2024

Understanding Our Digital Fingerprints: Metadata, Competency, and the Future Practice of Law

Stacey Lane Rowland
University of North Carolina School of Law, slrowlan@email.unc.edu

Publication: *University of St. Thomas Law Journal*

ARTICLE

UNDERSTANDING OUR DIGITAL FINGERPRINTS: METADATA, COMPETENCY, AND THE FUTURE PRACTICE OF LAW

STACEY LANE ROWLAND*

I introduce my law students to the concept of metadata by showing them a picture of one of my chickens. I project a single photograph of my rooster, Mr. Roo, onto the screen in our classroom. I then ask my class, "What do you see?" I get an unsurprising range of answers, "It's a chicken" being the most common response. So far, I have never gotten the answer that I am looking for from my audience. The photo disarms the audience and even draws some laughs and smiles. The answer that I am looking for is: "I see a treasure trove of personal information." It is the metadata attached to the picture, data like the timestamp, location data, and even altitude, that masks the potential consequences of sharing this photo that most users, including practitioners, do not see or understand.

The picture is notable in that there are no people present in the photograph. There are no landmarks or buildings. Submitting the photograph to Google Reverse Image Search does not yield any surprising results.[1] I then show my students how I can figure out who owns the property where the photo was taken. This is how I introduce the concept of metadata to my

* Clinical Associate Professor of Law, Assistant Director for Collection & Technology Services, University of North Carolina School of Law & Kathrine R. Everett Law Library; J.D., Florida State University (2005), M.I.S., Masters of Information Studies, Florida State University (2005), M.S., History, Florida State University (2005), B.A., History, University of Florida (1999). I first presented my ideas for this article at the *University of St. Thomas Law Journal* Fall 2022 Symposium: *A Roadmap for Law School Modernity: Teaching Technology Competence*. I am grateful for the helpful and supportive comments I received from the faculty, students, and my colleagues there. I am also indebted to Anne Klinefelter, Julie Kimbrough, Nicole Downing, and the entire law library for their support. The KRELL Scholarship workshop contributed clarity and valuable feedback to this Article and is greatly appreciated. I also owe my thanks and gratitude to the editors of the *University of St. Thomas Law Journal*.

1. *See Search with an Image on Google*, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/1325808?hl=en&co=GENIE.Platform%3DDesktop (last visited Jan. 11, 2024).

students and how this hidden information could impact them personally, as well as professionally, in the practice of law.

FIGURE 1. THE WHITE ROOSTER.
A Rhode Island White Rooster from Stacey Rowland's Flock. His name is Mr. Roo, and he is the inspiration for this article. I use this picture to demonstrate in my classes how I can locate my own personal information. The metadata has been removed from the picture for this publication.

Metadata, often referred to as "data about data," plays a crucial role in the digital world.[2] It encompasses embedded information within electronic documents that reveals details about their creation, modification, and transmission.[3] In legal proceedings, metadata can be both helpful and controversial, as it can expose sensitive information and potentially support or refute claims of fabricated evidence.[4] With the widespread use of smartphones and other electronic devices, individuals generate vast amounts of personal data, including metadata, that can provide detailed insights into their lives. This Article explores the significance of metadata in various contexts, such as digital photographs, and highlights the ethical and practical implications

2. CRAIG D. BALL, *Beyond Data About Data: The Litigator's Guide to Metadata, in* E-DISCOVERY: RIGHT. . .FROM THE START 781, 798 (AM. L. INST. 2011).

3. *See* Larry N. Zimmerman, *Metadata Brings More Value Than Harm to Attorneys' Practice*, J. KAN. BAR ASS'N, Apr. 2009, at 24, 24.

4. *See* Crystal Thorpe, *Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" and Prohibit the "Mining" of Metadata*, 84 N.D. L. REV. 257, 257–58 (2008).

it poses for practitioners. Understanding metadata is essential for practitioners and consumers alike, as it contributes to our technological competence and raises awareness of the risks and benefits associated with personal data. In this Article, I will break up the explanation of metadata into four parts. First, I will detail my approach to teaching metadata to law students. I start with understanding what metadata is, where metadata can be found, and how metadata can reveal personal information about a particular user. Next, I will explore how the use of metadata has impacted individuals in the news. The third part of this Article will focus on how metadata can be used as a hands-on, practical exercise in the classroom. The fourth and final part of this Article will look at how metadata impacts both attorney-client privilege and the ethical duty of attorneys to maintain privileged information.

Understanding Metadata

"Metadata is literally 'data about data.'"[5] There is extensive scholarship and court opinions on finding metadata and the ethical implications of using this data in legal proceedings ranging from discovery[6] to public records[7] to privileged information to accidental disclosure. Metadata is embedded information about an electronic document that describes "how, when, and by whom an electronic document was created, modified, and transmitted."[8] Other data can also appear hidden in the electronic document, such as tracked changes and comments made during the editing process. In the legal field, metadata can potentially reveal sensitive information about a practitioner's clients or their case. For instance, a document can contain deleted comments or edits that may reveal an attorney's strategy and theories about their case that they would not want opposing counsel to access.

From an evidentiary standpoint, metadata can be helpful because it can either support or refute a claim of fabricated evidence by exposing a document's author and creation date. Where the scholarship falls short is understanding how individuals generate so much personal data, particularly metadata, and how that data can be used to re-create intimate and detailed portraits of our personal lives.

The smartphone market in the United States is one of the world's largest, with almost 310 million smartphone users as of 2023.[9] As individuals, practitioners, and consumers, we all consume and generate an immense

5. Ned T. Himmelrich, *Metadata: Data About Data*, Md. Bar J., May–June 2010, at 34, 36.

6. *See, e.g.*, Elizabeth W. King, *The Ethics of Mining for Metadata Outside of Formal Discovery*, 113 Penn St. L. Rev. 801, 803 (2009).

7. *See, e.g.*, Lake v. City of Phoenix, 218 P.3d 1004 (Ariz. 2009).

8. Carrie Davey, *Find It Fast: Leveraging Meta Data*, OrangePages (Applied Discovery, Bellevue, Wash.), Aug. 3, 2003, at 5.

9. *Number of Smartphone Users in the United States from 2013 to 2028 (in Millions)*, Statista (July 2023), https://www.statista.com/forecasts/1145056/smartphone-users-in-the-united-states.

amount of personal data through electronic interactions that create a personalized digital halo for each user.[10] According to the United Kingdom's Ofcom's Communications Market Report, "[t]he volume of data used on fixed and mobile connections both grew significantly in 2020. Average monthly data use per fixed broadband connection increased by 36% to 429 GB, while average use per mobile data user was up by 27% to 4.5 GB per month."[11] While much has been written about metadata and its implications for electronic documents, other sources of electronically stored information (ESI) also have metadata attached—notably, digital pictures. As noted in an article on ESI and family:

> [S]uch unauthorized entry potentially allows the opposing party to change the account owner's privacy and other settings, whether on a platform or on a smart device itself. For example, one could surreptitiously add the GPS feature to Facebook photo posts so when the account owner posts pictures or comments about restaurants, concerts or other activities, the site would include the owner's location. Having such access could result in an account owner to report his whereabouts to others without his knowledge.[12]

Cell phones are a large part of everyone's daily life, both for private individuals and for future and practicing attorneys. Understanding how cellphones collect and utilize our personal data is part of being a technology-competent practitioner.[13] I frequently use my own cell phone for technology examples in my Law Practice Technologies (LPT) class, as well as in my Electronic Discovery Technologies (EDT) classes. I took the rooster photo on my Apple iPhone 12 Pro Max at 5:46 p.m. on August 31, 2022. I can see the date, time, and general location by merely looking at the individual photo in my iPhone Photos application. However, the photo contains much more information.

If I swipe up, I can see much more of the metadata attached to the photo. My first choice of action is to "Look Up" the subject matter contained in my photo.[14] Introduced in iOS 15, Visual Look Up is an iOS visual search engine that lets a user identify and learn about objects found in

10. Strategy Analytics, *Average Monthly Wireless Data Usage Per User in the United States in Q1 and Q2 of 2018 (in GB), By Age*, Statista (2018), https://www.statista.com/statistics/919501/average-monthly-wireless-data-usage-in-the-us-by-age/ (showing the average monthly wireless data usage per user in the United States by age in the first two quarters of 2018; users twenty-five years and younger used 4.1 GB of cellular and 16.8 GB of Wi-Fi wireless data).

11. OfCom, Communications Market Report 2021, at 2 (2021).

12. J. Michael Taylor, *Discovery of Social Media in Family Court Litigation*, S.C. Law., Sept. 2019, at 34, 38.

13. *See Attorney Professionalism Forum*, N.Y. St. Bar Ass'n J., July–Aug. 2016, at 54, 54–55.

14. *See Look Up What's in a Photo with Your iPhone or iPad*, Apple Support (Mar. 14, 2022), https://support.apple.com/en-us/HT213088.

their Photos app.[15] It applies on-device machine learning to detect photos in Photos and other built-in apps like Safari, Messages, and Mail.[16] It can detect and inform the user about plants, pets, popular landmarks, books, statues, and art, among other subjects, in each photo. Using Look Up on my rooster picture is slightly disappointing. Look Up does identify the photo of the subject correctly as a chicken, but it does not identify the breed or provide any similar pictures of a white rooster.

Next, I see the specific timestamp of the photo, the make and model of the phone that took the photo, and which camera on the iPhone took the photo. All of this data is stored with each individual photograph in a format known as EXIF. EXIF stands for Exchangeable Image File Format. It is a standard for storing metadata in images taken by digital cameras, smartphones, or other devices that capture images. This metadata includes information about the camera settings, such as aperture, shutter speed, ISO, and focal length, as well as the date and time the photo was taken. EXIF data can also include details about the device itself, such as the make and model of the camera or smartphone, as well as software information. Additionally, it can contain geolocation information, providing the latitude and longitude coordinates where the photo was taken, if the device has GPS capabilities. This data is embedded within the image file itself and can be accessed and viewed using various software applications or photo editing tools. EXIF data can be quite useful, as it allows photographers to review and analyze the settings used for a particular photo. EXIF data also helps in organizing and categorizing images based on their metadata. EXIF data, the metadata associated with photographs, can keep track of the camera used to take an individual photo. Was it the telephone camera or the "selfie" camera located on the front of the phone? A sophisticated understanding of metadata can yield these answers. Finally, using the native software on my iPhone, I am presented with a zoomed-out map indicating where the photo was taken. By touching the map, I can see a detailed picture of the area surrounding the location where the picture was taken. By zooming into the map, I can see precisely where the picture was taken, including surrounding structures and roads adjacent to the location of the photograph. All of this visual information is pulled from the geolocation data attached to the original photograph.[17] The metadata of the original photograph will remain intact during transmission unless there is a knowledgeable practitioner present who knows how and when to remove it. If the photo is used in a filing, texted to a third party, or emailed, the metadata will remain intact.

---

15. *See Recognizing People in Photos Through Private On-Device Machine Learning*, Apple: Machine Learning Rsch. (July 2021), https://machinelearning.apple.com/research/recognizing-people-photos.

16. *See id.*

17. *See* Chris Hoffman & Nick Lewis, *How to See Exactly Where a Photo Was Taken (and Keep Your Location Private)*, How-To Geek (Aug. 29, 2023), https://www.howtogeek.com/211427/how-to-see-exactly-where-a-photo-was-taken-and-keep-your-location-private/.

My next step is to determine the owner of the property captured in the photo. So far, I have successfully determined the exact time and location the photo was taken. Thanks to the geolocation data attached to the photo, I have acquired a good understanding of the neighboring streets and the potential whereabouts of the house. Utilizing the information solely derived from the photo, I can enter the general street name and county into Google Maps. Through a process of trial and error, I can recreate the map displayed on my iPhone by incorporating the geolocation photo data with Google Maps. By utilizing the Street View feature within Google Maps, I can explore the surrounding area in a 365-degree view, including detailed visuals of neighboring houses along with their corresponding house numbers. It only takes a few clicks to determine the house number of the house where the rooster photo was taken. I then query my students regarding their understanding of real estate records. My students can usually direct me to the county tax records website, which is free and easily accessible online. Now that we have the complete address of the house, finding out who owns the property is straightforward.

We then take the exercise a few steps further. Now that I have the homeowner's full name, we can run a Google Images search using the new information. Since I am listed on the North Carolina School of Law's website, it is not a difficult task to find a picture of me as well as my office location, email, and phone number.[18] I remind my students that I found all this information based on a single picture of a chicken. I did not have to install any additional software to uncover this information. I did not have to enable any special settings on my phone to attach this information. I also did not utilize any expensive databases, such as Westlaw or Lexis. The iPhone automatically attaches location and other metadata to photos so that the photos can be organized in a variety of ways such as by location, time, or individuals within the photos. I make a point of using my cell phone with the default options enabled.

It would take additional technology competency to disable these features or strip the photos of their attached metadata, but the metadata can be altered or removed. An app like EXIF Viewer allows a user to see all the metadata associated with a digital photograph.[19] While the native Apple Photo app displayed the geolocation and timestamp, I was not able to determine the altitude where the photo was taken. Using an app like EXIF Viewer, I can view the altitude where the picture was taken. I can also remove the geotag data from the photo or other individual pieces of metadata. These are other important points for practitioners to understand: where the metadata

18. *See Stacey L. Rowland*, Univ. N.C. Sch. L., https://law.unc.edu/people/stacey-l-rowland/ (last visited Jan. 11, 2024).

19. *See App Store Preview: EXIF Viewer by Fluntro*, Apple, https://apps.apple.com/us/app/exif-viewer-by-fluntro/id944118456 (last visited Jan. 11, 2024).

is stored, how it can be viewed, whether it is privileged information, and/or whether it is discoverable.[20]

FIGURE 2. MORE (INFORMATION) THAN MEETS THE EYE.
This is a Screenshot of the metadata revealed by the EXIF Viewer app.

20. *See* Mark Johnson Roberts, *Electronic Competence*, OR. ST. BAR BULL., June 2017, at 9, 11.

As more and more of our personal and professional lives take place online, competent practitioners need to understand the risks and benefits of technology. I hope to drive this point home with my students by illustrating the basic anatomy of "doxing"[21] an individual, in this case, myself, using the chicken picture. Using a single picture and the metadata attached to that picture, I am able to find the names and addresses, both personal and professional, of the individuals who live at the geolocation unmasked by the metadata.

Metadata in the News

Metadata can be used as a tool to facilitate both "swatting"[22] and doxing attacks.[23] Swatting attacks happen when individuals call in false law enforcement threats like bomb threats or hostage situations.[24] Law enforcement takes these threats seriously and responds with force.[25] In 2021, Mark Herring died after being swatted. The alleged swatter attacked Herring when Herring refused to hand over a coveted Twitter handle.[26] The paragraph that stands out in the article detailing Herring's ordeal: "They'd have food delivered at the person's house or report fires at their homes, according to court documents."[27] How did the swatters obtain Herring's address? "On April 27, 2020, Mr. Sonderman posted the names and addresses of Mr. Herring and his family members on Discord, a texting and talking app."[28] "A swatter can get a victim's address through methods ranging from a simple Google search to more complex Internet Protocol (IP) address tracking and hacking."[29] Knowing how to look for and use metadata can facilitate the information needed to direct authorities to a potential victim's whereabouts

---

21. *See* Victoria McIntyre, *"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent*, 19 Tulane J. Tech. & Intell. Prop. 111, 113 (2016).

> Doxing is a form of harassment that normally occurs when an individual obtains (through deep Internet searching or hacking, generally) private information about a person such as their phone number, home address, or social security number, and posts this information online without permission. The goal of doxing is to scare or intimidate a victim by posting the victim's confidential information online so that he or she becomes fearful about where the information may be posted next.

Id.

22. *See* Jacob Hoeferkamp, *Combatting the Swatting Problem: The Need for a New Criminal Statute to Address a Growing Threat*, 2019 Mich. St. L. Rev. 1133, 1137 (2019) ("Swatting is a term commonly used to describe hoax emergency reports in which the first responders are typically members of Special Weapons And Tactics (SWAT) teams.").

23. *See* McIntyre, *supra* note 21.

24. *See* Jason Fagone, *The Serial Swatter*, N.Y. Times Mag. (Nov. 24, 2015), https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html.

25. *See id.*

26. *See* Maria Cramer, *A Grandfather Died in 'Swatting' over His Twitter Handle, Officials Say*, N.Y. Times (July 24, 2021), https://www.nytimes.com/2021/07/24/us/mark-herring-swatting-tennessee.html.

27. *Id.*

28. *Id.*

29. Hoeferkamp, *supra* note 22, at 1137–38.

for the purposes of swatting. Just like I obtained my home address from the lone chicken photograph, nefarious parties can accomplish similar tasks with information their victims posted online.

After John McAfee's capture,[30] platforms like Facebook and Twitter began automatically removing location data from pictures their users posted.[31] Metadata, specifically photo location data, ultimately led to the capture of John McAfee in 2012.[32] Paul Manafort is notorious in legal technology circles for his many technology snafus which involved the lack of understanding metadata.[33] Other platforms, such as the now-defunct social media site, Parler, left the metadata of all uploaded materials intact.[34] "GPS coordinates taken from 618 Parler videos analyzed by Gizmodo has [sic] already been sought after by [the] FBI as part of a sweeping, nationwide search for potential suspects, at least 20 of whom are already in custody."[35] Ranging from understanding, obtaining, and preserving digital evidence to competently representing their clients, law schools need to embrace the teaching of technology so that future practitioners have a real path to future opportunities and employment.

Understanding metadata is fundamental to meeting the duty of technology competency for aspiring lawyers and current practitioners. In 2012, the American Bar Association modified its Model Rules to require lawyers to "stay abreast of changes in the law and its practice, including the benefits and the risks associated with relevant technology."[36] As of 2023, forty states

30. John McAfee was a British-American entrepreneur and cybersecurity pioneer. He founded the software company McAfee Associates in 1987, which became one of the leading antivirus software companies in the world. However, he resigned from the company in 1994. Following his departure from McAfee Associates, McAfee pursued various entrepreneurial ventures and investments, including in the field of cryptocurrency. He was a vocal advocate for privacy and cybersecurity. In 2012, McAfee faced legal issues related to the death of his neighbor in Belize, where he was residing at the time. He was named a person of interest in the investigation. While still claiming to the press to be in Belize, McAfee crossed the international border into Guatemala. In Guatemala, McAfee was arrested by the Guatemalan authorities on December 5, 2012. In a twist of irony, a photo posted by Vice with the intact EXIF data led authorities to McAfee's location, where he was taken into custody. *See* Eyder Peralta, *Betrayed by Metadata: John McAfee Admits He's Really in Guatemala*, Nat'l Pub. Radio (Dec. 4, 2012, 12:24 PM ET), https://www.npr.org/sections/thetwo-way/2012/12/04/166487197/betrayed-by-metadata-john-mcafee-admits-hes-really-in-guatemala; Jeff Wise, *In Pursuit of John McAfee, Media Are Part of Story*, N.Y. Times (Dec. 9, 2012), https://www.nytimes.com/2012/12/10/business/media/in-pursuit-of-john-mcafee-media-are-part-of-story.html.

31. *See* Igor Kuksov, *Do Your Online Photos Respect Your Privacy?*, Kaspersky: Kaspersky Daily (Oct. 31, 2016), https://usa.kaspersky.com/blog/exif-privacy/7957/.

32. *See* Wise, *supra* note 30.

33. *See* Herbert B. Dixon Jr., *Embarrassing Redaction Failures*, Judges' J., Spring 2019, at 37, 37–38.

34. *See* Dell Cameron & Dhruv Mehrotra, *Parler Users Breached Deep Inside U.S. Capitol Building, GPS Data Shows*, Gizmodo (Jan. 12, 2021), https://gizmodo.com/parler-users-breached-deep-inside-u-s-capitol-building-1846042905.

35. *Id.*

36. Model Rules of Pro. Conduct r. 1.1 cmt. 8 (Am. Bar Ass'n 2020).

have adopted some form of the duty of technology competency.[37] The duty of competence includes both substantive knowledge of law and competent use of the technology that lawyers use to practice law:[38] "Lawyers can't be Luddites."[39] While the Model Rules do not require lawyers to be technology experts in all areas of potential law practice, all lawyers are required to have at least a basic understanding of the technologies they and their clients use.[40] In my LPT and EDT classes, I emphasize the benefits and risks of metadata that is generated daily on our cell phones and electronic devices.

Hands-on Exercises with Metadata in the Classroom

After we discuss how metadata is generated, where it is stored, and how it can be altered, I give my students an in-class assignment to assess their understanding of metadata. I live in North Carolina and frequently enjoy the abundant hiking options available in the state and surrounding areas. When I hike, my husband and I take multiple pictures throughout the day. These pictures are the basis of my in-class exercise.[41] For this in-class assignment, I write up a fact pattern that puts my whereabouts in question.[42] I draft a fact pattern where I am suspected of armed robbery on a given day and at a given time. I am seeking the legal advice of my students before talking to law enforcement.

The goal of this assignment is to illustrate to my students how much digital information is being collected on any individual at a given time. To set up this assignment, I place the digital photos from the hiking trip into a Google Photos folder. Google sets the default option for shared folders to hide the location data. For this exercise, I enable the "Share photo location" option. Each picture contains specific and individual metadata. When the entire collection of pictures is viewed together, a narrative of the events can be corroborated using the metadata as well as the subject matter of the pictures. For example, based on the metadata, the first picture was taken on Friday, December 31, 2021, at 11:45 a.m. The geolocation data of the picture catalogs the picture as being taken in Hanging Rock State Park,

37. Robert J. Ambrogi, *Tech Competence*, LawSites, https://www.lawnext.com/tech-competence (last visited Jan. 11, 2023).

38. *See* Patricia A. Sallen, *Technology Competence: New Wine in an Old Ethical Bottle*, Law Prac., Mar.–Apr. 2016, at 35, 36.

39. Debra Cassens Weiss, *Lawyers Have Duty to Stay Current on Technology's Risks and Benefits, New Model Ethics Comment Says*, A.B.A. J. (Aug. 6, 2012, 7:46 PM CDT), https://www.abajournal.com/news/article/lawyers_have_duty_to_stay_current_on_technologys_risks_and_benefits.

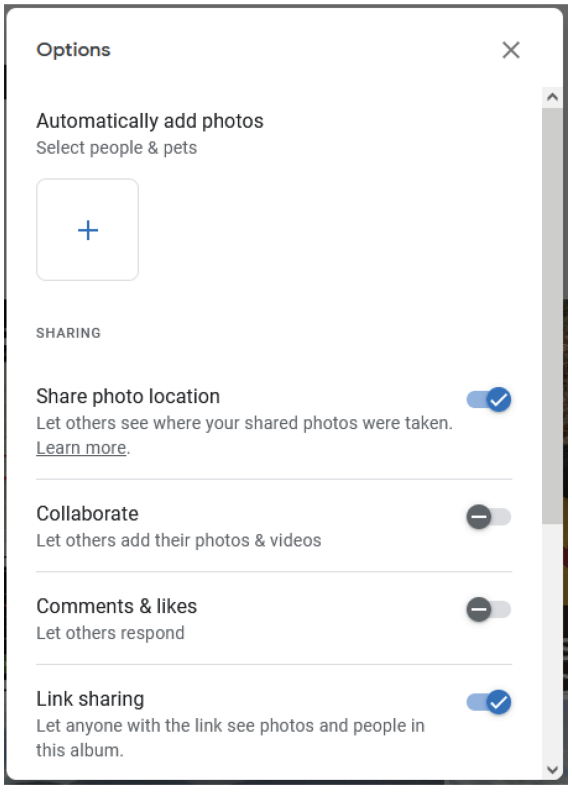
40. *See* Heidi Frostestad Kuehl, *Technologically Competent: Ethical Practice for 21st Century Lawyering*, 10 Case W. Rsrv. J. L. Tech. & Internet 1, 7 (2019).

41. *See Metadata Fact Pattern*, Google Photos, https://photos.app.goo.gl/aC59Jdw9XtRbDrrw9. I supply this link to my students so they can examine the EXIF metadata contained in the pictures. I also supplied a sample of the in-class assignment used for this material within the Google Photo Album listed above.

42. A sample fact pattern is included in the Google Photo album. *See id.*

at the Visitor Center in Walnut Cove, North Carolina. Initially, I want my students to establish a timeline for the album and when the pictures took place. The last picture in the album was taken at 5:30 p.m. Eastern Standard Time. Then, we can examine the individual pictures. Each individual picture carries its own unique fingerprint of metadata. Viewing the pictures, we can visually see there are two individuals on this hiking trip. By viewing the metadata, my students can see that at least two separate cell phones created the photos in the collection, an Apple iPhone 12 Pro Max and an Apple iPhone 12. The metadata shows the Apple iPhone 12 Pro Max has location data enabled, while the Apple iPhone 12 did not have any attached geolocation data.

FIGURE 3. GOOGLE PHOTOS UPLOAD PROMPTS.
Google implemented some privacy safeguards when sharing pictures through Google Photos. This is an example of the privacy settings I used for this assignment.



The pictures also contain hints to other sources of metadata. In addition to the pictures taken by the cell phones, I also include screenshots of other apps that were used during the hike. While the screenshots would

likely face a high bar to admissibility in a legal proceeding due to hearsay, the data they represent could be a better way to prove the whereabouts of an individual and could offer a better authentication trail. There are three other apps representing discrete data trails and utilizing the location data of the cell phone. The first app is AllTrails.[43] This app allows hikers to download maps of trails, and, if the user has a subscription, offers real-time trail location and off-route notifications.[44] I utilized this app on the hiking trip for safety concerns. The blue dots in the screenshots represent our locations throughout the hike. The second app is the native iPhone Weather app.[45] Like AllTrails, this app is also using my location to give me weather updates while we are out hiking.[46] The third app is Fitbit.[47] Fitbit is also using my location to keep track of where and how far we hiked, in addition to biometric data like heart rate and calorie burn.[48] Each of these apps is sending independent data back to their respective servers.

Fitbit data has been found to be admissible and self-authenticating in court. In *State v. Burch*, two of the three holdings applied to electronic evidence involving Fitbit.[49] First, the circuit court acted within its discretion in determining that expert testimony was not needed to support evidence from an electronic pedometer of the victim's boyfriend.[50] Second, the circuit court acted within its discretion in determining that records from the electronic pedometer were sufficiently authenticated:[51]

> The circuit court's authentication obligation is simply to determine whether a fact-finder could reasonably conclude evidence is what its proponent claims it to be [as authorized by] Wis. Stat. § 909.01. The circuit court did so here by reviewing the Fitbit records and the affidavit of "a duly authorized custodian of Fitbit's records" averring that the records "are true and correct copies of Fitbit's customer data records," and then concluding the data was self-authenticating under Wis. Stat. § 909.02(12).[52]

The key point I want my students to take away from this exercise is how many apps track a user's location and how various apps, depending on their privacy and use settings, can be used to corroborate an individual's

43. *See Download the App*, ALLTRAILS, https://www.alltrails.com/mobile (last visited Jan. 11, 2024).
44. *See id.*
45. *See App Store Preview: Weather*, APPLE, https://apps.apple.com/us/app/weather/id1069513131 (last visited Jan. 11, 2024).
46. *See id.*
47. *See* FITBIT, https://www.fitbit.com/global/us/home (last visited Jan. 11, 2024).
48. *See id.*
49. *See* State v. Burch, 961 N.W.2d 314 (Wis. 2021), *cert. denied*, 142 S. Ct. 811 (2022).
50. *See id.* at 322–23.
51. *See id.* at 323–24.
52. *Id.* at 323.

whereabouts on a particular day. This information is vital to practitioners as it could impact how a client is represented and how competently a practitioner can navigate digital discovery.

The Weather app is using my location data so it can accurately reflect the current weather conditions. While Fitbit and AllTrails can use GPS data when cellular data is not available, the Weather app must use cellular telephone data or a Wi-Fi connection.[53] My cell phone was able to ping a cell phone tower in the area. Hanging Rock State Park is in a rural and remote area of the state. My cell phone would not have many options to reach a tower. If needed, a warrant could be obtained and likely narrowed to the few cell phone towers that exist in the area. This is potential evidence that could be obtained and authenticated, if needed, in a court proceeding. But it would require a competent practitioner who knew where and how to obtain this electronic information. Technology competency and understanding metadata in the modern-day practice of law could provide an alibi or incriminate an individual. It is critical that new practitioners understand how these technologies influence our everyday lives and that law schools provide this foundational guidance.

Metadata and Its Impact on Attorney-Client Confidentiality and Maintaining Privilege

Once my students understand how metadata is generated, where it is stored, and how it can be removed, I discuss examples of ethical rules that involve metadata. The first example is attorney-client privilege and the ethics of metadata use. Attorney-client confidentiality is governed by two main sets of rules: attorney-client privilege and the ethical duty to maintain confidentiality.[54] Inadvertent disclosure of confidential information to third parties may result in waiver of attorney-client privilege and may constitute a violation of the ethical rules if reasonable precautions are not taken to prevent inadvertent disclosures.[55] Inadvertent disclosure of metadata poses additional issues for attorneys because metadata itself can contain confidential information that may appear hidden but is still accessible by third parties.[56]

---

53. *See* Matt Klein, *How to Make the iPhone Weather App Update on a Mobile Connection*, How-To Geek (Mar. 3, 2016), https://www.howtogeek.com/243368/how-to-make-the-iphone-weather-app-update-on-a-mobile-connection/.

54. *See* Am. Bar Ass'n Cybersecurity Legal Task Force, Report to the House of Delegates and Resolution 118, at 5 (2013) (report from the Cybersecurity Legal Task Force explaining the adoption of the resolution).

55. *See id.* at 12–13.

56. *See* Mark L. Tuft, Ellen R. Peck, Kevin E. Mohr, Paul W. Vapnek & Howard B. Weiner, California Practice Guide: Professional Responsibility & Liability § 7:156.6 (2022).

"The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law."[57] The purpose behind the privilege is to "encourage full and frank communication" between a client and their attorney so that an attorney has all the information needed to be able to adequately represent their client.[58] North Carolina's courts have established five elements that must be met for communications to be privileged:

> A privilege exists if (1) the relation of attorney and client existed at the time the communication was made, (2) the communication was made in confidence, (3) the communication relates to a matter about which the attorney is being professionally consulted, (4) the communication was made in the course of giving or seeking legal advice for a proper purpose although litigation need not be contemplated and (5) the client has not waived the privilege.[59]

The effect of this privilege is that a court may not force an attorney or a client to disclose privileged communications, either to private parties or the government.[60] Furthermore, the privilege belongs to the client, and only a client can waive it, although an attorney may assert the privilege on behalf of their client.[61]

The bedrock of this privilege is confidentiality. If attorney-client communications lose their confidential nature, they are no longer privileged, and a client is said to have "waived" the privilege.[62] Waiver can be voluntary or involuntary.[63] In some cases, inadvertent disclosure to third parties can destroy the privilege, including the inadvertent disclosure of metadata.[64] The reasoning behind this is that if a client is not concerned about keeping their communications confidential, they do not need this protection to be fully honest with their attorney, and the opposing side's interest in gathering all available evidence will prevail.[65]

Attorney-client privilege dictates what a lawyer *need not* disclose, while the ethical duty to maintain client confidentiality dictates what a lawyer *must not* disclose.[66] This ethical duty is governed under Rule 1.6 of North Carolina's Rules of Professional Conduct.[67]

---

57. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).
58. *Id.*
59. State v. Murvin, 284 S.E.2d 289, 294 (N.C. 1981).
60. *See* State v. Ballard, 428 S.E.2d 178, 182–83 (N.C. 1993).
61. *See In re* Miller, 584 S.E.2d 772, 788 (N.C. 2003).
62. *See Murvin*, 284 S.E.2d at 294.
63. *See* Scott v. Glickman, 199 F.R.D. 174, 177 (E.D.N.C. 2001).
64. *See* Hur v. Lloyd & Williams, LLC, 523 P.3d 861, 864–866 (Wash. Ct. App. 2023).
65. *See* Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485, 513 (2018).
66. *See* JOHN M. BURKOFF, CRIMINAL DEFENSE ETHICS: LAW AND LIABILITY § 5:8 (2d ed. 2023).
67. *See* N.C. RULES OF PRO. CONDUCT r. 1.6 (N.C. STATE BAR 2022).

Under Rule 1.6, a lawyer shall not reveal any information relating to the representation of the client unless the client gives informed consent, the disclosure is implicitly authorized, or the disclosure is permitted under the crime-fraud exception or other related exceptions.[68] Furthermore, a lawyer must make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client, including metadata.[69]

Metadata touches on many substantive areas of the law. For example, the third-party doctrine is usually analyzed in the criminal context as it relates to the Fourth Amendment.[70] The Fourth Amendment protects individuals from unreasonable searches and seizures by the government.[71] Warrantless searches and seizures are presumptively unreasonable.[72] For purposes of determining whether a search or seizure has occurred, the court will ask whether the government intrudes on an individual's "reasonable expectation of privacy."[73] In other words, the government is required to get a warrant before accessing information to which individuals have a reasonable expectation of privacy.

However, the third-party doctrine states that individuals have "no legitimate expectation of privacy in information [they] voluntarily turn[ed] over to third parties."[74] The Supreme Court has struggled over how to apply this test in a principled way given the modern-day reality that virtually all information is, by necessity, shared with third parties. Companies collect this information and freely sell it to private—and public—parties, including the government, effectively allowing the government to bypass Fourth Amendment warrant requirements.[75] An understanding of metadata is needed for both criminal and civil matters.

The rules relating to lawyer-client confidentiality also contain a version of the third-party doctrine, and it relates to metadata. Unlike Fourth Amendment jurisprudence, the rules relating to confidentiality recognize communications shared with a third party do not always lose their confidentiality.

Communications between attorney and client generally are not privileged when made in the presence of a third person who is not an agent of

68. *Id.* r. 1.6(a).
69. *Id.* r. 1.6(c).
70. *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (offering a defense of the Fourth Amendment's third-party doctrine); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (examining the privacy implications of the third-party doctrine in the Fourth Amendment context).
71. Katz v. United States, 389 U.S. 347, 353 (1967).
72. *See* Kentucky v. King, 563 U.S. 452, 459 (2011).
73. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).
74. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
75. *See* Diamantis, *supra* note 65, at 497–99.

either party.[76] However, the laws governing privilege recognize that attorneys must work with third parties such as translators, paralegals, and IT support to provide legal services.[77] Communications with these parties would not destroy confidentiality. Since many of these communications could happen electronically, the third-party doctrine will likely extend to the metadata associated with the digital documents. Furthermore, even inadvertent disclosure to unintended third parties will not necessarily destroy the privilege: "[t]he cornerstone of the privilege-waiver analysis is the intent of [the] parties and the reasonableness of their precaution[s] to preserve confidentiality."[78]

When analyzing whether inadvertent disclosure will destroy confidentiality, courts will consider: "(1) the reasonableness of the precautions taken to prevent inadvertent disclosure; (2) the time taken to rectify the error; (3) the scope of the discovery; (4) the extent of the disclosure; and, (5) the overriding issue of fairness."[79]

In the context of whether the use of third-party technology service providers will waive privilege, courts will similarly rely on a reasonableness standard. For example, in *In re Asia Global Crossing, Ltd.*,[80] the court considered whether a client had a reasonable expectation of privacy in an email sent to their lawyer from their personal email address over their employer's server.[81] The court analogized the online activity to keeping personal files in a work office, to which an individual may or may not have a reasonable expectation of privacy depending on office policies.[82] Considerations such as if the office is locked and where the files are kept would need to be thought about.[83] The court concluded that it needed more information about the employer's retention policies and facts surrounding the case to ultimately resolve the issue, but it held that "the transmission of a privileged communication through unencrypted e-mail does not, without more, destroy [attorney-client] privilege."[84]

The court also laid out a four-factor test to determine whether an employee has a reasonable expectation of privacy in an email sent over a company server: (1) Does the corporation maintain a policy banning personal or other objectionable use? (2) Does the company monitor the use of the employee's computer or e-mail? (3) Do third parties have a right of

76. State v. Murvin, 284 S.E.2d 289, 293 (N.C. 1981).
77. *See* Diamantis, *supra* note 65, at 516.
78. Diamantis, *supra* note 65, at 516–17.
79. Scott v. Glickman, 199 F.R.D. 174, 178 (E.D.N.C. 2001).
80. 322 B.R. 247 (Bankr. S.D.N.Y. 2005).
81. *See id.* at 256–57.
82. *Id.* at 257.
83. *See id.* at 257–58.
84. *Id.* at 256.

access to the computer or e-mails? And (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[85]

Other courts have adopted this test. For example, in *In re Reserve Fund Securities and Derivative Litigation*,[86] the court concluded that emails sent between the president of a company and his wife, over the company's email server, were not protected by marital privilege.[87] The court explained that the president did not have a reasonable expectation of privacy in the emails because the company banned personal use of its email system, the company explicitly reserved the right to access employee email, the company warned employees that emails sent over its system may be subject to disclosure by regulators, and the president was aware of these policies.[88]

In contrast, in *Convertino v. U.S. Department of Justice*,[89] the court held that a former employee at the Department of Justice (DOJ) had a reasonable expectation of privacy in personal emails sent from his DOJ email address to his lawyer.[90] The DOJ did not have a policy that banned the personal use of company emails.[91] Furthermore, although the DOJ did have access to emails sent from the employee's account, the employee was not aware that the DOJ would be regularly accessing and saving emails sent from his account.[92] In summary, when deciding whether a client has waived attorney-client privilege, the court's inquiry is very fact-specific. It considers both objective reasonableness standards and the subjective understanding of the person claiming the privilege.

Similar to case law governing waiver of attorney-client privilege, the ethical rules specifically recognize that accidental disclosure to a third party will not automatically constitute a violation of an attorney's ethical duty to their client. Comment 19 to Rule 1.6 states that the inadvertent disclosure of client information will not constitute a Rule violation as long as the lawyer has made reasonable efforts to prevent the disclosure.[93] The Comment states several non-exclusive factors that go to reasonableness: "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g.,

85. *Id.* at 257.
86. 275 F.R.D. 154 (S.D.N.Y. 2011).
87. *See id.* at 156, 164. Whether communications are protected by marital privilege is a similar inquiry to attorney-client privilege; it asks whether the communication was made in confidence, or whether the spouse had a reasonable expectation of privacy in the communication. *See id.* at 157.
88. *Id.* at 164.
89. 674 F. Supp. 2d 97 (D.D.C. 2009).
90. *See id.* at 110.
91. *Id.*
92. *Id.*
93. N.C. Rules of Pro. Conduct r. 1.6 cmt. 19 (N.C. State Bar 2022).

by making a device or important piece of software excessively difficult to use)."[94]

In order to provide additional protection for lawyers who unintentionally send writings to opposing parties, ethical rules have been established. According to these rules, if a lawyer receives a writing that they reasonably believe was inadvertently sent to them and it pertains to a client's representation, they are required to notify the sending attorney.[95] This rule extends to the inadvertent disclosure of metadata.[96] Recognizing the growing importance of metadata in relation to client confidentiality, the North Carolina State Bar issued an opinion in 2010. This opinion stated that lawyers must "use reasonable care to prevent the disclosure of confidential client information hidden in metadata."[97] Furthermore, a lawyer who receives an electronic communication "must refrain from searching for and using confidential information found in the metadata" of that communication.[98]

If a lawyer accidentally views confidential information embedded in the metadata of a document that was sent to them, the receiving lawyer "must notify the sender and may not subsequently use the information revealed."[99] Other states have taken the position that an attorney has the right to use metadata without informing opposing counsel to greater incentivize the sending attorney to take reasonable care to scrub their documents of sensitive data.[100]

To maintain client confidentiality when it comes to metadata, an attorney must first be aware of metadata and what it can potentially reveal. They should be familiar with the application they are working with, what type of metadata it stores, and how that data is stored and accessible. Knowing how to scrub a document and delete metadata that contains sensitive information is essential. However, sometimes a practitioner may want to keep some metadata depending on the circumstances, such as the date the document was created and internal links, or if the metadata is needed for the purposes of discovery. All of these reasons illustrate the need for competency when dealing with metadata.

Furthermore, attorneys should be familiar with their state bar's ethics rules on the issue, especially when it comes to the issue of inadvertent

---

94. *Id.*

95. *See id.* r. 4.4(b).

96. *See id.* r. 4.4 cmt. 3.

97. N.C. State Bar, Formal Ethics Op. 1 (2009), https://www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2009-formal-ethics-opinion-1 (reviewing and discussing the use of metadata).

98. *Id.*

99. *Id.*

100. *See* Joseph Mcginley, *Properly Addressing the Use of Metadata in the Legal Profession*, MEDIUM (Oct. 4, 2018), https://medium.com/@mcginley2019/properly-addressing-the-use-of-metadata-in-the-legal-profession-611fcad9d1b1. For example, in Oregon, if an attorney sends metadata that the receiving attorney knows or reasonably should know was inadvertently disclosed, the receiving attorney must notify the sender, but the receiving attorney is not required to abstain from reading the metadata. Or. State Bar, Formal Ethics Op. No. 2011-187, at 4 (2015).

disclosures. Practitioners should know whether and when they must notify opposing counsel in case of inadvertent disclosure. Attorneys should read their jurisdiction's case law on what constitutes "reasonable steps" to prevent inadvertent disclosures, to abide by ethics rules, and to avoid involuntary waiver which could destroy attorney-client privilege. Finally, they should be aware that the use of third-party technology service providers can destroy privilege in some circumstances where the confidentiality of communications is not properly maintained.

Takeaways for Understanding Metadata

The theme of the *University of St. Thomas Law Journal*'s 2022 Fall Symposium sought to provide a road map for teaching technology-competent lawyers and a framework for law schools to embrace and support this curriculum. I believe this roadmap includes a thorough understanding of metadata. Metadata is a consistent theme that runs through the entirety of my LPT and EDT courses. Metadata is central to understanding digital privacy, digital tracking, and maintaining attorney-client confidentiality. Understanding metadata and its implications is crucial for attorneys when it comes to maintaining client confidentiality and abiding by ethical rules. The attorney-client privilege and the ethical duty to maintain confidentiality play a significant role in protecting confidential communications. Inadvertent disclosure of metadata can pose additional challenges as it may contain hidden but accessible confidential information. Courts consider various factors, such as the reasonableness of precautions taken and the intent of the parties, when determining whether inadvertent disclosure destroys confidentiality. Additionally, attorneys must be aware of their jurisdiction's ethics rules and case law on the issue to ensure they take reasonable steps to prevent inadvertent disclosures. Furthermore, the use of third-party technology service providers can potentially jeopardize privilege if proper confidentiality measures are not in place. Overall, competency and familiarity with metadata and ethics rules are essential for attorneys to effectively protect client confidentiality. Understanding what metadata is, where it is located, and how it can be removed or preserved is crucial for a technology-competent practitioner.