In 2019, there is no shortage of media attention focused on the legal and ethical complications of our post-digital world: From the daily deluge of hacks and data-leaks to the increasing use of (often biased) algorithmic predictions in consumer and criminal contexts. But for far too long, the legal profession, as a whole, has sat on the sidelines, waiting for legislative solutions to magically solve our emerging crisis of privacy while failing to adequately update “standard” attorney-client procedures and litigation strategies to meet the demands, and opportunities, of our new technological environments.

In short, emerging technology will present a number of challenges for attorneys in Nebraska and nation-wide. Increasingly, our clients—even when dealing with seemingly routine civil and criminal issues—will have tech-related challenges requiring assistance and legal expertise. Technology will also—as it has in virtually every other sector of our economy—fundamentally change the practice of law as encryption, automation, and artificial intelligence become the new normal in our courthouses and client consultations. Whether our goal is to thrive as practicing attorneys or meet our professional civic obligations to ensure that due process and privacy rights are preserved for all citizens, lawyers must work to become familiar with and conversant about technology.1

Emerging Technology: Understanding the Terms

Rapid advances in technology are changing the world in ways that will affect every type of legal practice. A family law firm may be confronted with a messy divorce that requires the division of marital assets which include bitcoin. A criminal attorney may have to defend a client who was arrested based on being identified by facial recognition technology. The sheer breadth of the

---

**Thomas J. Freeman**

( JD, MS, MBA, Creighton University) works as an attorney for Governmental Law, LLC, where he provides legal guidance to county governments. He is also an Adjunct Professor at both Creighton University School of Law and Heider College of Business. His research is focused on fiduciary duties, business ethics, behavioral economics, and the legal and ethical issues posed by big data, predictive analytics, artificial intelligence, fintech, and other emerging technologies. Tom is a former Assistant Attorney General for the State of Nebraska.

---

**Prof. Aaron McKain**

(Ph.D., M.S.L., Ohio State University) is the Director of English, Digital Media, and Communication Arts at North Central University in Minneapolis. For fifteen years, his research on digital ethics, law, and politics has been featured in academic journals, local news broadcasts, a college textbook, and, most recently, the Czong Center for Contemporary Art in Korea. He is a native Nebraskan and a proud former member of the Nebraska Appleseed Center for Law in the Public Interest.
changes in store for the practice of law is encapsulated by the very definition of “cyberlaw,” which has already grown to include the law of the Internet, computer law, e-commerce law, copyrights, trademarks, domain disputes, contracts, patents, defamation, and data retention, to name just a few pertinent topics.2

All attorneys, regardless of their practice areas, will need to become more educated about how technology is affecting the areas they practice in. As the pace of technological progress continues to accelerate, it can be difficult to keep track of the different advancements we should be aware of. What follows is a non-comprehensive list of some of the technologies to be aware of – for novices – as well as a brief guide to the ethical and legal complications that have already begun to arise from them. Above all, this article is to serve as a quick primer – and gentle call to arms – for those members of the Nebraska Bar who have yet to take the leap into this new (and potentially lucrative) digital frontier of law.

Artificial Intelligence, Machine Learning, and Algorithmic Discrimination

Artificial intelligence (also “AI”) is the study of programmable agents that perceive the world around them, form plans, and make decisions to achieve their goals.3 The goal of AI is to create machines to perform human-like tasks.4 Its foundations include mathematics, logic, philosophy, probability, linguistics, neuroscience, and decision theory.

Machine learning is a subfield of artificial intelligence. Its goal is to enable computers to learn on their own.5 A machine’s learning algorithm enables it to identify patterns in observed data, build models that explain the world, and predict things without having explicit pre-programmed rules and models. It is the process by which a machine can be trained to learn, with the ultimate goal of thinking like a human. The reality is that in some respects, AI has proven to be similar to human thinking, for good and bad.

The pace of developments in artificial intelligence is staggering. AI programs have proven the ability to easily defeat the very best human opponents at games as complex as chess and Go.6 In the last month, researchers taught an AI program how to beat a combination of human and computer players in a multiplayer game.7 Each of these feats was once thought impossible for a computer program. But programmers can design a system with the ability to learn and then provide it with hundreds of thousands or even millions of repetitions to learn from. The programs can – allegedly – be designed to be free from human experiences and biases, which allows them to develop new strategies for gameplay that humans have never considered or employed.

That said, emerging research in the fields of digital humanities and digital ethics have begun to reveal, unsurprisingly, that human and statistical biases are often programmed into everyday AI: From predictive analytics in policing to new forms of digital “redlining” which actively discriminate based on race, class, and gender categories. Not only does this digital discrimination (and “micro-targeting”) often occur beneath the notice of the disadvantaged users, algorithmic statistical prejudices are sometimes even beyond the awareness of the programmers. And as humans and robotics become more and more intertwined, legal questions of human agency and liability will become necessarily more complex and thorny as robotic systems (from automated cars to the “internet of things”) begin to collaborate with humans to perform daily activities.

Blockchain, Encryption, and Privacy Law

Blockchain is a system of data recording, where each block is the digital record of a transaction. The block contains the date, time, amount, and information about the participants in the transaction. The technology itself makes it difficult to hack. Each block has a unique code, which is incorporated into subsequent blocks in the chain. A hacker would have to change the code of innumerable blocks in order to mask his activities. That would be very difficult and require an immense amount of computing power.8 Bitcoin is probably the most recognized application of blockchain technology, but the technology could be used in virtually any field. Matthew McKeever’s recent article in the November/December 2018 issue of The Nebraska Lawyer provides a deeper look into bitcoin currency and blockchain technology generally.9
AS TECHNOLOGY EVOLVES, SO DOES THE PRACTICE OF LAW, AND SO MUST ATTORNEYS

The chief motivations of blockchain- and all encryption innovations- are, of course, privacy and security. Currently the central battle in our post-digital legal world, privacy law deals with how information or data about individuals or entities can be collected, stored, transferred, sold, or monetized. In 2019, it is almost not hyperbole to say that every company is collecting (or attempting to collect) data about consumers, which it then stores, processes, uses, and monetizes. The amount of data gathered can be very extensive.

Google, for example, collects: your bookmarks; your contacts; your Google Drive files; your YouTube videos; the photos you’ve taken on your phone; the businesses you’ve bought from; the products you’ve bought through Google; data from your calendar; your Google hangout sessions; your location history; the music you listen to; the Google books you’ve purchased; the Google groups you’re in; the websites you’ve created; the phones you’ve owned; the pages you’ve shared; how many steps you walk in a day; every email you have ever sent or received, including those that were deleted or categorized as spam; every Google Ad you have ever viewed or clicked on; every app you have ever launched or used and when you did it; and every website you have ever visited and what time you did it at; and every app you have ever installed or searched for.

In the United States, HIPAA is probably the best-known example of a privacy law. In Europe, the recently passed General Data Protection Regulation (GDPR) covers data privacy regulation. There is currently no similar law in the United States with respect to data privacy. Some states have attempted to fill this void with state laws to protect individual privacy – such as the California Consumer Privacy Act (CCPA) and Minnesota’s recently failed attempts to regulate 3rd party data sales by internet service providers – but the current legal landscape is a patchwork that often fails to protect our most vulnerable post-digital citizens. (For instance, the turn toward “affirmative disclosure” in privacy regulation, which requires the companies that are collecting, storing, and processing data to also be responsible for “educating” the public about their rights re: privacy.) Whether your goal as an
As technology evolves, so does the practice of law, and so must attorneys. The nature of how we communicate with clients, courts, and other attorneys continues to change. E-filing is quickly moving from being an option to becoming a requirement. The technologies some of us rely on are increasingly obsolete. For example, the use of a fax machine is quickly becoming as outdated as using an abacus to calculate a contingency fee. Artificial intelligence and machine learning are changing the way lawyers conduct discovery. In many cases, a computer can more quickly and accurately perform an even complex review of documents than attorneys can. The computer program will still need to be programmed and trained by lawyers or those with legal training, but the bulk of the work can now be done by a computer program.

New technologies present a host of new challenges to adoption. Attorneys regularly send and receive text messages and emails, but more never pause to think about whether those texts or emails should be encrypted or what level of encryption should be required. Likewise, almost all attorneys store confidential client information on their computer systems, but never consider what measures they should take to protect that data. The American Bar Association has provided some guidance, but no hard and fast rules.

“From the ethics perspective, four rules generally govern the lawyer’s obligation to secure client data: ‘ABA Model Rule 1.1, which deals with competence; Rule 1.4, which involves communications; Rule 1.6, which covers the duty of confidentiality; and rules 5.1 through 5.3, which focus on lawyer and nonlawyer associations.’”

The scope of ABA Model Rule 1.1 was “clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology.”

The practice of law requires a mindset of continuous learning. It will be increasingly important for attorneys to bring that same philosophy to changes and advances in technology.

The legal profession has a unique opportunity to not repeat the mistakes of our recent digital past. While business and government have been, in hindsight, much too quick to rely on the “promise” of Big Data (and Silicon Valley’s assurances of privacy), scholars and researchers in the digital humanities have spent the last decade developing alternative ethical models for digital commerce and prescient (yet under-heeded) warnings about the impact of technology on our lives as citizens, employees, and consumers. (For instance, the Anti-Defamation League’s recent efforts to install algorithmic ethics in high school civics curricula, the ACLU’s privacy and technology initiatives, and our own recent pilot – with North Central University in Minneapolis – to bring digital ethics education to underserved minority communities via the student-led “Institute For Digital Humanity.”)

Technology Will Continue to Change the Way Attorneys Practice Law

Attorneys and law firms will need to adapt to and utilize new technology in order to practice effectively. The nature of how we communicate with clients, courts, and other attorneys...
in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.20

The ABA rules related to data security largely use a ‘reasonable efforts’ standard and decline to impose specific requirements. Attorneys should employ a fact-based analysis and employ reasonable security to fit the particular situation created by the client, case, and circumstances.21 In general terms, attorneys are required to:

1. Understand the Nature of the Threat
2. Understand How Client Confidential Information is Transmitted and Where It Is Stored
3. Understand and Use Reasonable Electronic Security Measures
4. Determine How Electronic Communications About Client Matters Should Be Protected
5. Label Client Confidential Information
6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security
7. Conduct Due Diligence on Vendors Providing Communication Technology

The basic level of encryption that most popular email providers support is HTTPS encryption.23 While HTTPS will prevent others in the network from reading a message, the email provider will still have an unencrypted copy of the communication.24 Governments and law enforcement agencies may be able to access that data with a warrant.25 A higher level of encryption, such as PGP, may be a good option for making communications more secure.26 Even PGP has come under fire however, with some opining that secure online portals are more secure options.27 Just as technology makes it easier for attorneys to communicate with our clients, it makes keeping those communications confidential more challenging. Attorneys will have to be tech-savvy enough to assess what level of security is appropriate under different sets of circumstances for their communications.

Conclusion

Society is changing rapidly, powered by incredible technological advancements. These changes will affect every attorney’s clients, regardless of his practice area. The tools that attorneys will use to communicate with clients, draft and file pleadings, and function as attorneys are changing as well. If attorneys are to competently represent clients, they must work to educate them...
As technology evolves, so does the practice of law, and so must attorneys themselves about emerging technology. And in these unprecedented technological times, it is incumbent upon us, as the guardians of the law, to help our clients and fellow citizens advocate, and litigate, for a just and equitable post-digital world.

Additional Resources

A practical guide about common types of encryption: https://www.lawtechnologytoday.org/2018/07/common-types-of-encryption/

More information about end-to-end encryption:

A look at alternatives to email that provide for more secure communications:
http://www.abajournal.com/magazine/article/alternatives_email_secure_communication

A guide for compliance with new ABA Guidelines:

Endnotes


4 Robotics Courses, edX https://www.edx.org/learn/robotics


10 Dylan Curran, “Are you ready? Here is all the data Facebook and Google have on you,” The Guardian, March 30, 2018 https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

11 Nebraska College of Law, Space and Cyber Law https://law.unl.edu/spacecyberlaw/

12 University of Nebraska-Lincoln, M.S. in Business Analytics https://business.unl.edu/online/ms-business-analytics/

13 Creighton University, M.S. in Business Analytics https://business.creighton.edu/program/business-intelligence-and-analytics-msbia

14 Creighton University, Ricketts Center in Analytics and Data Science https://business.creighton.edu/graduate/student-organizations/ricketts-center-analytics-and-data-science

15 Harvard University Online Data Science Courses https://online-learning.harvard.edu/subject/data-science

16 LinkedIn: inLearning, Blockchain: Beyond the Basics https://www.linkedin.com/learning/blockchain-beyond-the-basics/welcome

17 LinkedIn: inLearning, Data Science https://www.linkedin.com/learning/topics/data-science


20 Id., citing ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120805_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

21 Id.

22 Id.


24 Id.

25 Id.

26 Id.

27 Sean La Roque-Doherty, “Alternatives to email give law clients secure communication options,” ABA Journal, October 1, 2018 http://www.abajournal.com/magazine/article/alternatives_email_secure_communication