rest (commonly referred to as "exploits"), but these techniques are complex and rare.[173] Thus, a lawyer attentive to his duty of technological competence may generally rely upon the baseline encryption that is provided by Apple and Google to protect information when

[167] *See Announcing the Advanced Encryption Standard (AES)*, NAT'L INST. STANDARDS & TECH. (Nov. 26, 2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [https://perma.cc/4H7Q-V7RE].

[168] *See Cryptographic Standards and Guidelines*, NAT'L INST. STANDARDS & TECH., https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development [https://perma.cc/HE97-XXRD] (last updated Feb. 12, 2018).

[169] *See id.*

[170] Nate Lord, *Data Protection: Data in Transit vs. Data at Rest*, DIGITAL GUARDIAN (Jan. 15, 2018), https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest [https://perma.cc/YU62-AEN8].

[171] *See iOS Security: iOS 10*, APPLE (Jan. 2018), https://www.apple.com/business/docs/iOS_Security_Guide.pdf [https://perma.cc/XPF8-26AP].

[172] *Full-Disk Encryption*, ANDROID OPEN SOURCE PROJECT (Dec. 18, 2017), https://source.android.com/security/encryption/full-disk [https://perma.cc/Y69W-P6XF].

[173] Device-based encryption vulnerabilities are present in both Android and iOS devices, and new methods continue to be discovered. *Content & Services Customer Support*, SAMSUNG, https://help.content.samsung.com/csweb/faq/searchFaq.do [https://perma.cc/LMM7-ANEU] (last visited Dec. 9, 2017). For example, malicious actors can unlock Samsung phones remotely, so long as the user has a Samsung account and leaves the phones' remote controls enabled. *Id.* Apple, on the other hand, recently corrected an exploit that enabled users to gain access to contacts and photos from the lock screen, and also allowed full access to the device beyond the lock screen through Siri. *See About the Security Content of iOS9.0.2*, APPLE, https://support.apple.com/en-us/HT205284 [https://perma.cc/TV98-65H2] (last visited Mar. 24, 2018); *see also* iDeviceHelp, *How to Unlock ANY iPhone Without Passcode Access Photos, Contacts & More iOS 9/10 – 10.2*, YOUTUBE (Nov. 15, 2016), https://www.youtube.com/watch?v=LWJG5I8xCDU [https://perma.cc/RD2C-V6UY]. Just last year, the United States government paid $900,000 for the use of an exploit to unlock the iPhone owned by the San Bernardino shooter. Eric Tucker, *Senator Reveals that the FBI Paid $900,000 to Hack into the San Bernardino Killer's iPhone*, BUS. INSIDER (May 8, 2017, 9:26 AM), http://www.businessinsider.com/dianne-feinstein-fbi-paid-900000-to-hack-into-san-bernardino-iphone-2017-5 [https://perma.cc/ZU9P-4NK2]. The method employed remains undisclosed and it is uncertain whether it has been fixed. *Id.*

their phones are locked and not in use. Lawyers should also be aware of the Apple and Google solutions to remotely erase a lost or stolen device. The remote erasure solution protects access to confidential information; hackers perpetrating the rare, complex instances of breaking into the phone's encryption usually require physical access to the mobile device.

### ii. Data in Transit

Data in transit is data that travels through a network.[174] That network may be local (computer-to-computer on a private network) or public (over the internet). Using a smartphone to search the Internet is akin to using a traditional computer, so the security precautions and security mishaps that may occur from a desktop or laptop computer also apply when using a smartphone to access the Internet via WiFi.[175] In fact, the manner in which data is transferred over the Internet is often misunderstood such that many people, including lawyers, fail to both appreciate the vulnerabilities and the need for securing Internet connections.

The idea that connecting to a website simply involves typing a URL or website address into an Internet browser is a common misperception. In fact, a computer (or mobile device) that attempts to connect and download data from a particular website must first determine the Internet Protocol address ("IP address") of the server where the website is hosted.[176] An IP address is similar to a phone number in that every device has one, and a device's search for an IP address is analogous to a search for a phone number in a telephone directory (e.g. Yellow Pages) or calling 411: a computer searches Domain Name Systems ("DNS") to match the URL (e.g., www.reasonablesolutions .com) to an IP address (e.g., 127.0.0.1).[177] DNS servers are operated by an Internet Service Provider ("ISP").[178] Companies such as Google and Cisco operate public DNS servers. DNS requests are temporarily stored locally on a computer in order to speed up the process for accessing frequently used websites, which is similar to creating a contact

[174] Nate Lord, *Data Protection: Data in Transit vs. Data at Rest*, DIGITAL GUARDIAN, https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest [https://perma.cc/VVL9-7P38] (last updated Jan. 15, 2018).

[175] Using a smartphone via WiFi rather than the default cellular data connection has the same risks as a computer connected to WiFi. Nadia Kovacs, *How Safe is Surfing on 4G vs. WiFi?*, NORTON, https://community.norton.com/en/blogs/norton-protection-blog/how-safe-surfing-4g-vs-wi-fi [https://perma.cc/UDX4-RQZ6] (last visited Feb. 28, 2018). Cellular data connections can be compromised, but it takes a far more skilled and resourceful agent, which is most often a state actor. *Id.*

[176] *What is an IP Address? What Does it Do?*, WHATISMYIPADDRESS.COM, https://whatismyipaddress.com/ip-address [https://perma.cc/46AP-8NPX] (last visited Feb. 28, 2018).

[177] *See id.*

[178] *See id.*

on a mobile device to associate a phone number with a person's name.[179]

All of the data transmitted in a search or a download can be received in an encrypted manner or in an unencrypted manner.[180] Transport Layer Security ("TLS") or Secure Sockets Layer ("SSL") encrypts data between the application making the request and the servers where the information is stored.[181] For example, a website that has the header "HTTPS" instead of "HTTP" is encrypting the data transmitted between a device and its servers.[182]

DNS and the transmission of data are the two most significant and vulnerable attack vectors. Most users are unaware of the ease with which someone may take advantage of these vulnerabilities. Cyberattacks no longer require a deep, cunning understanding of the Internet to hijack a user's Internet presence: there are many off-the-shelf products that assist someone with a low-to-moderate level of skill in performing so called "Man-In-The-Middle" attacks.[183]

For example, DNS spoofing is a type of attack that can be perpetrated with relative ease.[184] DNS spoofing occurs when a malicious actor tricks a person's computer into "thinking" that the malicious actor is a DNS server, and then selects and sends an IP address to the searching computer.[185] To illustrate, the malicious actor might establish and direct an individual to a fake Google or Facebook login page. Having arrived at the fake login page, the individual will likely attempt to access the site and will receive a wrong password error message after every attempt to enter a password. Meanwhile, the fake site will log every credential that the user enters in attempting to log into the website. The unsuspecting individual often enters the various passwords he or she uses on all of their accounts hoping to remember the correct one. In the process, the malicious actor sees and stores all of these passwords.

SSL or HTTPS stripping is another simple form of attack.[186] HTTPS stripping sees the malicious actor standing in as the Man-in-

[179] *DNS Server*, TECHOPEDIA, https://www.techopedia.com/definition/28503/dns-server [https://perma.cc/SD4W-EM2B] (last visited Feb. 24, 2018).

[180] *See Cryptographic Standards and Guidelines*, *supra* note 168.

[181] *What is SSL, TLS, and httpS?*, SYMANTEC, https://www.symantec.com/page.jsp?id=ssl-information-center [https://perma.cc/DG44-A8WC] (last visited Feb. 24, 2018).

[182] *See id.*

[183] *What is a Man in the Middle Attack*, SYMANTEC, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html [https://perma.cc/RS9M-F3FB] (last visited Feb. 24, 2018).

[184] *See What Is DNS Spoofing?*, KEYCDN (July 16, 2017), https://www.keycdn.com/support/dns-spoofing/ [https://perma.cc/ME9J-S76U].

[185] *See id.*

[186] Chris Sanders, *Understanding Man in the Middle Attacks – Part 4: SSL Hijacking*, TECHGENIX (June 9, 2010), http://techgenix.com/understanding-man-in-the-middle-attacks-arp-part4/ [https://perma.cc/M2KR-NCGW].

the-Middle, preventing an individual from achieving a secure connection to any website that the target may attempt to reach.[187] The malicious actor logs all transmitted data, and when the target enters his or her credentials to log into the real Google or Facebook, his or her user name and password are transmitted as plain text (i.e., unencrypted) and easily readable by the malicious actor.[188] The attack may be entirely hidden from the individual user.[189]

Even setting these Man-In-The-Middle attacks aside, accessing public WiFi with a smartphone remains a dangerous endeavor. Both Android and iOS have been susceptible to malicious code implemented over WiFi.[190] Attacks over the Internet or through a hijacked Internet connection are becoming more complex, while simultaneously becoming more accessible to the malicious actor. Thus, a rudimentary understanding of how the Internet works, as well as basic knowledge of methods of attack allows a user with any degree of technological skill to appreciate how certain reasonable practices protect their data.

### *b. Solutions*

#### i. Full-Phone Encryption

As discussed above, most smartphone manufacturers designed phones to be fully encrypted when in default mode, meaning locked and not in use. The security concern arises when the phone is unlocked and the user is searching the Internet, emailing, or messaging. Thus, ensuring that the phone is locked via a default password when not in use is paramount to securing data at rest. Apple recently increased security measures by changing the default iPhone password to six-digits from four-digits; however, six-digit codes can still be cracked in a matter of minutes.[191] Put more simply, encryption is only as strong as the password assigned to it; in properly skilled hands, physical access to a mobile device coupled with a weak password is nearly as useless as having no password at all. There are three recommendations that may be implemented on any phone that has access to client data to alleviate the risk of inadvertent disclosure: (1) ensure that you allow your data to be erased after a certain number of password fail-

[187] *See id.*

[188] *See id.*

[189] *See id.*

[190] *See* Dan Goodin, *Android Devices Can Be Fatally Hacked by Malicious Wi-Fi Networks*, ARSTECHNICA (Apr. 5, 2017, 3:46 PM), https://arstechnica.com/security/2017/04/wide-range-of-android-phones-vulnerable-to-device-hijacks-over-wi-fi/ [https://perma.cc/5PTY-T9CR]; *see also See About the Security Content of iOS 10.3.1*, APPLE, https://support.apple.com/en-us/HT207688 [https://perma.cc/4VZV-X9DY].

[191] Cadie Thompson, *Apple made a simple change in iOS 9 that will make your iPhone a lot safer*, BUS. INSIDER (Sept. 22, 2015, 4:00 PM), http://www.businessinsider.com/ios-9-defaults-to-6-digit-passcode-2015-9 [https://perma.cc/ST3E-9RT9].

ures, this protects against brute force attacks;[192] (2) switch from digit-only passcodes to passphrases, and implement a strong, secure password;[193] and (3) enable the mobile device's fingerprint reader to ensure that mobile device use is as convenient as it is secure.[194]

### ii. Virtual Private Network ("VPN")

A virtual private network functions as a virtual "tunnel" through which information may be securely transferred across the Internet.[195] The tunneling or encapsulation of data encrypts the entire transmission from one end of the virtual tunnel to the other.[196] A smartphone may access and use a VPN either via an application installed on the phone or through profiles that organizations may provide to employees.[197] Both individuals and organizations can establish VPNs to encrypt Internet traffic using one of two methods.[198] A private VPN may be established or a VPN may be obtained from a third-party VPN service provider.[199] Some larger firms and organizations establish private VPNs and require all of the members of the firm or organization to use the VPN to access any data that is stored on the firm or organization's servers.

Smaller firms, solo practitioners, and individuals often contract with a VPN service. However, selection of the service implicates the legal ethics outsourcing concerns discussed above so the buyer must be cautious. Concerns as to pricing aside, the confidentiality of information,

[192] *See iCloud: Erase your device*, APPLE (Feb. 1, 2018), https://support.apple.com/kb/ph2701?locale=en_US [https://perma.cc/8PB3-HVUL] (for Apple devices); *see also Find, lock, or erase a lost Android device*, GOOGLE, https://support.google.com/accounts/answer/6160491?hl=en [https://perma.cc/D79B-CFAJ] (last visited Feb. 28, 2018).

[193] *See Use a passcode with your iPhone, iPad, or iPod touch*, APPLE (Nov. 16, 2017), https://support.apple.com/en-us/HT204060 [https://perma.cc/9HQY-KPEH] (for Apple devices); *see also Set screen lock*, GOOGLE, https://support.google.com/android/answer/2819522?hl=en&ref_topic=7340889 [https://perma.cc/RN6J-F6H5] (last visited Feb. 28, 2018).

[194] *See generally Use Touch ID on iPhone and iPad*, APPLE (Nov. 7, 2017), https://support.apple.com/en-us/HT201371 [https://perma.cc/NMX2-PNJZ] (explaining Apple Touch ID); *see also About Face ID Advanced Technology*, APPLE (Dec. 20, 2017), https://support.apple.com/en-us/HT208108 [https://perma.cc/P8SR-DGF5] (explaining Apple Face ID). For Android, please consult the specific device you have—not all Android devices support fingerprint unlocking.

[195] Andrew Tarantola, *VPNs: What They Do, How They Work, and Why You're Dumb for Not Using One*, GIZMODO (Mar. 26, 2013, 3:30 PM), https://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one [https://perma.cc/B6TL-7AF4].

[196] Lee Matthews, *What A VPN Is, And Why You Should Use It To Protect Your Privacy*, FORBES (Jan. 27, 2017, 4:00 PM), https://www.forbes.com/sites/leemathews/2017/01/27/what-is-a-vpn-and-why-should-you-use-one/#3f6a22e4b8f1 [https://perma.cc/4F87-PH89].

[197] Tarantola, *supra* note 195.

[198] *See id.*

[199] *See id.*

the process for notice when there may be vulnerability, and the assurance that data is not being captured and sold are all considerations.[200] The legal ethics rules and opinions that explain competence as the need to understand the benefits and disadvantages of technology, whether by acquiring knowledge or by hiring a qualified nonlawyer, are also applicable to the selection of a VPN service provider.

### 4. Messaging

#### *a. The Risks*

In the past ten years, myriad methods of communication have provided mobile device users with the means to transmit text well beyond simply emailing.[201] Lawyers now use Short Message Service ("SMS") (or text messages), iMessage, and other platforms to communicate with each other in real time. These messages may contain important and sensitive information such as a client's name, case number, facts

[200] There are many on the internet who spend a lot of time and money researching these sorts of considerations. The largest wealth of information on the various third-party VPN solutions can be found on "That One Privacy Site." *See Detailed VPN Comparison Chart*, THAT ONE PRIVACY SITE, https://thatoneprivacysite.net/vpn-comparison-chart/ [https://perma.cc/KSE5-GULL] (last updated Feb. 28, 2018).

[201] Email, regardless of whether it is accessed on a smart device or computer, is subject to attack vectors such as phishing and man-in-the-middle attacks. *See* David G. Ries, *Safeguarding Confidential Information Attorneys' Ethical and Legal Obligations*, ABA (May 13, 2016), https://www.americanbar.org/content/dam/aba/events/law_practice_management/2016/SpringMeeting/CybersecurityLPSpringMeeting2106.authcheckdam.pdf [https://perma.cc/LF3A-474H]. Email is especially dangerous for lawyers because the sensitive information they possess is often attached to their email accounts. For example, a bank may use an email for a password reset for online access to a bank account. Once a malicious actor has access to that user's email (or is able to intercept it), that actor can fairly quickly determine the user's accounts and reset all of his or her passwords to gain access to client's files, information, and money (in some cases). (Yet another reason for avoiding the use of the same password for all of a user's accounts—fewer passwords may lead to greater damage.) In fact, some technology experts controversially advocate abandoning the use of email. *See, e.g.*, Ansel Halliburton, *Secure Messaging for Lawyers,* LAWYERIST (Jan. 23, 2017), https://lawyerist.com/secure-messaging-lawyers/ [https://perma.cc/498J-W2MP]; *see also* Andy Ninh, *Why Lawyers Should Use Slack and Eliminate Email,* (Oct. 6, 2015), http://www.andyninh.com/blog/2015/10/7/why-lawyers-should-use-slack-and-eliminate-email [https://perma.cc/5SHH-5ZY6]. The suggestion stems from the fact that email passes through multiple servers before it reaches the intended recipient and opens up multiple attack vectors for each email sent, including interception and DNS spoofing, even if the user is on a secure network. Moreover, using an email account on a public, unsecured WiFi adds another serious vulnerability to the entire chain. Finally, even if an email is sent without any problems, there still may be concern about the recipient's security practices. Understanding that ceasing the use of email is unlikely for most organizations, the next best reasonable practice is the continued use of encryption with email—both for the email itself and the email attachment when appropriate. Generally speaking, third-party solutions such as Outlook 360 or Gmail, securely store emails so users do not need necessarily to download and encrypt emails. Encryption of a document has become a fairly user-friendly process—it may be done directly from some document programs, such as word, or through the use of an encryption application.

of the case, or information necessary for a hearing. Confidentiality risks arise when lawyers assume that messages sent from one phone to another are secure and accessible only by the person to whom the message was sent.

The assumption is flawed in many cases, especially for lawyers who use regular SMS to communicate with other lawyers or employees in their organization. Eavesdropping and spying through SMS interception is not new.[202] In fact, in 2007, a Wal-Mart employee was fired for eavesdropping on cell phone calls and SMS conversations.[203] Since the Wal-Mart event, SMS methods of interception have become more complex, and in July of 2016, the National Institute for Standards and Technology ("NIST") reported that the use of SMS for two-factor authentication was no longer secure.[204] And in December 2016, the NIST stated that a high likelihood of interception renders SMS communication and authentication unreliable.[205]

Frequently, upon learning about the risks in SMS communication, many individuals, including lawyers, make the assumption that they are unlikely to be the target of such an attack. But this kind of assumption is as unsafe and illogical as leaving the doors to an office filled with confidential documents unlocked because it is unlikely to be burglarized. Although hackers will need to be relatively sophisticated in order to hack into SMS messages, lawyers are high-value targets, and therefore reasonable objects of sophisticated attacks. Moreover, as discussed above, the Rules of Professional Responsibility require lawyers to protect against reasonable intrusions.

### *b. Solutions*

One solution is to refrain from using regular SMS to communicate sensitive information to clients, other lawyers, and employees at your organization. Instead a lawyer might use a messaging platform such as iMessage—an end-to-end encrypted platform that may be used to securely communicate from one iPhone to another.[206] End-to-end encryption uses encryption keys so that only the devices in use can read the messages.[207] An attacker would require physical access to the mo-

[202] *See, e.g.,* Christopher Beam, *How Do You Intercept a Text Message?*, SLATE (Mar. 7, 2007, 6:53 PM), http://www.slate.com/articles/technology/technology/2007/03/how_do_you_intercept_a_text_message.html [https://perma.cc/4X4X-V8WM].

[203] *See id.*

[204] *See Digital Identity Guidelines*, NAT'L INST. STANDARDS & TECH. (Dec. 10, 2017, 4:38 PM), https://pages.nist.gov/800-63-3/sp800-63b.html [https://perma.cc/Y48E-SUH2] at Section 5.1.3.2.

[205] *See id.* at Table 8-1.

[206] *Approach to Privacy*, APPLE, https://www.apple.com/privacy/approach-to-privacy/ [https://perma.cc/ZP2Y-98RX] (last visited Feb. 28, 2018).

[207] Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [https://perma.cc/B6WF-8THL].

bile devices in the message thread or an extremely complex method of attack in order to read the messages.[208] iMessage, however, does not remain secure when used with other messaging platforms. In other words, if an Android user joins the messaging group, the entire conversation is converted into an insecure SMS conversation.

Another method to ensure confidentiality and prevent accidental disclosure of information would be for an entire law firm or legal organization to adopt a single, cross-platform, end-to-end, encrypted messaging application. Four of the most popular cross-platform, end-to-end, encrypted messaging apps are WhatsApp, Telegram, Signal, and Wire.[209]

Facebook purchased WhatsApp in 2014 and has since begun mining and collecting the metadata for every message sent and received.[210] This metadata includes when a user's account was activated, when it was last opened, who was contacted, the address book on the device used, phone numbers, and location information.[211] Metadata can be used with precision to obtain a great deal of information about a message sender.[212] In fact, former National Security Agency Director General Michael Hayden is quoted as having said, "We kill people based on metadata."[213] Many state ethics opinions already require reasonable care when handling metadata that may reveal confidential information.[214]

Telegram, although famously used by ISIS to promote terror,[215] is not encrypted by default and does not have the ability to access encrypted chats via its desktop application. Like WhatsApp, Telegram has a metadata leakage problem that can be used to compromise sen-

[208] *See id.*

[209] John E. Dunn & Thomas Macaulay, *Best Secure Mobile Messaging Apps*, TECHWORLD (Feb. 12, 2018), https://www.techworld.com/security/best-secure-mobile-messaging-apps-3629914/ [https://perma.cc/P974-T3TH].

[210] Natasha Lomas, *WhatsApp to Share User Data With Facebook For Ad Targeting – Here's How to Opt Out*, TECHCRUNCH (Aug. 25, 2016), https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/ [https://perma.cc/3KBE-JX8A].

[211] Thomas Fox-Brewster, *Forget About Backdoors, this is the Data WhatsApp Actually Hands to Cops*, FORBES (Jan. 22, 2017, 10:00 AM), https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#7676a2ed1030 [https://perma.cc/8HXL-NUDF].

[212] *Former CIA Director: "We Kill People Based on Meta-Data"*, RT (May 12, 2014, 6:27 PM), https://www.rt.com/usa/158460-cia-director-metadata-kill-people/ [https://perma.cc/MM8R-R9EX].

[213] *See id.*

[214] *Metadata Ethics Opinions Around the U.S.*, ABA, https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html [https://perma.cc/3ZC5-DCF7] (last visited Feb. 24, 2018).

[215] Joby Warrick, *The 'App of Choice' for Jihadists: ISIS Seizes on Internet Tool to Promote Terror*, WASH. POST (Dec. 23, 2016), https://www.washingtonpost.com/world/national-security/the-app-of-choice-for-jihadists-isis-seizes-on-internet-tool-to-promote-terror/2016/12/23/a8c348c0-c861-11e6-85b5-76616a33048d_story.html [https://perma.cc/RZ8Z-JAVJ].

sitive information.[216] In fact, both WhatsApp and Telegram contain serious vulnerabilities.[217]

While platforms like Signal and Wire are not perfect solutions, they may be the best alternatives available for lawyers at the time of the writing of this Article.[218] Both applications transmit a user's contact list to its servers.[219] Signal encrypts this information, but Wire does not.[220] Signal requires users to find other users via cell phone numbers, while Wire allows a search for users by user-name without providing any personal contact information.[221] Finally, both services are open sourced, have been formally audited by the cryptography community, and have received positive results from their audits.[222]

Depending on personal preferences and privacy concerns, a lawyer deciding to use a messaging app may select Wire because it does not require users to share their personal phone numbers. However, many employees who work remotely likely share personal phone numbers to ensure necessary availability and access. So, if sharing a phone number does not create an impediment, then Signal would likely be the preferred method of communication for a lawyer as it is deemed the most sophisticated encrypted messaging platform.[223]

### 5. Final Thoughts on Legal Ethics, Vendors & Devices

Malicious actors, phishing, doxxing, data encryption—these are terms that have not typically been found in casebooks or on law school syllabi. Legal education and the legal profession are slowly adapting to society's rapid technological change. The Code of Professional Conduct and the ABA's 2012 amendments to the comments of the rules regarding the definition of competence, the reasonable efforts required to maintain confidentiality, and the enhanced standard

[216] Joseph Cox, *Encrypted Messaging App Telegram Leaks Usage Data*, MOTHERBOARD (Nov. 28, 2015, 11:30 AM), https://motherboard.vice.com/en_us/article/encrypted-messaging-app-telegram-leaks-usage-data [https://perma.cc/QW3C-TGY3].

[217] Andy Greenberg, *Whatsapp Hack Shows That Even Encryption Apps are Vulnerable in a Browser*, WIRED (May 15, 2017, 3:39 PM), https://www.wired.com/2017/03/whatsapp-hack-shows-even-encryption-apps-vulnerable-browser/ [https://perma.cc/ZE5G-7VU6].

[218] David Kennedy, *Wire Messenger – A New Competitor to Signal and More?*, TRUSTEDSEC (Dec. 24, 2016), https://www.trustedsec.com/2016/12/wire-messenger-new-competitor-signal/ [https://perma.cc/S27A-TLCH].

[219] *See id.*

[220] *See id.*

[221] *See id.*

[222] Natasha Lomas, *Messaging App Wire Now Has an External Audit of its e2e Crypto*, TECHCRUNCH (Feb. 10, 2017), https://techcrunch.com/2017/02/10/messaging-app-wire-now-has-an-external-audit-of-its-e2e-crypto/ [https://perma.cc/D8D2-4MFV]. Emma Whitehead, *Signal's Protocol Gets Glowing Reviews in First Security Audit*, CYBERSCOOP (Nov. 8, 2016), https://www.cyberscoop.com/signal-security-audit-encryption-facebook-messenger-whatsapp/ [https://perma.cc/JG3P-RAB2].

[223] Whitehead, *supra* note 222.

for supervision of nonlawyer assistance all reflect recognition of the need for lawyers to evolve with the times.

Lawyers must strive to understand both the benefits and disadvantages of technology in order to both provide effective, ethical representation and to remain competitive. The technological suggestions in this Article offer a snapshot of some precautions in the here and now—specific solutions may become rapidly outdated. The larger takeaway is that lawyers must be aware of the impact of technology—specifically on their legal ethics obligations and generally on the practice of law. Moreover, Artificial Intelligence, whether regarded as a blessing or a curse, has arrived.

## IV. CONCLUSION

> "[S]ociety can only be understood through a study of the messages and the communication facilities which belong to it; and that in the future development of these messages and communication facilities, messages between man and machines, between machines and man, and between machine and machine, are destined to play an ever-increasing part."
>
> —Norbert Wiener[224]

Norbert Wiener, a prominent mathematician and philosopher, envisioned a future society in which machines would play a prominent role in "messages and communication facilities."[225] No doubt, Max Tegmark's current concerns over the development of AI stem from the fact that society has evolved as Wiener predicted.[226] Wiener's neutral statement about the growing impact of machines must now be infused with ethical and goal oriented understanding.

To pretend that AI is not changing every aspect of society is to ignore a vast amount of evidence. While lawyers are generally behind the curve when it comes to embracing technology, they are nonetheless skilled at curating evidence. And while some lawyers fear that robo-lawyers will replace human lawyers, many innovative legal minds envision a legal profession in which attorneys shed the burden of mundane tasks and spend more time engaged in the higher-level aspects of lawyering. These innovators also believe that AI has the potential not only to create a new type of "legal-tech" employment, but also to increase access to justice for millions of individuals.

AI's capabilities are increasing at a dizzying pace. The legal profession, known for coming late to the technology dance, should step in now to take control of AI's impact on the profession, rather than looking back in a few years and wondering, "What happened?" After

[224] *See* RALPH PARKMAN, THE CYBERNETIC SOCIETY: PERGAMON UNIFIED ENGINEERING SERIES 5 (1972).

[225] *Id.*

[226] *See* TEGMARK, *supra* note 25.

all, “[t]he only way to make sense out of change is to plunge into it, move with it, and join the dance.”[227]

[227] Alan Watts, *The Wisdom of Insecurity*, ORGANISM, http://www.organism.earth/library/document/52 [https://perma.cc/FCZ5-9U89] (last visited February 24, 2018).