SMU | Dedman School of Law

SMU Law Review

Volume 76 | Issue 4 Article 7

2023

Data Milkshakes: The Rule of Capture and the Constitutionality of Data Mining

Bryce Pilawski
Southern Methodist University, Dedman School of Law

Data Milkshakes: The Rule of Capture and the Constitutionality of Data Mining

*Bryce D. Pilawski**

ABSTRACT

This Comment examines, explains, and attempts to reconcile the federal judiciary's implicit reasoning behind the lax protection of metadata in years past, specifically through the lens of the Rule of Capture. With the goal of explaining the historical hesitance courts have shown when protecting metadata, this Comment illustrates why this hesitance is actually motivated by reasoned restraint rather than a mere refusal to protect. In fact, through the lens of the Rule of Capture, metadata tracks the characteristics of resources that have traditionally counseled for the Rule's application, specifically that the resource is: (1) emerging in value and (2) difficult to define in terms of location at any given moment or "fugacious" in nature.

It is no coincidence that, until recently, technological developers enjoyed a free-for-all in the sense that they could collect, store, and even market as much personal information from their users as their technology could absorb. However, this informational buffet will not last forever. As addressed in the latter portion of this Comment, courts have already begun—and as predicted here, will continue with increasing scrutiny—recognizing these unregulated captures as potential violations of individual privacy. In the near future, this Comment suggests that the Supreme Court will definitively establish and protect individual privacy rights for the information falling outside the definition of traditional data, especially because, given rapid advancements in handheld technology, metadata is often more intimate and revealing.

TABLE OF CONTENTS

https://doi.org/10.25172/smulr.76.4.7

* J.D. Candidate, SMU Dedman School of Law, 2024; B.A. Philosophy, Texas Tech University, 2021. I would like to thank Professors Dale Carpenter and James Coleman for their influence in writing this Comment. I would also like to thank my family and friends, as well as Tehya and Mishka, for their support.

I. INTRODUCTION

"HERE, if you have a milkshake, and I have a milkshake, and I have a straw. There it is, that's the straw, you see? Watch it. Now, my straw reaches across the room and starts to drink your milkshake. I drink your milkshake!"[1] This quote comes from Daniel Day-Lewis's character in the 2007 film There Will be Blood: a power-hungry oilman explaining to a helpless landowner how he was able to extract and market the minerals underlying the landowner's property without permission and without legal consequence.[2] This extraction method would become known in the oil and gas industry as "drainage,"[3] which, despite sounding like a theft, was completely legal for nearly a century under a concept known as the Rule of Capture, which, to a degree, remains in effect today in some states.[4] The above-quoted movie artfully portrays the conflicts in the early twentieth-century United States between individuals who recognized the increasing value in a relatively new—or at least newly useful—resource. This Comment explains how these same conflicts have famously emerged in the context of other resources with similar characteristics like, for example, wild animals and water. As these resources became commonly recognized as more personal and more valuable, the law began to bolster and recognize respective protections. Drawing on this, this Comment suggests that in terms of privacy law, the lax treatment of large-scale data collection and the minimal protection of individual metadata can be explained by the Rule of Capture. Thus, as we have seen over the last two decades,[5] a shift in the understanding of how data relates to the individual is likely to trigger increased awareness, eventually resulting in the abandonment of the Rule of Capture altogether for a better tailored mechanism of legal protection relative to our modern understanding of the resource.

---

1. There Will Be Blood (Ghoulardi Film Company 2007).
2. *Id.*
3. *See Drainage*, Schlumberger Energy Glossary, https://glossary.slb.com/en/terms/d/drainage [https://perma.cc/WEA8-GVKS].
4. *See, e.g.*, Coastal Oil & Gas Corp. v. Garza Energy Tr., 268 S.W.3d 1, 13 (Tex. 2008) (finding that the Rule of Capture "gives a mineral rights owner title to the oil and gas produced from a lawful well bottomed on the property, even if the oil and gas flowed to the well from beneath another owner's tract"); Kelly v. Ohio Oil Co., 49 N.E. 399, 401 (Ohio 1897).
5. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056 (2004).

By suggesting that "data" will become "more personal," this Comment focuses on metadata. The National Information Standards Organization defines metadata as "the information we create, store, and share to describe things,"[6] however, commentators have referred to it more simply as "data about data."[7] This distinction is important because traditional data (for example, an individual's social security number, voting history, or even a country's nuclear codes) have been established as significantly personal for quite some time,[8] thus receiving attention and eventual protection from the courts. On the other hand, metadata, or "data about data," (for example, how many times in a day an individual opened the Twitter app on their iPhone) has historically received little to no legal protection since, until recently, it was understood to be virtually useless and without any practical value.[9] Now, thanks to technological advancements not unlike those that catalyzed the oil industry to eventually produce a resource so valuable that countries would fight to protect it,[10] the value of metadata in terms of marketing, law enforcement, and privacy is beginning to receive public appreciation.[11] Before this recognition, metadata had been liberally captured, monetized, utilized, and stored without legal protection, similar to how oil and water were treated before their modern value was realized and they became understood as more personal forms of property.[12] The same conflicts, such as that between the oilman and the landowner described above, have emerged with increased frequency in the courts over the last several decades, forcing the judiciary to reevaluate the relationship between individuals and their metadata, and what type of protection that relationship requires.

Two key similarities between metadata and similarly governed resources support the explanation for why courts have, although perhaps not expressly, implicitly applied the same reasoning underlying the Rule of Capture to the jurisprudence governing metadata. First, in terms of utility, the resource is relatively new.[13] Until recently, marketing firms and governments had little use for a bank of information about other information.[14] However,

---

6. Jenn Riley, Nat'l Info. Standards Org., Understanding Metadata: What is Metadata, and What is it For? 1 (2017), https://www.niso.org/publications/understanding-metadata-2017 [https://perma.cc/CW2D-KCNA].

7. *See, e.g.*, Hans P. Sinha, *The Ethics of Metadata: A Critical Analysis and a Practical Solution*, 63 Me. L. Rev. 175, 176 (2010); *id.* at 176 n.1 (collecting sources).

8. *See* Robin Andruss, *A Brief History of Data Privacy, and What Lies Ahead*, Skyflow (June 27, 2022), https://www.skyflow.com/post/a-brief-history-of-data-privacy-and-what-lies-ahead [https://perma.cc/JU2M-T2XW].

9. *See id.*

10. *See* Luis E. Cuervo, *OPEC from Myth to Reality*, 30 Hous. J. Int'l L. 433, 492–98 (2008).

11. *See* Kurt Cagle, *The Value of Metadata*, Forbes (Feb. 26, 2019, 4:39 PM), https://www.forbes.com/sites/cognitiveworld/2019/02/26/the-value-of-metadata [https://perma.cc/VJ9V-PFXY].

12. *See Everything You Need To Know About the Rule of Capture*, Courthouse Direct (June 11, 2019), https://info.courthousedirect.com/blog/everything-you-need-to-know-about-the-rule-of-capture [https://perma.cc/L98Q-FFYL].

13. *See* Louise de Leyritz, *What is Metadata? — Benefits and Examples*, CastorDoc (May 9, 2023), https://www.castordoc.com/blog/what-is-metadata [https://perma.cc/5753-QL3V].

14. *See generally id.*

as technology continues to intertwine with everyday life, and individual use is higher than ever,[15] the resource becomes more and more valuable every day, causing parties to race to the courts seeking protection when they feel that value has been wrongly apportioned. Second, the physical properties of metadata create a complex puzzle for the courts, especially because property rights have traditionally covered only tangible property.[16] Because of its novelty in value and amorphous character, the lack of legal protection for metadata can be explained by the Rule of Capture. Nonetheless, as the resource increases exponentially in value, this Comment predicts a parallel increase in judicial protection. This Comment explains why, in the United States, this protection will likely be grounded in the Constitution, either classifying the data as property itself or recognizing it as so personal to be protected as a matter of privacy.[17]

The purpose of this Comment is threefold: (1) to inform the reader about the history of the Rule of Capture, discuss how it has been applied in different contexts, and explain the circumstances that supported its judicial application; (2) to analyze the developing history of privacy jurisprudence, as it pertains to metadata, specifically through the lens of the Rule of Capture; and (3) to argue in favor of increased recognition and protection of individual privacy rights based in the Fourth Amendment of the U.S. Constitution.

To accomplish this purpose, Part II introduces and defines the subjects—privacy and metadata—as well as provides a brief history of their treatment under the law of the United States. Part III reconciles this treatment by drawing parallels between other resources like water, oil, and wild animals, explaining how courts employ the Rule of Capture and when it is most applicable. Part III continues explaining that as metadata evolves, the Rule of Capture will fall out of style and be replaced by individual privacy protections grounded in the Constitution.

Part IV recounts key developments in privacy law pertaining to metadata, seeking to understand their outcomes by way of a Rule of Capture analysis. Finally, Part V addresses and rebuts a counterargument to the individual rights approach, arguing that we exist in a transformative period of privacy law and can expect to see the Supreme Court, with increasing frequency, acknowledge and accept individual privacy protections based on the Fourth Amendment of the U.S. Constitution.

---

15. Laura Silver, *Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally*, Pew Rsch. Ctr. (Feb. 5, 2019), https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally [https://perma.cc/HUZ6-WP5P].

16. *See* U.S. Const. amend. IV.

17. Some commentators even believe privacy itself to be so important as to be the likely subject of the next constitutional amendment. *See, e.g.*, Deborah Pierce, *Reasons Why We Should Amend the Constitution to Protect Privacy*, 84 Chi.-Kent L. Rev. 851, 852 (2010) (arguing "the best way to address privacy is to add it expressly to the Constitution via a [c]onstitutional amendment").

II. DATA COLLECTION IN THE UNITED STATES

In 1971, the term metadata was unheard of.[18] Nonetheless, Arthur Miller, author of *The Assault on Privacy*, predicted its future importance.[19] "Given the advancing state of both the remote sensing art and the capacity of computers to handle an uninterrupted and synoptic data flow," he predicted, "there seem to be no physical barriers left to shield us from intrusion."[20] Miller's early hypothesis was likely scoffed at during its time, the same way someone might scoff today at a suggestion that advertisers will pay real money to know how many times a consumer's iPhone connects to its charger. This is because, at that time, technology had yet to evolve to a space where that kind of data was relevant, much less valuable; for example, GPS would not be introduced to the world until two years later.[21] Toshiba would not launch the world's first mass-marketed laptop computer until 1985,[22] and Apple would not begin to market iPhones until 2007.[23] To continue the analogy to oil and gas introduced above, metadata's value was essentially that of oil before the invention of derricks and combustion engines: not only was there no real way to extract it, but even if doing so was possible, there was no use for it. As handheld technology became more popular moving into the twenty-first century, however, both data extraction and use received increased demand as every individual with a cell phone would eventually produce millions of bytes of their own metadata every day.[24] The first significant instance of this newfound value receiving public attention at a large scale would emerge from governmental necessity following the September 11 terrorist attacks on the United States.

In September 2001, a series of foreign attacks stirred up support for the passage of the USA PATRIOT Act (Patriot Act or the Act) only forty-five days following 9/11 in an effort to tighten U.S. national security.[25] Among other things, the Act expanded the government's surveillance capabilities, including phone taps—both foreign and domestic—and made it easier for federal agencies to share this information with each other.[26] This new law initially received praise from an insecure American public willing to

18. It actually would not even begin to emerge until the 1990s. *See* Leyritz, *supra* note 13.

19. *See* Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers 46 (1971).

20. *Id.*

21. *See Satellite Navigation–Global Positioning System (GPS)*, Fed. Aviation Admin. (Dec. 27, 2022), https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps [https://perma.cc/GMG7-GVHZ].

22. *See First of Their Kind: Products*, Toshiba (2023), https://toshiba-mirai-kagakukan.jp/en/history/ichigoki/products.htm [https://perma.cc/RBV8-5NUA].

23. Raymond Wong, *What it's Like to Use the Original iPhone in 2017*, Mashable (June 29, 2017), https://mashable.com/article/original-iphone-2g-does-it-still-work [https://perma.cc/DU23-97U2].

24. *See* Branka Vuleta, *How Much Data is Created Every Day? + 27 Staggering Stats*, Seed Sci. (Oct. 28, 2021), https://seedscientific.com/how-much-data-is-created-every-day [https://perma.cc/9ZC8-9DRU].

25. The Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

26. *See id.*

temporarily relinquish freedoms in exchange for safety.[27] However, after several decades in force, in combination with the increased value of metadata as a resource, the statute's lenience in collecting innocent citizens' phone records, computer records, credit history, and banking history has been criticized as an abuse of privacy.[28]

The Patriot Act marked the first instance of large-scale recognition of the value in metadata.[29] Specifically, aspects of phone records, later termed "telephony data," were considered resourceful in their ability to locate and prevent terrorist activities.[30] The issue was, to determine which calls, emails, and text messages were linked to terrorism, the government used "bulk collection" techniques, sorting through the metadata of millions of innocent Americans.[31] This was legally justified under the Patriot Act, leaving telephone companies and service providers powerless in the face of government requests.[32] In an Administration White Paper addressing the bulk collection, the government explained:

> In the context of communications metadata, in which connections between individual data points are important, and analysis of bulk metadata is *the only practical means* to find those otherwise invisible connections in an effort to identify terrorist operatives and networks, the collection of bulk data is relevant to FBI investigations of international terrorism.[33]

For metadata, the Patriot Act was like Spindletop in terms of the resource's newfound value.[34] Information that was once considered useless now presented the opportunity for its possessor to piece together intimate details about the history and habits of its creator; for instance, the 45% of Americans who owned cell phones in 2001.[35] As technology advanced exponentially, it is clear why this resource's value likewise skyrocketed,

---

27. *See* Lydia Saad, *Americans Generally Comfortable With Patriot Act*, GALLUP (Mar. 2, 2004), https://news.gallup.com/poll/10858/americans-generally-comfortable-patriot-act.aspx [https://perma.cc/A3GX-WHYR].

28. *See Surveillance Under the Patriot Act*, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act [https://perma.cc/MTB2-DH7D].

29. *See* Jake LaPerruque, *The History and Future of Mass Metadata Surveillance*, POGO (June 11, 2019), https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance [https://perma.cc/QS3D-5WHQ].

30. NAT'L SEC. AGENCY, ADMINISTRATRION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2–3 (2013), https://irp.fas.org/nsa/bulk-215.pdf [https://perma.cc/R2TQ-YTC4].

31. *See* LaPerruque, *supra* note 29.

32. *See id.*

33. *See* NAT'L SEC. AGENCY, *supra* note 30, at 5 (emphasis added).

34. *See* B.A. Wells & K.L. Wells, *Spindletop Launches Modern Petroleum Industry*, AM. OIL & GAS HIST. SOC'Y (Dec. 31, 2009), https://aoghs.org/petroleum-pioneers/spindletop-launches-modern-oil-industry [https://perma.cc/LZD6-WVZD].

35. *See Number of Mobile Wireless Connections Per 100 People in the United States from 2001 to 2011*, STATISTA (Mar. 21, 2013), https://www.statista.com/statistics/184946/estimated-mobile-wireless-penetration-rate-in-the-us-since-2001-nruf [https://perma.cc/R4MM-KUTN].

as today, cellphone ownership—the principal method for the creation of metadata—approaches 100% in the United States.[36]

In tandem with the development of technology used to *create* metadata, so too was technology developed to *collect* metadata.[37] However, unlike the first flashy iPhone commercial to be televised,[38] collection tools remained in the shadows, likely due to the concern that they would be perceived as potentially facilitating privacy violations.[39] Nonetheless, with the Patriot Act legitimizing the government's bulk collection practice, tools and programs continued to develop for the purpose of siphoning metadata, an especially easy task since, at the time, such data collection was virtually unrestricted.[40] The National Security Agency (NSA), a lesser publicized intelligence agency of the United States government, was at the height of its power in terms of data collection.[41] It would take nearly fifteen years following the Patriot Act's passage for the details of the extent of the government's collection practice to be exposed.[42]

In 2013, the United States public was reminded of a similar insecurity it felt in the wake of 9/11; however, this time, rather than being used as a shield, the public began to question whether the Patriot Act was, in fact, being used as a sword.[43] This was the year that an NSA contractor named Edward Snowden disclosed highly classified information about several global surveillance programs utilized to collect metadata by the United States and other foreign governments.[44] After years of work for the NSA, Snowden had become upset with the disparity between the government's actual collection practices and how they were perceived by the public.[45] Months before the disclosure, a period Snowden would refer to as his "breaking

36. *See Mobile Fact Sheet*, Pew Rsch. Ctr. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/84JG-B9N5].

37. *See Surveillance Under the USA/PATRIOT Act*, ACLU (Oct. 23, 2001), https://www.aclu.org/documents/surveillance-under-usapatriot-act [https://perma.cc/CRU5-73VZ].

38. Danackermangreenberg, *First Official iPhone Ad*, YouTube (Feb. 26, 2007), https://www.youtube.com/watch?v=6Bvfs4ai5XU [https://perma.cc/ES69-WWJA] (reposting the original ad titled "Hello" by Apple).

39. *Cf. Surveillance Under the USA/PATRIOT Act*, *supra* note 37.

40. *See id.*

41. With the Patriot Act legitimizing bulk collection, the same power would not be limited until the Act was amended following the Snowden disclosures, preventing such indiscriminate collection. *Compare* The Patriot Act, *supra* note 25, *with infra* notes 61–64 and accompanying text; *see also* Christopher Drew & Somini Sengupta, *N.S.A. Leak Puts Focus in System Administrators*, N.Y. Times (June 23, 2013), https://www.nytimes.com/2013/06/24/technology/nsa-leak-puts-focus-on-system-administrators.html [https://perma.cc/9MU9-CLN6] (explaining how the "two-man rule," implemented following the Snowden disclosures, "would limit the ability of . . . system administrators to gain unfettered access to the entie system" and "require a second check on each attempt to access sensitive information").

42. *See generally Edward Snowden Discloses U.S. Government Operations*, History (June 5, 2020), https://www.history.com/this-day-in-history/edward-snowden-discloses-u-s-government-operations [https://perma.cc/D28E-LHLU].

43. *See generally id.*

44. *Id.*

45. *See* Conor Friedersdorf, *What James Clapper Doesn't Understand About Edward Snowden*, The Atlantic (Feb. 24, 2014), https://www.theatlantic.com/politics/archive/2014/02/what-james-clapper-doesnt-understand-about-edward-snowden/284032 [https://perma.cc/8XNP-92RF].

point," he accused then-Director of National Intelligence, James Clapper, of directly lying to Congress under oath.[46] Soon after, Snowden fled the United States, and his story received national attention after being published in *The Guardian*, *The Washington Post*, and other notable news outlets.[47]

After these disclosures came to light, Americans were astonished to discover just how extensive the United States' data collection had become.[48] Programs like XKeyscore and DNI Presenter enabled the government to have virtually unlimited access to metadata communicated through computer networks.[49] DNI Presenter allowed the NSA to access stored emails, Facebook chats, and private messages.[50] XKeyscore, an even more powerful tool, allowed "'real-time' interception of an individual's internet activity."[51] Although the NSA claimed the programs' usage was narrowly tailored toward essential and specific collection efforts, critics[52]—including Snowden—feared the potential for abuse, suggesting that such tools are, in fact, not used exclusively for the purposes that prompted the Patriot Act: counterterrorism.[53]

The issue with the NSA's bulk collection program was not necessarily that it was against the law since, again, even at this time, metadata was nowhere near considered as personal, much less valuable, as it is today.[54] Instead, Snowden's disclosures alerted the public to the idea that the parameters of this kind of data collection were far broader than they had previously understood.[55] Until then, programs like XKeyscore and DNI Presenter were kept secret, allowing the NSA to reassure the average U.S. citizen that their data was likely never collected since even collection under the broad Patriot Act required some process.[56] Nonetheless, by disclosing the capabilities of XKeyscore, Snowden revealed that the data of innocent individuals may still be vulnerable to exposure, even without a warrant, so long as, for example, an NSA analyst possesses certain identifying information like an email or IP address.[57] Furthermore, warrants for the collection were obtained through a special court (FISC) established by the Foreign

46. *Id.*
47. *Edward Snowden Discloses U.S. Government Operations*, *supra* note 42.
48. *See* Friedersdorf, *supra* note 45.
49. Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, The Guardian (July 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [https://perma.cc/KPH2-SSP4].
50. *Id.*
51. *Id.*
52. *See* Jay Stanley, *Why Government Access to Metadata is More Than a "Modest Encroachment" on Privacy*, ACLU (June 7, 2013), https://www.aclu.org/news/national-security/why-government-access-metadata-more-modest [https://perma.cc/HYE4-UV7A].
53. *See* Ellen Nakashima & Sari Horwitz, *Newly Declassified Documents on Phone Records Program Released*, Wash. Post (July 31, 2013), https://www.washingtonpost.com/world/national-security/governments-secret-order-to-verizon-to-be-unveiled-at-senate-hearing/2013/07/31/233fdd3a-f9cf-11e2-a369-d1954abcb7e3_story.html [https://perma.cc/ZY5L-HHTP].
54. *See generally id.*
55. *See id.*
56. *See* Greenwald, *supra* note 49.
57. *See id.*

Intelligence Surveillance Act of 1978 (FISA).[58] FISC proceedings are non-adversarial and take place *ex parte* and behind closed doors, meaning that the details are not publicly accessible.[59] Between 1979 and 2006, the FISC was presented with over 22,900 warrant applications, only 5 of which were denied.[60] These striking statistics suggest that the FISC was more of a mere formality than a democratic institution working to protect the privacy of individual citizens.

In response to the public's demand for more transparency regarding the collection of their metadata, Congress enacted the USA FREEDOM Act (USA Freedom Act) on June 2, 2015, amending the Patriot Act.[61] The modification's full title—"Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015"—purported to provide a more "balanced approach" to data collection, enabling the government to continue efforts to deter terrorism while creating safeguards that protected individual privacy rights.[62] Among the safeguards introduced, "bulk" metadata collection was no longer allowed, meaning that the NSA must request *specific* records, rather than the previous practice of cellphone companies handing over entire databases for the agency to sift through at will.[63] Additionally, the USA Freedom Act required certain disclosures to be made by the FISA court, namely "novel" interpretations of the law that would modify the courts' precedent.[64] Interestingly, the USA Freedom Act did not mandate the disclosure of similarly novel decisions that had already occurred in the courts under the Patriot Act—the details of which might have verified Snowden's allegations.[65]

While the USA Freedom Act made significant progress in the area of surveillance reform by limiting the government's ability to collect bulk catalogs of personal data, it continued to permit various forms of metadata collection so long as there was a remote link to a legitimate and properly warranted target.[66] Further, the vague nature of FISC decisions left Americans curious about how remote that link must be: "Even surveillance aimed at a single target under the call detail records program can quickly

58. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783.

59. *See Foreign Intelligence Surveillance Court (FISC)*, Elec. Priv. Info. Ctr., https://epic.org/foreign-intelligence-surveillance-court-fisc [https://perma.cc/CT8M-YXPJ].

60. *See id.*

61. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

62. *Id.*; Ellen Nakashima, *With Deadline Near, Lawmakers Introduce Bill to End NSA Program*, Wash. Post (Apr. 28, 2015, 7:04 PM), https://www.washingtonpost.com/world/national-security/with-deadline-near-lawmakers-introduce-bill-to-end-nsa-program/2015/04/28/8fd1cf6e-edb4-11e4-a55f-38924fca94f9_story.html [https://perma.cc/7JJM-E2WG].

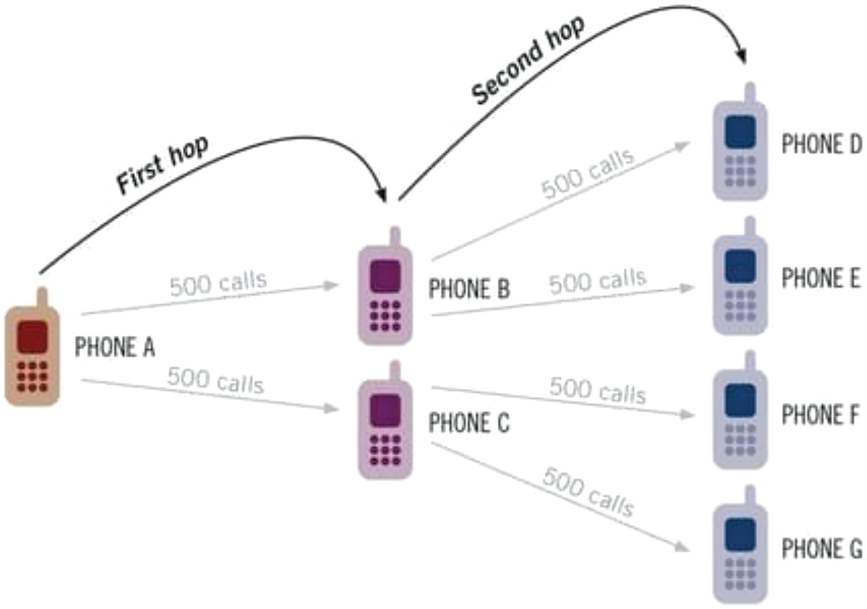
63. LaPerruque, *supra* note 29.

64. *Id.*

65. *See* Spencer Ackerman, *ACLU Takes on FISA Court Over Secret Decisions on Surveillance Laws*, The Guardian (Oct. 19, 2016, 4:14 PM), https://www.theguardian.com/law/2016/oct/19/aclu-fisa-court-surveillance-laws-classified [https://perma.cc/Y296-7EZU].

66. *See generally* Off. of the Dir. of Nat'l Intel., Statistical Transparency Report Regarding the Use of National Security Authorities 29–31 (2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf [https://perma.cc/MJ76-DLRM].

snowball, which means collection of phone metadata is highly damaging to individual privacy rights."[67] Therefore, an individual may still be exposed to government collection tools without notice if, for example, they work with someone whose father-in-law is the acquaintance of the grandfather of a suspected terrorist.[68] The image below illustrates how this may occur under the NSA's current practice. "Even without revealing the content of calls, the records of who you are calling and when can reveal the most intimate details about your life," suggesting that this information, which was becoming increasingly personal, required even more protection.[69]



Pilawski Figure 18[70]

Even after the USA Freedom Act introduced what were then considered to be sufficient safeguards, the surveillance tools possessed by the United States and its respective ability to monitor its own citizens' metadata remained troubling. Despite its appearance as a more modest approach to the objectives originally set forth by the Patriot Act, technological advancements had saturated the supply of existing metadata for collection, and the NSA alone continued to collect over 19,000,000 phone records between May 23, 2018, through the end of 2018.[71]

67. LaPerruque, *supra* note 29.
68. *See id.*
69. *Id.*
70. Off. of the Dir. of Nat'l Intel., *supra* note 66, at 29.
71. *Id.* at 31.

Additionally, although not this Comment's explicit focus, the increased popularity and use of social media applications like YouTube, Instagram, and TikTok has raised similar concerns in regard to the collection of metadata.[72] While most apps purport to only use the collected personal data, such as location and "click and search" habits, to improve the user's experience within their own service, popular social media app TikTok has received recent criticism for its practice of marketing the metadata collected from its users to third parties who are under no obligation to disclose, much less protect, how and where they are using the data.[73] Even more concerning, a recent study noted that these third parties' tracking abilities are not limited to the app from which they purchase the metadata, but can track activity across other sites even after a user closes the app.[74]

III. RECONCILING THE BROAD AUTHORITY TO COLLECT WITH THE LAW

Although, as explained in Part I, individual metadata has, at best,[75] received *limited* protections under current law, this is not to suggest that such minimal regulation of a resource of this kind by the courts defies precedent. Metadata, as a resource, is a unique example of the kind of asset that the law struggles to adapt to protect given its rapid increase in value over a short period of time, in conjunction with the asset's unique characteristics. Similar difficulties have arisen in regard to the ownership and correlative rights associated with oil and gas, water, and wild animals. Part III briefly juxtaposes historic legal decisions involving the early ownership of these resources with the courts' modern approach in an effort to reconcile the minimal individualized protection metadata has historically received. While the example of wild animals stands out as less similar than the other two comparisons, the early judicial reasoning employed by the court in *Pierson v. Post* provides valuable insight regarding what supported the Rule of Capture's application for more than two centuries.[76]

---

72. *See* Jada Jones, *TikTok Bans Explained: Everything You Need to Know*, ZDNet (Aug. 21, 2023), https://www.zdnet.com/article/tiktok-why-is-it-being-banned-from-government-devices [https://perma.cc/Z9U3-4FDQ]; Adam Satariano, *Meta Fined $400 Million for Treatment of Children's Data on Instagram*, N.Y. Times (Sept. 5, 2022), https://www.nytimes.com/2022/09/05/business/meta-children-data-protection-europe.html [https://perma.cc/5JZ3-MQCH].

73. *See* Tom Huddleston Jr., *TikTok Shares Your Data More Than Any Other Social Media App—and It's Unclear Where It Goes, Study Says*, CNBC (Feb. 22, 2022, 3:43 PM), https://www.cnbc.com/2022/02/08/tiktok-shares-your-data-more-than-any-other-social-media-app-study.html [https://perma.cc/ZHF5-9FCN].

74. *See* Brian Klais, *New Research Across 200 iOS Apps Hints That Surveillance Marketing is Still Going Strong*, URL Genius (Jan. 20, 2022), https://app.urlgeni.us/blog/new-research-across-200-ios-apps-hints-surveillance-marketing-may-still-be-going-strong [https://perma.cc/32KS-9Q7G].

75. At worst, being subject to bulk collection by the U.S. government during the lifetime of the Patriot Act.

76. *See* Pierson v. Post, 3 Cai. R. 175 (N.Y. Sup. Ct. 1805).

The Rule of Capture provides the correct and appropriate lens to understand how U.S. courts have treated the collection of metadata since the emergence of the resource. In the following Subsections, this Comment teases out which characteristics lead courts to apply the Rule of Capture to a particular resource and then demonstrates why metadata fits that same template.

A. Wild Animals

One of the earliest and most notable instances of the Rule of Capture's application is found in the Supreme Court of New York's reasoning in the 1805 case, *Pierson v. Post*.[77] In this case, a dispute between two local hunters over the rightful possession of a wild fox caused the court to ignore traditional common law precedent and instead rely on a variety of alternative sources of reasoning to redefine notions of property and ownership.[78] Some would later consider this decision to be the most famous case in American property law.[79]

While hunting a wild fox, Post and his hound began chasing the animal for some time through a vacant property.[80] During the same chase, another hunter named Pierson encountered the fox; however, Pierson swiftly killed and retrieved the animal.[81] Post sued, claiming that under the common law governing the hunting of wild animals, because he had been engaged in a chase with the fox, it was legally his property.[82] Post felt he was wronged by Pierson, who intercepted the animal and interfered with his hunt.[83] The trial court agreed, applying the traditional common law rule and awarding Post damages in trespass.[84] Pierson appealed.[85]

Despite the custom at the time, which recognized rightful ownership from the pursuit of the animal alone, the majority opinion pieced together a patchwork of reasoning, dating back as far as the fifth century, to change the rule and suggest that pursuit alone is insufficient to grant ownership; rather, actual capture—in this case mortally wounding the animal—was required.[86] The court noted that although Pierson's actions may have been considered impolite, they were not of the kind requiring legal protection.[87] Judge Livingston's dissent argued that pursuit was the proper gauge for ownership since, at the time, the fox was considered a "wild and noxious beast," and a lower standard for ownership encouraged hunters to eradicate

77. *Id.*
78. For example, the Institutes of Justinian (fifth century), the writings of Henry de Bracton (thirteenth century), and Samuel von Pufendorf (seventeenth century). *Id.* at 177–78.
79. Thomas W. Merrill & Henry E. Smith, Property: Principles and Policies 87 (2d ed. 2012).
80. *See Pierson*, 3 Cai. R. at 175–76.
81. *See id.*
82. *See id.* at 176.
83. *See id.* at 175.
84. *See id.*
85. *See id.*
86. *See id.* at 176–77.
87. *See id.* at 179.

the species.[88] Interestingly, the majority notes that one reason counseling its shift in jurisprudence was that the rule was easier to administer.[89] As explained in the following Section, unworkability—either caused by physical attributes or lack of technology—tends to be the strongest factor that counsels for application of the Rule of Capture.[90] Here, in the early nineteenth century, technology that might determine who first captured the animal, like cameras or modern hunting tools, had yet to be developed. Additionally, wild animals like the fox possessed physical characteristics that made them especially evasive.[91] In combination, these facts supported the application of the Rule of Capture to wild animals.

> We are the more readily inclined to confine possession or occupancy of beasts *ferae naturae*, within the limits prescribed by the learned authors above cited, for the sake of certainty, and preserving peace and order in society. If the first seeing, starting, or pursuing such animals, without having so wounded, circumvented or ensnared them, so as to deprive them of their natural liberty, and subject them to the control of their pursuer, should afford the basis of actions against others for intercepting and killing them, it would prove a fertile source of quarrels and litigation.[92]

As suggested above, although it may be difficult to see the similarity between wild animals and metadata at this point, the case is relevant to show what type of circumstances caused the court to adopt a lower standard of judicial protection. The dissenting opinion counsels that ownership should exist upon pursuit—a higher standard of protection and a lower standard of ownership.[93] This case, and the ones that follow, are great examples of the fact-specific inquiries with which courts engage to determine if the Rule of Capture should apply. Unlike 1805, the modern United States is much more developed, and thus, Pierson would be far less likely to interfere with Post's hunt today.[94] With these updated circumstances, however, so too has the law been updated—despite the expected "lag time" for the proper issues to reach the courts—in the form of conservation and wildlife laws, hunting regulations, and modern technology to help identify ownership of wild animals.[95] These supplemental protections can be explained by the resource's increased value: whereas in 1805, wild animals like foxes

88. *See id.* at 180 (Livingston, J., dissenting).
89. *See id.* at 179.
90. *See, e.g.*, Hous. & Tex. Cent. R.R. Co. v. East, 81 S.W. 279, 280–81 (Tex. 1904).
91. *See Pierson*, 3 Cai. R. at 179–80.
92. *See id.* at 179.
93. *See id.* at 180–82 (Livingston, J., dissenting).
94. Because there is more developed land and, as hunting itself is no longer a necessity for survival, the characteristics—specifically value—have fluctuated with regard to foxes. Today, a fox would be considered to have a completely different form of value (probably much higher than in *Pierson*), and courts have responded properly with more nuanced protection, in contrast to the Rule of Capture.
95. *See generally* Stefan Sirucek, *Extremely Rare Fox Seen in Yosemite—First Time in 100 Years*, Nat'l Geographic (Feb. 3, 2015), https://www.nationalgeographic.com/animals/article/150204-sierra-nevada-red-fox-species-animals-science-rare [https://perma.cc/7RJP-NZYX].

were considered "noxious beast[s],"[96] today, they receive significantly more protection because, as the country grew more crowded, the supply of wild animals plummeted and their value significantly increased.[97] In the context of wild animals today, the Rule may still have occasional applicability in rare cases; however, due to over two-hundred years of legal development and technological advancement, it would be unusual for a court to apply the Rule of Capture to the ownership of wild animals as it did in *Pierson v. Post*.

B. Water

Another relevant instance of courts applying the Rule of Capture involved one of the most abundant resources on Earth: water.[98] In the early United States, courts initially expounded on the reasoning employed in *Pierson*, highlighting the similarly "fugacious" characteristics between wild animals and groundwater.[99] The common law rule permitted nineteenth-century landowners autonomy to withdraw—that is, reduce to certain control—unlimited quantities of water without regard for the negative effects suffered by neighboring landowners.[100] However, as circumstances changed,[101] so too did the American jurisprudence. Through a patchwork of various legal schemes, developed in different states at different times, slowly but surely, courts began to increase judicial protection and regulation regarding water use, straying further away from the Rule of Capture as technology advanced and the resource became more valuable.[102]

Just like oil, water has always been treated differently than traditional resources due to its peculiar attributes. Traditionally, the English Rule governed the use of water, which asserted that a landowner may take and use all water captured on their land so long as they were not acting with malice towards a neighboring landowner, despite the chance that such action results in depriving that neighbor use of the water.[103] In so many words, this was merely an early application of the Rule of Capture.[104] This early rule governing water, arising from the English common law, likely went unchallenged due to the heavy rains in the region, cool weather, plentiful access to coastal waterways, and lack of significant technological need for the resource. However, as the American common law continued to

96. *Pierson*, 3 Cai. R. at 180 (Livingston, J., dissenting).
97. *See* Sirucek, *supra* note 95.
98. *See* Westmoreland & Cambria Nat. Gas Co. v. De Witt, 18 A. 724, 725 (Pa. 1889).
99. *Id.* (explaining that having "the power and tendency to escape without the volition of the [landowner]," meant water, oil, and natural gas could not be governed by the rules applicable to hard-rock minerals).
100. *See* Anthony Scott & Georgina Coustalin, *The Evolution of Water Rights*, 35 Nat. Res. J. 821, 874–75 (1995).
101. For example, increased population causing increased demand for water supply or technological developments such as water wells and advanced irrigation systems. *See id.* at 955.
102. *See Water Law: An Overview*, Nat'l Agric. L. Ctr., https://nationalaglawcenter.org/overview/water-law [https://perma.cc/2268-MP8Q].
103. *Id.*
104. *See id.*

develop, this would change. For example, the Reasonable Use Doctrine would become a popular diversion from the English Rule, creating a more nuanced and fact-specific structure of legal protection in an effort to put the resource to its best use.[105] Nonetheless, an opinion styled *Houston & Texas Central Railroad Co. v. East* provides an illustrative example of when and why courts tend to apply the much simpler Rule of Capture, especially when they are asked to regulate resources that technology is not yet able to help them understand.[106]

In *Houston & Texas Central Railroad Co. v. East*, a railroad company dug a water well on its property to supply the resource for its commercial needs.[107] The well was designed to provide for both the trains and the shops, eventually producing 25,000 gallons of water each day.[108] However, in doing so, the company dried out the well of a neighboring landowner who used the supply for his house.[109] The neighboring landowner sued the railroad company, eventually asking the Supreme Court of Texas to choose between the application of the Rule of Capture or the Reasonable Use Doctrine.[110] Noting that in the "absence . . . of positive authorized legislation," the court, at that time, was ill-equipped to create judicial protections or requirements regarding ownership of a resource that it didn't completely understand.[111] Resting its decision on two key policy considerations, the Supreme Court of Texas applied the Rule of Capture, reasoning:

> Because the existence, origin, movement, and course of such waters, and the causes which govern and direct their movements, are so secret, occult, and concealed that an attempt to administer any set of legal rules in respect to them would be involved in hopeless uncertainty, and would, therefore, be practically impossible[, and b]ecause any such recognition of correlative rights would interfere, to the material detriment of the commonwealth, with drainage and agriculture, mining, the construction of highways and railroads, with sanitary regulations, building, and the general progress of improvement in works of embellishment and utility.[112]

Interestingly, the *East* court justified its application of the Rule of Capture by appealing to the unworkable nature of such regulation, similar to the justification provided by the *Pierson* court.[113] First, the *East* court noted that the physical attributes of water are unique in that they make the resource incredibly difficult to grasp—almost a form of *ferae naturae*.[114] Although neither *East* nor *Pierson* mention the failure of technology to aid this understanding, in hindsight, we might find it obvious that technology

105. *See id.*
106. *See* Hous. & Tex. Cent. R.R. Co. v. East, 81 S.W. 279, 280–81 (Tex. 1904).
107. *See id.* at 280.
108. *Id.*
109. *Id.*
110. *See id.* at 280.
111. *See id.* at 280–81.
112. *Id.* (quoting Frazier v. Brown, 12 Ohio St. 294, 311 (1861)).
113. *See id.*; Pierson v. Post, 3 Cai. R. 175, 179 (N.Y. Sup. Ct. 1805).
114. *See East*, 81 S.W. at 280–81; *see also Pierson*, 3 Cai. R. at 175–76.

would become a key motivator for the law's evolution away from the Rule of Capture.[115] Second, the *East* court concluded its policy considerations by expanding upon its first point: because water, as a resource, is so mysterious in character, attempts to establish a more complex scheme of regulation would be frivolous, merely interfering with more valuable developments.[116]

What would soon happen would become a sign that the Rule of Capture was on its way out of fashion. New technology would lead to an increase in the resource's value; simultaneously, the resource's increased value would motivate the development of new technology.[117] Together, these forces exponentially added to the pressures placed on the courts to establish a more complex scheme of judicial protection, guarding correlative rights while respecting notions of individual ownership. A prime example, just more than a decade after the *East* decision, appeared in the form of an amendment to the Texas Constitution.[118] Following a period of extreme drought between 1910 and 1917—dramatically increasing the value of water as a resource—the Texas Legislature passed a conservation amendment declaring conservation of the resource a "public right[] and dut[y]."[119] Although the amendment did not overrule the application of the Rule of Capture, it did open the door for the legislature to pass more nuanced and appropriate laws to better regulate the resource—a step in the direction away from the English Rule.[120] As water-related technology continued to develop, so did the intricacies of water law in the United States.

To contrast the early approach taken by the courts in applying the Rule of Capture, the Kansas City Court of Appeals in *Higday v. Nickolaus* explains why the Reasonable Use Doctrine is more appropriate given the changed circumstances.[121] In this 1971 decision, a group of landowning farmers sued the City of Columbia for an injunction preventing the city from extracting any more water from their water wells.[122] At the time, a water shortage in the city had prompted officials to travel and acquire rural farmland near a water reservoir for the purpose of extracting and transporting the resource back to the city for sale.[123] However, the city's plan to extract over 11 million gallons a day quickly caused the reservoir to dry out and left neighboring farmers seeking a judicial remedy.[124] When the farmers sued, the city drew attention to the common law Rule of Capture, arguing that because

115. For example, the way that modern cameras might allow use to determine "ownership" of the wild fox and modern excavation tools can help to determine the size, shape, and location of a water reservoir to determine "ownership," or at least what proportions underlie which tracts of land, no longer causing the resource to be understood as so mysterious to be "occult" as described by the *East* court. *See East*, 81 S.W. at 280–81.

116. *See id.*

117. *See* Scott & Coustalin, *supra* note 100, at 955.

118. *See* Barshop v. Medina Cnty. Underground Water Conservation Dist., 925 S.W2d 618, 626 (Tex. 1996).

119. Tex. Const. art. XVI, § 59(a) (amended 2023).

120. *See Barshop*, 925 S.W.2d at 626.

121. Higday v. Nickolaus, 469 S.W.2d 859, 865–66 (Mo. Ct. App. 1971).

122. *Id.* at 861–62.

123. *See id.*

124. *See id.* at 862.

the water was extracted on their land, they should not be limited in *how much* water they extracted.[125] The trial court agreed with the city, applying the Rule of Capture; however, on appeal, the court reversed in favor of the farmers, updating the common law and adopting the Reasonable Use Doctrine.[126] This change in precedent is likely explained by the resource's new value, in conjunction with the court's desire to put the resource to its best use.[127] Under the updated law, the city was found to be in the wrong; however, the court noted that if the city were to limit its extraction (say, to only 2 million gallons per day), then it was likely that they might do so legally.[128] The key is that the extraction must be reasonable relative to the circumstances.

Notably, several key circumstances have changed since *East*. Now, in the United States, water technology is much more advanced.[129] It is likely that the *Higday* court felt more confident relying on the quantities of water being extracted. Moreover, large trucks and pumping stations now exist to transport the water—increasing its value.[130] Further, suburban housing developments have increased in popularity, also increasing the resource's value.[131] Altogether, these considerations counsel for the courts to get involved, setting particularized rights and duties, in contrast to what they might have done in the past, simply applying the Rule of Capture's "first in time is first in right" scheme.

C. Oil & Gas

As a final example, and probably the most common today, this Comment highlights the application of the Rule of Capture in the context of oil and gas development. Although oil and gas are distinct resources, this Comment generally groups them together since, for our purposes, they are essentially identical in legal treatment, evolution of value, and development of technology. Just like the oilman's illustrative quote from this Comment's introduction, when oil was first discovered as a resource in the late nineteenth and early twentieth centuries, similar instances of drainage were routine. Because the courts were not yet alerted of the potential value of this new resource, nor did the technology or science at the time provide judges the tools to understand it, the Rule of Capture left neighboring landowners at the mercy of having their "milkshake" consumed by

125. *See id.* at 863–64.
126. *See id.* 869–72.
127. *See generally id.*
128. *See id.* at 871–72.
129. *See, e.g.*, *The More You Know: The History of Water Pumps*, Omnia Mech. Grp. (May 27, 2021), https://antler.nyc/the-more-you-know-the-history-of-water-pumps [https://perma.cc/AV8S-VT7C].
130. *See* Manya Kotian, *Pumping Stations in a Water Distribution System*, The Constructor, https://theconstructor.org/environmental-engg/water-supply/pumping-stations-in-a-water-distribution-system/79506 [https://perma.cc/HK3F-FMX8].
131. *See* Colin Stief, *The History and Evolution of Suburbs*, ThoughtCo. (Aug. 15, 2018), https://www.thoughtco.com/overview-of-suburbs-1435799 [https://perma.cc/WFP7-64ZA]; Alissa Walker, *No Water? No Subdivision.*, Curbed (June 5, 2023), https://www.curbed.com/2023/06/arizona-water-housing-development-sprawl.html [https://perma.cc/2G5X-LM4K].

a neighbor's drill, so long as the drill did not cross the property line.[132] Their only option: develop their own well and engage in the same drainage that they had become victim of.[133] Given the novelty of the resource and its fugacious nature, judicial protection was out of the question.

In *Kelly v. Ohio*, the Supreme Court of Ohio applied the Rule of Capture in an early 1897 decision describing the judicial understanding of the resource at the time.[134] There, the court refused to impose liability on a defendant who allegedly placed their oil wells in positions with the intention of draining a neighboring plaintiff's reservoir.[135] After the neighboring plaintiff filed suit, the court noted that the plaintiff might have a remedy in the case of negligent or wasteful capture; however, simply because the defendant was *believed* to have drained a resource from under the plaintiff's land was insufficient evidence to give rise to liability.[136] The *Kelly* court noted that regulations such as spacing rules are better suited to resolve these issues, passing responsibility to the legislature to provide protection.[137] Again, this is not an uncommon practice, given the characteristics of oil and gas. Just like a wild animal or a groundwater reservoir in the nineteenth century, at this time, the courts lacked sufficient understanding of the resource to provide judicial protection and instead relied on the more simplistic Rule of Capture.

Eventually, as advancements in technology and the energy market were made, oil and gas became more valuable and several states departed from the Rule of Capture, transitioning to a more protective set of legal rules.[138] Some of these new protections included conservation laws, setting allowable limits for drilling, and increasing agency oversight.[139] Courts, too, began to imply covenants into oil and gas contracts, for example, against drainage, in an effort to protect the rights of individual landowners.[140] Nonetheless, some states continue to apply the Rule of Capture, perhaps indicating that when it comes to a resource such as natural gas, either: (1) technology is not yet advanced enough for the courts to be confident in creating particularized rules, or (2) the courts feel that landowners have sufficient remedies in alternative forms of protection.[141] The answer is likely a combination of both explanations, as well as a consideration of

132. *See* Kelly v. Ohio Oil Co., 49 N.E. 399, 401 (Ohio 1897).
133. *See id.*
134. *See id.*
135. *See id.*
136. *See id.*
137. *See generally id.* at 400 ("[I]n view of the well-known tendency of said wells to drain a large extent of territory immediately surrounding them, it is the custom and almost universal practice of oil operators, when operating adjoining lands, to locate their wells at least two hundred feet from the line of lands . . . .").
138. *See, e.g.*, Champlin Expl., Inc. v. W. Bridge & Steel Co., 597 P.2d 1215, 1216 (Okla. 1979) (holding that the Rule of Capture was inapplicable).
139. *See, e.g.*, Ray R. Friederich & Maurice E. Garrison, *Legal History of Conservation of Oil and Gas in North Dakota*, 24 N.D. L. Rev. 175, 179–80, 189–90 (1948); Phillip E. Norvell, *The History of Oil and Gas Conservation Legislation in Arkansas*, 68 Ark. L. Rev. 349, 355–57 (2015).
140. *See* Amoco Prod. Co. v. Alexander, 622 S.W.2d 563, 568 (Tex. 1981).
141. *See generally* Wronski v. Sun Oil Co., 310 N.W.2d 321, 323–24 (Mich. Ct. App. 1981).

the new practice of hydraulic fracturing, also known as directional drilling, which allows a developer to drill for gas horizontally, deep below neighboring tracts of land.[142] In 2008, the *Garza Energy* decision, an opinion by the Supreme Court of Texas, extended the application of the Rule of Capture to a new form of drilling termed "fracking."[143] This novel and geographically wide-reaching style of drilling created an entirely unique set of issues for courts to address prior to regulating the practice.[144] Furthermore, technology was not available to determine exactly how far and in what direction the hydraulic fractures used to extract the natural gas extended.[145] Therefore, the majority explained, and the concurrence agreed, that the trespass law must be updated in a manner which resembles the Rule of Capture, allowing fracking gas developers to collect resources from underneath neighboring lands.[146] Notably, the dissenting opinion drew attention to the popular criticism of the Rule of Capture—that it would encourage drainage.[147] Nonetheless, the Rule of Capture won the day due to the novel characteristics of natural gas, the unique practice of fracking, and the fact that technology had not quite caught up to the resource to permit the court to create a reasoned scheme of protection for individual rights.

D. Metadata

Drawing on the discussion above, U.S. courts seem to rely on the Rule of Capture to regulate resource ownership when two critical circumstances are present. First, there must be a sense of novelty in regard to the value of the resource, whether due to new technology or an unprecedented form of application. Second, all resources historically governed by the Rule of Capture have possessed a uniquely amorphous character, rendering them—quite literally—difficult to grasp. Directly in line with this analysis is the evolution of metadata and surrounding technology. The emerging value of metadata is undeniable given the fact that it was virtually unrecognized prior to the Patriot Act, whereas now, it can be the difference between success and failure for an emerging business, offering critical insight into the habits of a company's customer base.[148] Forbes explained:

> In the modern digital age, [metadata] has immense value to your enterprise. That data can help to create a better overview of the financial activity within your organization, and can help you better understand (and subsequently capture) customers, to the extent that one of the most popular new initiatives in the last couple of years has been

142. *See generally* Coastal Oil & Gas Corp. v. Garza Energy Tr., 268 S.W.3d 1, 6–7 (Tex. 2008).
143. *See id.* at 17 (applying the Rule of Capture in the context of horizontal drilling).
144. *See id.*
145. *See id.* at 7.
146. *Id.* at 16–17.
147. *Id.* at 43–44 (Johnson, J., dissenting in part).
148. *See* Kurt Cagle, *The Value of Metadata*, Forbes (Feb. 26, 2019, 4:39 PM), https://www.forbes.com/sites/cognitiveworld/2019/02/26/the-value-of-metadata [https://perma.cc/V29B-UUP6].

> a move towards a "customer 360" application that lets you see your customers, current and potential, from many different perspectives.[149]

Additionally, perhaps even more than any of the resources previously discussed, metadata presents the courts with a relatively unprecedented characterization issue in that it is both invisible and intangible. Intellectual property law, which to a degree mirrors the issue, has received much criticism for facilitating the ownership of that which cannot (and, as some commentators argue, should not) be owned.[150] Similar concerns have led courts to apply the "hands off" principle that is the Rule of Capture to metadata.[151] However, advocates for the individualized protection of metadata should be hopeful given the technological boom that has occurred in the twenty-first century, which allows judges to understand metadata better in terms of what it is, how much is out there, what its use is, and who deserves to dictate where it goes.

Another commonality between the resources discussed above and their governance is that the application of the Rule of Capture is not permanent. With the exception of oil and gas in some states, the Rule of Capture has been a temporary solution that allowed both technology and the understanding of judges the time to catch up to the newfound value of a particular resource.[152] In its place, courts armed with a better grasp of the resource have substituted a more comprehensive analysis, resulting in a more nuanced scheme of protection.[153] So too, this Comment suggests the Rule of Capture, in relation to metadata, is approaching—if not already at—the point where it falls out of style, likely to be replaced by individual rights, secured and protected by the courts. The discussion to follow in Part IV analyzes recent developments concerning the protection of metadata in an effort to highlight two relevant avenues that have received much attention in the public zeitgeist: protection as a property right and protection as a privacy right. As briefly mentioned above, courts have struggled with—and are often criticized for—proscribing protection in the form of property rights for intangible things. Therefore, as this Comment explains, it is likely that, in line with recent judicial developments, the increased protection of metadata as a resource will occur through the mechanism of privacy law. As information is recognized as more and more personal, U.S. courts should extend the umbrella of privacy protections by recognizing that access to an individual's metadata is no different than access to the most intimate details of their life.

---

149. *Id.*

150. *See generally* Linus Torvalds, A Critique on Intellectual Property (2001), https://chsasank.com/classic_papers/intellectual-property-critique-linus-torvalds.html [https://perma.cc/M3CG-55G6]; Brian Martin, *Against Intellectual Property*, 21 Phil. & Soc. Action 7, 8 (1995).

151. *See infra* Section IV.

152. *See supra* Sections III.A–C.

153. *See supra* Sections III.A–C.

IV. RECENT DEVELOPMENTS

To better predict the direction that courts may take in protecting metadata, this Section will address the major cases that shed light upon the reasoning behind past judicial treatment of metadata. Along the way, it is impossible to ignore the resource's increased value and the adjacent technological evolution. The American public raised more and more concerns about individual rights violations as they recognized the increasingly personal nature of the data. To begin, it is important to acknowledge the emergence of the issue in the courts, initially receiving treatment from a Rule of Capture perspective. Next, this Section will fast-forward several decades to analyze a famous circuit split centering around the issue, which is helpful to highlight the conflicting philosophies behind the movement for a more nuanced protection scheme. Finally, this Section summarizes the current state of the law on metadata to provide a holistic picture of its evolution and a prediction, grounded in precedent, of its eventual destination.

A. *Smith v. Maryland*

Far before cellphones were invented—or most handheld technology for that matter—American courts first seriously addressed the issue of a third parties' unregulated access to an individual's "data about data"[154] in a case styled *Smith v. Maryland*.[155] Eventually reaching the Supreme Court, the 1979 case was centered around the robbery and subsequent harassment of Patricia McDonough.[156] McDonough was robbed of her wallet, which contained her personal information, including her phone number.[157] After receiving disturbing phone calls from a man claiming to be the robber, the police stepped in, eventually observing a suspicious vehicle around McDonough's house matching a description from the robbery.[158] The owner of the vehicle was named Michael Smith.[159] Law enforcement officers then approached Smith's telephone company requesting a pen register—an early form of technology that recorded call records, but not their content, one of the earliest forms of metadata collection—be placed on Smith's telephone.[160] Notably, the officers succeeded in installing a pen register without the aid of a warrant.[161]

Sure enough, the pen register was successful in its intended purpose, and the police noticed an outgoing call from Smith's to McDonough's home telephone.[162] This evidence, in conjunction with other evidence, allowed police to receive an actual warrant and arrest Smith, eventually discovering a phone book in his possession with McDonough's name specifically

154. Sinha, *supra* note 7, at 176.
155. Smith v. Maryland, 442 U.S. 735 (1979).
156. *Id.* at 737.
157. *See id.*
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.*

selected.[163] After McDonough identified Smith out of a lineup, Smith was charged with robbery.[164]

At trial, Smith argued that the evidence from the pen register was improperly obtained without a warrant, which violated his constitutional rights under the Fourth Amendment.[165] Nonetheless, both the trial and appellate courts found Smith's conviction proper.[166] The issue eventually reached the Supreme Court through successful petition by Smith.[167] While Smith's petition would provide a foundation for metadata's future regulation, perhaps due to how early in the resource's evolution the case occurred, the Supreme Court held that Smith's Fourth Amendment rights had not been violated and that a warrant was not required for police to use a pen register.[168] The Court applied a test developed years earlier in *Katz v. United States*,[169] which dealt with a similar issue but involved *actual* data rather than metadata.[170] The test defined a "search," and thus a potential constitutional violation, as requiring: (1) a subjective expectation of privacy and (2) that such an expectation was objectively reasonable.[171]

The U.S. government, which at this time was relatively inexperienced in terms of modern technology, argued, and the court held, that even if Smith could satisfy the first element of the *Katz* test, the pen register was not a "search" because, at that time, it was not considered objectively reasonable to think that a telephone company would protect an individual's call records.[172] Specifically, Justice Blackmun found such an expectation difficult to defend when the information (telephone metadata) was "voluntarily conveyed."[173] The Court distinguished *Katz* from *Smith*, holding that, while callers in 1979 may have had a reasonable expectation that the *content* of their conversations was not being shared, no such expectation existed in regards to their *metadata*.[174] The majority was unpersuaded by Smith's argument that because the phone was located in his home, the information was that much more personal; therefore, although pen registers may ordinarily be constitutional without a warrant, in this case, it had collected intimate details that Smith had no other way to protect.[175] In a sense, Justice Blackmun simply applied the Rule of Capture, electing to allow unregulated collection of what was beginning to seem like a new resource rather than creating a particularized set of rules about something he could not yet fully grasp.

163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.* at 738.
167. *Id.*
168. *See id.* at 745–46.
169. Katz v. United States, 389 U.S. 347 (1967).
170. *See Smith*, 442 U.S. at 739–40.
171. *See id.* at 740.
172. *See id.* at 742–43.
173. *See id.* at 744.
174. *See id.* at 741.
175. *See id.* at 743.

The crux of the majority's argument hinged on the relationship between the caller and the telephone company, insisting that the caller was aware of the implications stemming from the relationship and nonetheless continued to voluntarily allow absolute collection of the information exchanged during that relationship.[176] This notion of an implied awareness troubled Justice Marshall, which is reflected in his dissent[177]—likely because in decades prior, many American homes had yet to even install a telephone, meaning the technology and its implications were relatively new.[178] In his well-aged dissent, Marshall explained his disagreement, classifying Smith's exchange of information with the telephone company as involuntary, mainly because Smith did not have much of a choice.[179]

> [H]ere, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.[180]

Justice Marshall concluded his dissent by analogizing the instant case to *Katz*, arguing that even by collecting Smith's metadata, a constitutional violation had occurred:

> Just as one who enters a public telephone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded, if at all, solely for the phone company's business purposes.[181]

B. Circuit Split: *Klayman* and *Clapper*

Despite Justice Marshall's well-reasoned dissent in *Smith*, for more than thirty years, minimal movement occurred in the jurisprudence relating to the protection of metadata. As discussed above, major events like 9/11, the Patriot Act, and the disclosures made by Edward Snowden reinvigorated the discussion, yet limited new protections resulted.[182] For the most part, the framework of the Rule of Capture continued to allow the free collection of metadata without much legal consequence; however, as a new age of technology was ushered in by way of the iPhone, Smart Cars, 3-D

176. *See id.* at 742–44.
177. *See id.* at 748–52 (Marshall, J., dissenting).
178. *See* Statista Research Department, *Percentage of Housing Units With Telephones in the United States From 1920 to 2008*, Statista (Sept. 30, 2010), https://www.statista.com/statistics/189959/housing-units-with-telephones-in-the-united-states-since-1920 [https://perma.cc/U9BD-73YG] (revealing that the percentage of homes with telephones was 36.9% the 1940s, 61.8% in the 1950s, and 78.3% in the 1960s).
179. *See Smith*, 442 U.S. at 750 (Marshall, J., dissenting).
180. *Id.* (internal citation omitted).
181. *Id.* at 752 (quoting Katz v. United States, 389 U.S. 347, 352 (1967)).
182. *See supra* Part II.

technology, virtual reality headsets, and more,[183] American courts began to change their positions on the regulation of metadata.

In the 2010s, the discussion was revived by the conflicting lines of reasoning between the U.S. Courts of Appeals for the D.C. Circuit and the Second Circuit.[184] As explained below, two cases that would rise through the federal courts directly involved the government's practice of collecting metadata.[185] While the Second Circuit resolved the question of individual rights to metadata protection in favor of the individual—albeit on statutory grounds—the D.C. Circuit would not go so far, refusing to find sufficient harm to the individual whose data is collected through certain mass surveillance programs.[186] While both the D.C. Circuit and the Second Circuit carefully avoided ruling on the constitutionality of metadata collection, the U.S. District Court for the District of Columbia did not take the same cautious approach, instead finding that the practice likely violated the Fourth Amendment.[187] Although some of these opinions predate the amendment to the Patriot Act that followed the Snowden disclosures, thus involving outdated statutes, discussion of the *Klayman*/*Clapper* split is nonetheless valuable because it serves to take the judicial temperature on whether or not judges were prepared to protect data privacy through the Constitution.[188]

The first half of this infamous duo emerged in the U.S. District Court for the District of Columbia in 2013 as a challenge by Larry Klayman and other cell phone/internet service users.[189] In *Klayman v. Obama*, the plaintiffs sought to challenge the NSA's data collection program and argued, among other things, that the government's mass collection, even if authorized by the Patriot Act, was an unconstitutional search under the Fourth Amendment.[190] In response, the government countered by pointing to the need for preventative tools to combat terrorism.[191] Judge Richard Leon, however, was critical of the government's argument, as the NSA was unable to provide *specific* examples of the program's success in actually preventing

183. *See generally* Noel McKeegan, *Top Ten Technology Firsts of 2010*, New Atlas (Nov. 24, 2010), https://newatlas.com/technolgy-world-firsts-2010/16942 [https://perma.cc/FGR6-P54B].

184. *See* Randal John Meyer, *Second Circuit and* ACLU v. Clapper*: A Step in the Right Direction*, The Hill (May 11, 2015), https://thehill.com/blogs/congress-blog/judicial/241493-second-circuit-and-aclu-v-clapper-a-step-in-the-right-direction [https://perma.cc/4UAR-4ZUL].

185. *See id.*

186. *See id.*

187. Klayman v. Obama, 957 F. Supp. 2d 1, 42–43 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam) (granting the plaintiff's injunction, halting the government's bulk collection of metadata).

188. *See, e.g.*, *id.*

189. *Id.* at 7–8.

190. *Id.* at 11.

191. *Id.* at 21 (noting the government's argument that collection of metadata "function[ed] as a tool for counter-terrorism").

an attack.[192] Instead, it seemed that the collection was mostly prophylactic, helping to aid more traditional forms of counterintelligence.[193]

Judge Leon found that the plaintiffs had sufficient standing and acknowledged *Smith v. Maryland* as the controlling precedent.[194] These acknowledgments alone were a big step forward in the realm of legal protection for metadata; the intangible resource was finally recognized by a modern court as potentially deserving Fourth Amendment property-based protection. The recognition signaled a change in the times, suggesting data *about other data* had become recognized as a valuable resource that may need protection. The court's determination that the plaintiffs had standing was interestingly based on contentions made by the government.[195] Although Klayman attempted to show particular injuries to himself and his co-plaintiffs, Judge Leon was most convinced by the government's own description of the collection program as "comprehensive," involving Verizon, AT&T, and Sprint—the United States' three largest cell phone carriers.[196] To illustrate the program's importance, the government explained how valuable its *broad* database was to detect terroristic threats, which the court found to prevent the government from later arguing that the database was not so broad as to have collected the plaintiffs' data.[197] "Put simply, the Government want[ed] it both ways."[198]

After concluding that the plaintiffs had standing, the court turned to the constitutional claim.[199] Although *Smith* was identified as the controlling precedent, the court noted that *Klayman* and the NSA's bulk collection was notably different from the pen register used by police on a single individual in *Smith*.[200] For example, the pen register was temporary, and the information was not kept by law enforcement after the investigation, whereas here, the NSA admittingly retained collected data for five years.[201] Similarly, in *Smith*, law enforcement collected data directly, as opposed to the case at bar where the NSA collected from the service providers only to potentially, if ever, be used by law enforcement.[202]

Next, Judge Leon took issue with the scope of the NSA's program—the source of plaintiffs' standing—as the government had explained it collected metadata from "millions of people" rather than a single suspect, as in *Smith*.[203] Finally, and most important to our discussion, Judge Leon noted

192. *See id.* at 40 ("[T]he Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature.").
193. *See id.* at 40–41.
194. *Id.* at 29–30 ("The analysis of this threshold issue of the expectation of privacy must start with the Supreme Court's landmark opinion in *Smith v. Maryland* . . . .").
195. *See id.* at 27–29.
196. *Id.* at 27.
197. *See id.*
198. *Id.*
199. *Id.* at 29.
200. *Id.* at 31.
201. *Id.* at 33.
202. *See id.*
203. *Id.*

that "the nature and quantity of the information contained in people's telephony metadata" is "much greater" today than it was in 1979.[204] In other words, the resource had evolved in value; today, nearly every American has a cellphone, and those cellphones are used for so much more than just verbal communication, such as for taking photos, browsing the internet, or navigating a vehicle. Thus, the district court concluded that a warrantless search *had* occurred, and the burden shifted to the government to show a special-needs exception.[205] The court concluded that the government's interest did not outweigh the privacy invasion.[206] Judge Leon's opinion served as the strongest signal yet that individual metadata rights were on the brink of receiving constitutional protection. Judge Leon explained, "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval."[207] Continuing, he concluded:

> The Government, in its understandable zeal to protect our homeland, has crafted a counterterrorism program with respect to telephone metadata that strikes the balance based in large part on a thirty-four year old Supreme Court precedent, the relevance of which has been eclipsed by technological advances and a cell phone-centric lifestyle heretofore inconceivable.[208]

This quasi-victory for metadata was short-lived, as the government quickly appealed the decision to the D.C. Circuit Court of Appeals, which issued a per curiam opinion in 2015.[209] That opinion vacated the lower court's decision on the basis of insufficient standing, refusing to comment on the constitutional implications addressed by Judge Leon.[210] On remand, Klayman and co-plaintiffs struggled to establish the actual harm that Judge Leon had previously identified, and the suit was eventually dismissed.[211] *Klayman v. Obama* serves as an important case in the evolution of the protection of metadata because it signified that at least one federal court was finally willing to find that the broad and unwarranted government practice of collecting its citizens' metadata was unconstitutional under the Fourth Amendment. Despite later being overturned on jurisdictional grounds, the NSA's mass surveillance program finally received serious consideration as to the constitutional threat it poses.

The same year that *Klayman* was filed, the ACLU initiated a similar lawsuit in the U.S. District Court for the Southern District of New York against, among others, National Intelligence Director James Clapper and NSA

204. *See id.* at 34.
205. *Id.* at 37–39.
206. *Id.* at 43.
207. *Id.* at 42.
208. *Id.* at 43.
209. *See* Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).
210. *See id.* at 570.
211. *See* Klayman v. Nat'l Sec. Agency, 280 F. Supp. 3d 39, 42–43 (D.D.C. 2017).

Director Keith Alexander.[212] The ACLU claimed that the Government's practice of bulk data collection was an invasion of privacy and violated the Fourth Amendment.[213] Unsurprisingly, the claims of *Klayman* and *Clapper* were invigorated by the recent information disclosed by the Snowden leaks earlier that year.[214] The plaintiff in *ACLU v. Clapper* advanced claims that First Amendment rights were also being violated because, after recent news of the breadth of the government's collection program, cellphone users would likely become reluctant to communicate in fear that they were being recorded.[215]

At the trial court level, the ACLU unsuccessfully argued the merits of their case, and the district court held that phone users did not have a reasonable expectation of privacy in phone metadata.[216] Thus, no warrants were required for the government to engage in their collection program.[217] Like in *Klayman*, the district court in *Clapper* applied the *Smith* test, but came to a different result despite the thirty years of technological innovation between *Klayman* and *Smith*.[218] Unlike Judge Leon's finding in *Klayman* that specific examples of the program's benefits were lacking, the New York district court was persuaded by the NSA that numerous successes existed—for example, the identification of those involved in the New York City subway bombing and the New York Stock Exchange bombing plot.[219] Ultimately, the court found no constitutional violation.[220] The ACLU then appealed its case to the Second Circuit.[221]

On appeal in 2015, the Second Circuit held that the government's bulk collection program violated the authority conferred by Congress in the Patriot Act.[222] Thus, the majority of the NSA's more than ten-year-old surveillance program was illegal. This ruling, however, left several commentators unsatisfied, as the Second Circuit limited its holding to invalidation based on statutory considerations instead of more permanent and concrete constitutional considerations.[223] The court analogized the powers of a grand jury to those intended to be conferred by Congress in the Patriot Act.[224] Even with the extensive power provided to a grand jury to issue a subpoena,

212. Am. Civ. Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part*, *vacated in part*, *remanded*, 785 F.3d 787 (2d Cir. 2015).
213. *Id.* at 735.
214. *See generally id.* at 730.
215. *See id.* at 753–54.
216. *See id.* at 752.
217. *See id.*
218. *See id.* at 749–50.
219. *See id.* at 755; *see generally* Spencer Ackerman, *NSA Chief Claims "Focused" Surveillance Disrupted More Than 50 Terror Plots*, The Guardian (June 19, 2013), https://www.theguardian.com/world/2013/jun/18/nsa-surveillance-limited-focused-hearing [https://perma.cc/RQX2-UHR4].
220. *Clapper*, 959 F. Supp. 2d at 749–54.
221. Am. Civ. Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015).
222. *Id.* at 821 (holding "that the text of § 215 cannot bear the weight the government asks [the court] to assign to it, and that it does not authorize the telephone metadata program").
223. *See id.* at 826; *see, e.g.*, David A. Graham, *Does the PATRIOT Act Allow Bulk Surveillance?*, The Atlantic (May 7, 2015), https://www.theatlantic.com/politics/archive/2015/05/does-the-patriot-act-allow-bulk-surveillance/392651 [https://perma.cc/H3TL-6R8Y].
224. *See id.* at 811.

the grand jury nonetheless requires probable cause and is limited within reason.[225] Therefore, "bulk collection" by its own terms was insufficiently tailored to the purposes authorized by Congress.

In his concurrence, Judge Sack emphasized the balance the government must find between individual privacy and national security.[226] That same balance was addressed less than a month later, not by a court, but instead by Congress through the passage of the USA Freedom Act.[227] In what was effectively an amendment to the Patriot Act, the USA Freedom Act sought to avoid many of the pitfalls that the Second Circuit highlighted in *Clapper*, specifically that the program was far too broad.[228] In *Clapper*, the court held that collection was only proper insofar as it was "relevant to an authorized investigation."[229] If not relevant to an actual investigation, then the NSA had no reason to be collecting that information without a warrant, something Judge Leon might classify as "arbitrary" surveillance.[230]

The "split" between the D.C. Circuit and the Second Circuit mostly focused on whether plaintiffs had standing to challenge the NSA's program. The real significance of the *Klayman-Clapper* circuit split, however, was that it left open the question: Should the Fourth Amendment protect individual metadata from these mass surveillance and collection programs? The district court in *Klayman* was more direct on this issue (despite eventual overturning on procedural grounds) and actually analyzed the Fourth Amendment claim.[231] On the other hand, the Second Circuit in *Clapper* avoided the constitutional analysis[232] but interestingly noted that a "Fourth Amendment claim, in particular, presents potentially vexing issues."[233]

The *Klayman-Clapper* circuit split reignited the discussion concerning metadata and its potential for constitutional protection. In both cases, the government relied significantly upon the third-party doctrine to explain that when a third-party cellphone carrier or internet service provider is involved, reasonable expectations of privacy are weakened.[234] Following the application of this doctrine, the *Smith* test for determining privacy expectations was frustrated, making it more difficult to reach plaintiffs'

225. *A Brief Description of the Federal Criminal Justice Process*, FBI, https://www.fbi.gov/how-we-can-help-you/victim-services/a-brief-description-of-the-federal-criminal-justice-process [https://perma.cc/X2GU-R95B] ("If the grand jury concludes that there is probable cause to believe that a particular individual committed a crime, the grand jury will issue a charging document known as an indictment.").

226. *See id.* at 832 (Sack, J., concurring).

227. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

228. *See generally id.*; *Clapper*, 785 F.3d at 810–21.

229. *Clapper*, 785 F.3d at 818–19.

230. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam) ("I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data . . . .").

231. *See id.* at 37.

232. *Clapper*, 785 F.3d. at 824 ("Because we conclude that the challenged program was not authorized by the staute on which the government bases its claim of legal authority, we ned not and do not reach these weighty constitutional issues.").

233. *Id.* at 821.

234. *See* Meyer, *supra* note 184.

constitutional claims.[235] However, as commentators have noted, the third-party doctrine is "an increasingly disfavored and anachronistic legal rule," suggesting that the increased prevalence of mobile electronics may require us to change the way we calculate expected privacy.[236] As discussed in the following Section, although not framed as a challenge to the USA Freedom Act, the Supreme Court did eventually rule on a related issue pertaining to the bulk collection of individual metadata.

C. *Carpenter v. United States*

In 2018, the Supreme Court readdressed the government's practice of compelling the production of metadata from wireless service providers without a warrant in *Carpenter v. United States*.[237] In this decision, despite lacking probable cause, police officers obtained a court order under the Stored Communications Act to access the stored cell-site location information of Timothy Carpenter because he was named by other suspects who had been arrested for involvement in robberies.[238] The records pinpointed where Carpenter's cell phone had pinged different cell towers, informing law enforcement where the phone was for the four-month period during the robberies.[239] The metadata at issue had electronically stored Carpenter's location around 100 times per day.[240] The Court, with Chief Justice Roberts writing, explained just how personal this cell site data was, and took issue with reconciling the lack of protection, noting that "[c]ell phones continuously scan their environment . . . . Most modern devices, such as smartphones, tap into the wireless network several times a minute . . . even if the owner is not using one of the phone's features."[241]

Carpenter attempted to suppress the metadata as being improperly obtained on the grounds that the government violated the Fourth Amendment by seizing the records without a warrant supported by probable cause.[242] However, the district court denied Carpenter's motion to suppress. Carpenter eventually appealed the case to the Sixth Circuit.[243] Similarly, the Sixth Circuit affirmed the denial of the motion to suppress the cell-site location evidence on the grounds that Carpenter lacked a reasonable expectation of privacy, thus failing the *Smith* test to determine whether a Fourth Amendment search in fact occurred.[244] The Supreme Court eventually granted certiorari to resolve this contentious question of constitutional protection.[245]

In resolving the question of whether an individual has a reasonable expectation of privacy in certain types of metadata, despite requiring a third-party

235. *See id.*
236. *See id.*
237. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
238. *See id.* at 2212.
239. *Id.*
240. *Id.* (finding collection of "an average of 101 data points per day").
241. *Id.* at 2211.
242. *Id*. at 2212.
243. *See id.* at 2213.
244. *Id.*
245. *See id.*

service provider to use the technology, the Supreme Court found that such an expectation was reasonable, and therefore, the government's use of the metadata equated to a search under the Fourth Amendment.[246] Finally, nearly forty years after the *Smith* decision, the Supreme Court recognized that changes in circumstances, both technological and societal, require that metadata be understood as a valuable resource to be protected under the Fourth Amendment. In this case, after finding that a search had occurred, the Court also stated that "the Government must generally obtain a warrant supported by probable cause before acquiring [telephone metadata] records."[247] This statement was probably intended to remind the Government that the special-needs exception might potentially excuse certain warrantless searches, for example, in the case of identified terrorism; however, the spirit of the Court's opinion more closely tracked Judge Leon's holding in his original *Klayman* decision. That holding found that common, non-terroristic criminal suspicion is not a sufficient special need to outweigh a privacy right that is becoming more and more valuable each day.[248]

In what effectively served as a nail in the coffin to the third-party doctrine as it pertains to metadata, the Court declined to extend the reasoning from prior decisions in *Smith* and *Miller*, which prevented a court from finding a reasonable expectation of privacy in information that was shared with a third party.[249] In his modern understanding of the issue, Chief Justice Roberts wrote, "Cell phone location information is not truly 'shared' as one normally understands the term."[250] Therefore, the reasoning underlying the third-party doctrine was inapplicable in the modern context.[251] Cell phones, the Chief Justice explained, have become "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[252] In combination with the finding that no active part, other than turning the phone on, was required by the user to be tracked to the same degree as Carpenter, Chief Justice Roberts concluded that this was surely an unconstitutional invasion of privacy if the government could access such data without respecting constitutional safeguards.[253]

The *Carpenter* opinion, like those before it, was relatively limited in its holding. "[O]ur opinion does not consider other collection techniques involving foreign affairs or national security."[254] Nonetheless, it would be difficult not to apply similar reasoning to the government's collection practices discussed within this Comment and currently authorized by the USA Freedom Act. Although not the same kind of "bulk" collection as

246. *See id.* at 2223.
247. *Id.* at 2221.
248. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 38–39 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).
249. *See Carpenter*, 138 S. Ct. at 2217.
250. *Id.* at 2220.
251. *See id.*
252. *Id.* (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)).
253. *See id.* at 2223–24.
254. *Id.* at 2220.

was permitted under the Patriot Act, the current program's broad statutory authorization raises clear constitutional concerns. In an effort to heed Justice Frankfurter's warning, the *Carpenter* Court noted the need to "tread carefully" in this area of new innovation.[255] Justice Frankfurter's advice should properly be understood to counsel against the Court interfering with policy in areas where it is unequipped to do so. But, as discussed earlier, this reasoning also supports the application of the Rule of Capture.[256] Thus, just as significant regulation and protection have "carefully" followed Justice Frankfurter's warning in the context of airplanes and radios, so too has it followed in the area of metadata.[257]

Although intentionally limited in scope, the *Carpenter* opinion signaled the downfall of the third-party doctrine and the rise of constitutional protection for metadata. Following the lead of previously discussed resources, this means that the courts are finally prepared to establish a more nuanced scheme of protection, moving away from the reasoning that has resembled the Rule of Capture.[258] It is important to recognize, however, that metadata, as a concept, remains relatively novel. Especially given the qualities of the resources discussed above, intangibility, for example, is likely to lessen the court's confidence in understanding and properly protecting individual ownership rights to metadata.[259] Regardless, groundbreaking opinions like *Smith*, *Clapper*, Judge Leon's holdings in *Klayman*, and especially the most recent decision in *Carpenter*, signal that the judiciary is prepared to evaluate and classify metadata in terms of the Constitution rather than freely allow for its capture, mostly due to its recent increases in value, prevalence, and function in modern, everyday life. And these increases show no sign of slowing down, suggesting that soon, as metadata grows more and more personal, the Court will eventually protect all forms of metadata from involuntary bulk collection, despite the involvement of a third party, under the Fourth Amendment of the Constitution. "There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[260]

V. COUNTERARGUMENT

Now, in an effort to support the prediction that the law will continue to recognize an individual constitutional right to the protection of metadata, grounded in the Fourth Amendment, this Comment addresses an article written by Professor Ari Ezra Waldman titled *Privacy's Rights Trap*.[261] In the article, Waldman "warns against relying on individual rights to protect

255. *See id.*
256. *See supra* Part III.
257. *See* Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944).
258. *See supra* Part III.
259. *See supra* Part III.
260. *Carpenter*, 138 S. Ct. at 2219.
261. Ari Ezra Waldman, *Privacy's Rights Trap*, 117 Nw. L. Rev. Online 88 (2022).

privacy" for a variety of reasons.[262] This Comment briefly addresses some of Waldman's five critiques of the individual rights method of protection and attempts to reconcile his concerns with the historical practice of courts applying the Rule of Capture to novel and fugacious resources. It should be noted that Waldman's argument seems to pertain to data more generally, whereas this Comment focuses on metadata. Nonetheless, assuming his argument applies equally to "data about data," especially in the context of what Waldman calls "informational capitalism,"[263] the perspective offered in the previous Sections of this Comment aims to reconcile Waldman's concerns regarding privacy protection grounded in individual constitutional rights.

If Professor Waldman and this Comment agree on one thing, it is certainly that in this modern age, technological developments are occurring exponentially faster than legal developments to protect the individuals involved in the same developments.[264] Where we disagree, however, is what method best ensures that those legal developments are equipped to keep pace with technology. While this Comment suggests that leading with individual rights, as the Court has shown an inclination to do, can successfully balance privacy with government and tech companies' inclination towards informational capitalism, Waldman believes that individual rights of control are ineffective at regulating a data-extractive economy.[265] Waldman argues that individual rights often "crowd out" necessary reform and have immunized large technology companies from being held accountable.[266] In response, this Comment attempts to explain Waldman's dissatisfaction as the product of judicial restraint and the Rule of Capture, eventually showing that such restraint is no longer necessary and that the recognition of individual rights to metadata privacy is the correct approach to balancing large-scale data collection and the rights of everyday citizens.

Waldman criticizes the first and second waves of privacy, for example, explaining that although the first wave is often described as providing notice and choice to technology users, "[i]n practice, notice and choice provides neither notice or choice."[267] Professor Waldman's skepticism of past regulations is reasonable. In fact, the same skepticism could have been raised, for example, in the legal field of oil and gas prior to a departure from the Rule of Capture. Waldman's focus on regulations that were passed years, if not decades, before decisions like *Carpenter*, however, fails to acknowledge the change in circumstances that Chief Justice Roberts pointed out in *Carpenter*.[268] The author's claim that "[i]ndividual rights cannot place limits on technology companies when the law has already immunized their

262. *Id.* at 106.
263. *Id.* at 88.
264. *See id.* at 89.
265. *See id.* at 88.
266. *See id.* at 91 ("When rights go first, they almost always crowd out rather than pave the way for real reform.").
267. *Id.* at 91–92.
268. *Compare id.* at 92, *with* Carptenter v. United States, 138 S. Ct. 2206, 2220 (2018).

business models from accountability"[269] focuses retrospectively on previous courts' application of the Rule of Capture rather than acknowledging the shift in judicial recognition of individual privacy rights. Now that courts appear more comfortable to prescribe a detailed scheme of protection, what may previously have been perceived as immunity for data collectors will surely be subject to more detailed and stringent regulation demanded by the Constitution. Regardless of the capitalist-based desire for large companies to collect as much data on their users as legally possible, these same companies—and governments, as is much the focus of this Comment—may no longer "define the practical reach of the law."[270] In the case that they attempt to, courts now, after forty years, have stable Supreme Court precedent to see through such attempts to functionally, although not formally, violate individual rights. The best example comes from the *Carpenter* decision, where Chief Justice Roberts declined to extend the third-party doctrine to metadata, finding that although the user technically had consented to "share" their data with their service provider, such an assumption of risk was not voluntary in any meaningful sense.[271]

Therefore, while Professor Waldman's disappointment in prior waves of data privacy law is understandable—after all, who among us reads the terms and conditions of agreements we often enter—the unavoidable trend towards increased judicial protection of individual rights and away from the Rule of Capture will properly balance the economic interests of tech companies and the privacy of individuals while paving the way for a more nuanced scheme of regulation in the legislature. At the end of the day, the protection of a right as critical—and now personal—as that of data privacy, must be administered by the Court, especially given the demands of the Fourth Amendment. To do this, individual privacy rights must be declared as grounded in the Constitution, and then later regulations may be properly analyzed, for example, the need for "visibility" or "choice" for their functional abilities to secure those rights.[272]

Now, this Comment will address three of the five critiques that it considers to be the strongest arguments presented by Waldman against recognizing individual privacy rights, at least prior to implementing more effective regulations on informational capitalism. The three specific critiques addressed are referred to as: the social critique, the practical critique, and finally, the structural critique.[273]

First, Waldman presents a social critique of the recognition of individual privacy rights.[274] He explains that because the informational economy is necessarily a social economy, "[d]ecisions to consent to data collection are

269. *See* Waldman, *supra* note 261, at 88.
270. *See id.*
271. *See Carpenter*, 138 S. Ct. at 2220.
272. Waldman, *supra* note 261, at 90 ("Rights, like visibility, are traps."). This is the same way Roberts was able to analyze the need for *consent* in terms of shared data in *Carpenter*. *Carpenter*, 138 S. Ct. at 2210 ("Cell phone location information is not truly 'shared' as the term is normally understood.").
273. *See* Waldman, *supra* note 261, at 93–94, 96–98, 102–03.
274. *See id.* at 93–94.

never purely personal decisions."[275] Indeed, this critique tracks the same issues this Comment has highlighted with the government's "amended" data collection practices, authorized under the USA Freedom Act.[276] Under those practices, one constitutionally proper search may lead to the recovery of the metadata of hundreds, if not thousands, of other individuals despite having a far more attenuated connection to the suspicion that initially authorized the search. Therefore, this Comment agrees with Waldman that a more comprehensive scheme of protection is required.[277] Individual rights are the proper "first step" in establishing this scheme; however, without grounding in an individual constitutional right, policymakers would struggle to provide the radical protections that Waldman suggests are necessary, especially when faced with massive, multi-national tech companies lobbying against more comprehensive protections. The harms that Waldman describes can be analogized to the issue of drainage in the oil and gas context.[278] Now that data, particularly metadata, is better understood, regulations and legal concepts such as the implied covenant against drainage can be crafted to fix these adjacent concerns outside of the direct relationship between the creator of the data and its processor.

Next, Waldman explains his practical critique of individual privacy rights.[279] And again, Waldman and I agree that simply recognizing an individual right will not provide the protection required here.[280] Nonetheless, this Comment suggests that it is the right place to start. Waldman suggests that individual "rights only have real power with structural reform."[281] Again, I agree! I am, however, skeptical that any structural reform could truly precede the recognition of those individual rights, especially in the case that this Comment focuses on—metadata, in light of the Rule of Capture. I imagine little, if any, "structural reform" occurred in regard to one's Fourth Amendment rights in areas like water or oil prior to departure from an analysis based on the Rule of Capture. My point is this—in order for structural reform to take place, the Court should first recognize the individual right to privacy so that its true value can be weighed against competing considerations.

Waldman continues to suggest that "U.S. courts have been notoriously and consistently unwilling to recognize anything but the most obvious pecuniary harms in privacy cases,"[282] however, as this Comment closely analyzes, this is simply not the case. The opinions discussed previously indicate a gradual recognition of various non-pecuniary harms.[283] Specifically, metadata, which was once considered to be virtually useless, received

275. *Id.* at 93.
276. *See supra* Part II.
277. *See* Waldman, *supra* note 261, at 94.
278. *See generally id.*; SCHLUMBERGER, *supra* note 3.
279. Waldman, *supra* note 261, at 96–98.
280. *See id.* at 97.
281. *Id.* at 91.
282. *Id.* at 98.
283. *See supra* Part IV.

recognition as being a valuable form of property just four years ago.[284] Furthermore, the same discussions, signaling a decline in the third-party doctrine, should alleviate Professor Waldman's concerns regarding the issue of individual plaintiffs having standing to vindicate privacy violations.[285] It is true that "[c]ourts *could* recognize those harms,"[286] and as they become more comfortable in the new age of data privacy, they will recognize them; in fact, they have already have begun to.

Finally, this Comment addresses Professor Waldman's structural critique, in which he argues that "individual rights have always been a convenient yet ineffective quarter-baked solution to throw at a structural problem."[287] By analogizing individual rights of control (or more generally, a right to privacy) to the right to counsel, Waldman, citing Paul Butler, suggests that recognizing an individual right could actually legitimize a broken system and diffuse political resistance.[288] He continues to explain that individual privacy rights may provide "a fairer process," but they ultimately would make "it harder for social movements to argue that the system was broken."[289] In response, this Comment counters that, understood through the Rule of Capture framework, even if individual rights are a "convenient" option for the court, the last forty years have been characterized by judicial restraint in that area, specifically towards metadata, given the novelty of the resource. Just as the author of the counterargument seems to favor, regulation has been left to the legislature up until recently.[290] The result of not leading with individual right recognition, however, is unavoidable; for example, take the passage of the Patriot Act. Without being able to refer to concrete individual rights, Congress will continue to push the limits of data collection, just as bulk collection programs in the past have done. Now that courts have shown evidence that they are prepared to declare individual rights to data privacy, they can begin to do so, while simultaneously providing proper direction for Congress to address the nuanced details. Moreover, those details will receive heightened constitutional scrutiny from the courts to prevent the individual rights, which serve as the basis for these protective schemes, from being trampled over, as they have been in the past.

In conclusion, Waldman offers a thought-provoking alternative to the reconigion of individual rights, which he considers the "classic liberal responses to social problems."[291] However, this Comment disagrees that the individual "rights model is a gift to the information industry,"[292] instead

284. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).
285. *See* Waldman, *supra* note 261, at 97–98.
286. *Id.* at 98 (emphasis in original).
287. *Id.* at 91; *see also id.* at 102–03.
288. *See id.* at 102; Paul D. Butler, *Poor People Lose:* Gideon *and the Critique of Rights*, 122 Yale L.J. 2176, 2178–79 (2013).
289. *See* Waldman, *supra* note 261, at 102.
290. For example, the Patriot Act. *See supra* Part II.
291. *See* Waldman, *supra* note 261, at 102.
292. *Id.* at 106.

suggesting that it is the proper first step in achieving the same goal that Waldman and this Comment agree upon: protecting citizens' data privacy. Just like Waldman explains, I believe individual rights to be "a critical piece of a larger regulatory structure"; if anything, they are the proper foundation.[293] On the other hand, he suggests that recognizing these rights merely impedes more effective options.[294] When approached from an understanding of how the Rule of Capture has impeded these protections in the area of data privacy up until this point, however, I believe that many of his critiques towards recognition of an individual, constitutional right to data privacy can be reconciled. It is true that mere recognition of a right will do little to hold powerful corporate violators accountable; however, the only way to effectively begin to do so, in my view, is to first ground that interest—in individual data privacy—in the single text which defines the fundamental laws of this country.

VI. CONCLUSION

> Most people, even today, tend to think of mass surveillance in terms of content—the actual words they use when they make a phone call or write an email . . . . The unfortunate truth, however, is that the content of our communications is rarely as revealing as its other elements—the unwritten, unspoken information that can expose the broader context and patterns of behavior.[295]

Since the founding of this country, its law has continued to evolve. Unique to the United States' legal system is an emphasis on judicial restraint. When considering the treatment of metadata by American courts over the last several decades, I believe that the lack of complex protection schemes was no accident, rather, it was a reasoned form of judicial restraint. Specifically, over the last several decades, the judiciary has encountered a new resource with exponentially increasing value. To make classification more difficult, the resource is both invisible and intangible. Because of these two key features, courts have properly applied the Rule of Capture to metadata, just as if it were an oil reservoir, a fox, or even a water well. In doing so, they have avoided judicial overreach and allowed the courts—and society for that matter—to develop a better understanding of metadata, its value, its implications, and its relation to its creators.

Nonetheless, after so many years, the time arrives when judges can finally feel confident in their classification, analysis, and subsequent protection of the technological resource. That time is approaching and is closer than it has ever been. Landmark decisions in privacy jurisprudence such as *Klayman*, *Clapper*, and *Carpenter* signal that the judiciary is ready to protect the relationship between an individual and the metadata they produce, particularly through the Fourth Amendment of the Constitution.

---

293. *See id.*
294. *See id.*
295. Edward Snowden, Permanent Record 178–79 (2019).

Despite suggestions by commentators that individual rights are not the correct approach, previous statutory schemes of protection have come and gone, failing in their efforts to constantly update their provisions to adapt to the rapidly changing technological environment. Instead, humans—particularly judges in their application of the Fourth Amendment—should be the ones to properly gauge our society's ever-developing expectations of privacy.