Wire(less) Tapping: Protecting Arkansans' Fourth Amendment Right in the Era of the Cloud

Erin James
University of Arkansas, Fayetteville

Follow this and additional works at: https://scholarworks.uark.edu/alr

Part of the Constitutional Law Commons, Fourth Amendment Commons, Jurisprudence Commons, Privacy Law Commons, Property Law and Real Estate Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://scholarworks.uark.edu/alr/vol72/iss4/4

This Article is brought to you for free and open access by ScholarWorks@UARK. It has been accepted for inclusion in Arkansas Law Review by an authorized editor of ScholarWorks@UARK. For more information, please contact ccmiddle@uark.edu.
Every day we surround ourselves with dozens of devices that monitor our every move, every request, all connecting with one another and sending massive amounts of data back to the device manufacturers. The idea of the prosecution placing the little black cylinder of your Amazon Alexa on the witness stand and asking Alexa to testify against you seems like something pulled from an Orwellian nightmare. But, in reality, it is already occurring.

This futuristic idea originated from a case in our backyard—State v. Bates1—involving the murder trial of a Bentonville, Arkansas, resident.2 After a football watch party went wrong, one of Bates’s guests turned up dead in Bates’s hot tub.3 Bates said he went to bed around one in the morning, but a witness came forward claiming he heard music playing during the time Bates alleged he was asleep.4 This prompted investigators to subpoena tech giant, Amazon, for the transcripts of Bates’s Amazon Alexa to see if the device played music or if Bates gave a command during this time period.5 This case took

* University of Arkansas School of Law J.D. Candidate 2020. The author would like to thank Professor Brian Gallini for inspiring the topic of this article and his continued guidance and feedback throughout the drafting process. The author would also like to thank Brandon Chapman, an Arkansas Law Review Note & Comment Editor, for devoting time to provide many suggestions on this article.

2. Id.
3. Id.
5. Id.
the national spotlight and prompted Amazon to write a brief requesting, on First Amendment grounds, that the court quash the search warrant for Bates’s Amazon Alexa. Bates eventually conceded and turned the information over.

Alexa may have been the star that caught the Nation’s attention, but this case illustrated much broader implications. Investigators found evidence on the deck near the hot tub showing signs of a struggle. Bates’s water company used smart water meters to keep track of water consumption. The police subpoenaed these records and found that between 1 a.m.—when Bates claimed he was asleep—and 3 a.m., 140 gallons of water were used. Investigators questioned whether this quantity of water could have been used to wash away blood or other evidence during clean up.

This case was one of the first showing the potential legal battles that have begun to emerge as we continue to implement smart home devices into our daily lives and homes. With various smart home devices and other interconnected devices ever increasing in options and quantities sold, our privacy rights are more at stake now than ever. Every day, more applications and functions are added to our arsenal of technology. These rapid improvements generate even more unique and invasive data on their users.

Though the Fourth Amendment protects citizens’ “right . . . to be secure in their persons, houses, papers, and effects, against

---

6. Nat Levy, Amazon Hands over Alexa Data in Arkansas Hot Tub Murder Case, but 1st Amendment Questions Remain, GEEKWIRE (March 7, 2017), [https://perma.cc/4AEY-GJQQ]. While some scholars believe the First Amendment will create standing, I argue that the Fourth Amendment would provide more comprehensive coverage to data from all smart devices.
7. Id.
9. Dwyer, supra note 1; Josh Hart, Smart Meter Data at Crux of Arkansas Murder Case, STOP SMART METERS! (Aug. 26, 2016), [https://perma.cc/DPN3-S24N].
11. Id.
unreasonable searches and seizures,"¹⁴ the third-party doctrine allows for warrantless searches and seizures of information voluntarily turned over to third parties.¹⁵ As the law currently stands, the third-party doctrine proceeds virtually unchecked for data gathered from smart devices as the devices require users to share data with technology companies, service providers, and other devices.¹⁶ This allows law enforcement to gain access to massive amounts of users’ data—data that gives a comprehensive look into a user’s life.¹⁷ It is time to retire the doctrine and create a workable doctrine to give citizens increased protection. This Article argues that a return to a property-based analysis of the Fourth Amendment, with the states playing a stronger role, would result in a more workable and straightforward approach.

Part I provides an overview of two categories of technology—personal devices and smart home devices—that have become woven into society and will continue to grow more pervasive. This Part will briefly explain how these technologies work, as it is imperative to understand the inner workings and how they will relate to the current law. Part II looks at the development of the Fourth Amendment with a particular focus on the recent Supreme Court case, Carpenter v. United States.¹⁸ This Part illustrates how the Supreme Court has shaped the Fourth Amendment jurisprudence in light of advancing technology. Part III argues that states may now be better-situated to make key changes in the Fourth Amendment realm while presenting evidence that Arkansas is open to differentiating the state Fourth Amendment doctrine from the federal Fourth Amendment doctrine. Finally, Part IV argues that a flexible framework largely based on property principles that would provide Arkansas citizens more Fourth Amendment protections as technology continues to advance.

¹⁴. U.S. CONST. amend. IV.
¹⁷. See id.
I. THE EXPANSIVE DATA GATHERED BY CURRENT TECHNOLOGY

Today, the tech industry in America is a multi-trillion dollar per year industry, with the top five technology companies collectively worth $2.9 trillion.\textsuperscript{19} Though technology develops at an exponential rate, the law is several steps behind. Once a case’s final opinion is published, the law can border on obsolescence. Consider Carpenter, which began in the Eastern District of Michigan in 2013 and finally reached a decision in the Supreme Court in 2018.\textsuperscript{20} By this time, other new and more problematic (at least in terms of the Fourth Amendment) technology had surpassed the main concern of the case, which was cell phone location data.\textsuperscript{21}

A. The Cloud and Internet of Things

Understanding cloud storage (the Cloud)\textsuperscript{22} is essential to understanding the Fourth Amendment issues that current technology evokes. The Cloud runs on the internet and consists of both storage and software.\textsuperscript{23} Cloud storage allows people to upload—periodically or constantly, on command or automatically—various types of data to a remote server.\textsuperscript{24} The user can then access his or her data anywhere and potentially on any device.\textsuperscript{25}

Each smartphone producer and tech giant has its own unique cloud available for both personal and business use. A user can rely on the cloud to backup files for safe keeping,

\textsuperscript{19} Jeff Desjardins, Chart: Here’s How 5 Tech Giants Make Their Billions, VISUAL CAPITALIST (May 12, 2017), [https://perma.cc/9DTC-9V2L].
\textsuperscript{21} Michael Caccavale, The Impact of the Digital Resolution on the Smart Home Industry, FORBES (Sept. 24, 2018), [https://perma.cc/YKK2-FX5W]. Consumers now have a plethora of smart home devices that monitor and share the details of what goes on inside of a home. When viewed together, these devices can give law enforcement a comprehensive look into the intimate activities of the home and its residents.
\textsuperscript{22} What Is the Cloud?, GCF GLOBAL, [https://perma.cc/7UQA-E8SQ] (last visited Oct. 16, 2019).
\textsuperscript{23} Id.
\textsuperscript{24} Id.
\textsuperscript{25} Anuj Gupta, Understanding Cloud Computing, HUFFPOST (Dec. 6, 2017), [https://perma.cc/3UNJ-8YE7]. Common cloud platforms include Microsoft’s Office Online, Google Drive, Apple’s iCloud, Amazon Cloud Drive, and Dropbox. Id.
extend the storage capacity of their device, or work on a variety of documents from different devices. Take Apple’s iCloud for example. Each Apple device owner gets five gigabytes of space on the iCloud for free and can purchase up to two terabytes of space. The iCloud allows each device owner to store data and documents on the Cloud and sync the information to the owner’s other Apple devices.

The Cloud has contributed to the “Internet of Things.” The Internet of Things involves multiple devices connecting via a wireless network and exchanging information with one another. This allows information on the Cloud to sync with multiple devices and provide users with a seamless interaction between devices. Because this information is stored on a server owned by someone else, the government must request the information from the company or owner of the storage.

B. Devices and Their Features

The plethora of smart devices that gather our personal data every day creates privacy concerns. Most of these devices communicate with one another on the Cloud, thus creating even more legal issues regarding ownership and the third-party doctrine.

In 2017 alone, approximately 1.54 billion smartphones were sold worldwide. Most major tech companies have some version of a smartphone on the market. Apple dominates the market with the iPhone, Samsung’s Galaxy is another popular

---

27. Id.
28. Id.
30. Jacob Morgan, A Simple Explanation of The Internet of Things,’ FORBES (May 13, 2014), [https://perma.cc/JGN6-THPA].
31. iCloud, supra note 26.
32. See U.S. GOV’T ACCOUNTABILITY OFF., GAO-17-75, INTERNET OF THINGS 11, 28-32 (2017). Compare to information that is stored on the device itself. In that case, the government would have to obtain the device/information from the device owner. This may mean that the Fifth Amendment, self-incrimination provision could potentially kick in.
33. See id.
34. Arne Holst, Number of Smartphones Sold to End Users Worldwide from 2007 to 2020 (in Million Units), STATISTA, [https://perma.cc/56HG-B3C8] (last updated Aug. 30, 2019).
choice, and Google is entering the market with its Pixel.\textsuperscript{35} These smartphones hold mass amounts of data. The new iPhone Xs offers a storage option of a massive 512 gigabytes,\textsuperscript{36} though many smartphone users will never pass the 40-gigabyte capacity.\textsuperscript{37} With large capacities, these phones can hold thousands of personal photos, videos, notes, text messages, apps, and other documents.\textsuperscript{38}

With the release of new phones comes the release of new technology that generates new types of data. This data provides key insights into our lives and reduces our privacy. For example, the iPhone contains a Find My Friends feature that tracks a user’s location.\textsuperscript{39} Siri keeps track of a user’s voice commands.\textsuperscript{40} Apple Wallet stores a user’s debit and credit cards along with various tickets the user has linked.\textsuperscript{41} Apple Wallet allows a user to use the phone to pay at businesses that accept Apple Pay.\textsuperscript{42} Apple has used biometrics for security since the introduction of Touch ID.\textsuperscript{43} Recently, Apple unveiled Face ID as part of its iPhone X, which relies on facial recognition to unlock a user’s phone and gain access to both apps and Apple Pay.\textsuperscript{44}

\textsuperscript{35} See Robert Triggs, 5 Best Selling Smartphones of All Time, ANDROID AUTHORITY (Aug. 5, 2018), [https://perma.cc/5FMF-83Z6]; Joe Maring, Google Pixel Is Now the United States’ Fastest-Growing Smartphone Brand [Update], ANDROIDCENTRAL (Feb. 12, 2019), [https://perma.cc/6FFU-VRA3].

\textsuperscript{36} iPhone Compare, APPLE, [https://perma.cc/KJJ3-2LWJ] (last visited Oct. 4, 2019).

\textsuperscript{37} See Andrew Martonik Let’s Be Honest, 64GB of Internal Storage is Plenty in 2018, ANDROIDCENTRAL (Feb. 2, 2018), [https://perma.cc/83T2-BJXE].

\textsuperscript{38} iCloud, supra note 26.


\textsuperscript{40} See Siri, APPLE, [https://perma.cc/M35P-65JC] (last visited Oct. 4, 2019).

\textsuperscript{41} Use Wallet on Your iPhone or iPod Touch, APPLE SUPPORT, [https://perma.cc/Z6EM-7ZJB] (last visited Oct. 4, 2019).

\textsuperscript{42} Id.

\textsuperscript{43} Touch ID uses capacitive touch to take high-resolution images of your fingerprint and creates a mathematical representation of your print. About Touch ID Advanced Security Technology, APPLE SUPPORT (Sept. 11, 2017), [https://perma.cc/9SK6-PA3K]. It then cross references this to the fingerprint you register. Id. Only the mathematical representation is stored and all fingerprint data is encrypted. Id.

\textsuperscript{44} “Face ID provides intuitive and secure authentication enabled by the state-of-the-art TrueDepth camera system with advanced technologies to accurately map the geometry of your face. With a simple glance, Face ID securely unlocks your iPhone or iPad Pro.” About Face ID Advanced Technology, supra note 43. Face ID data is encrypted, stays on your device, and is never backed up to iCloud. Id.
Additionally, there are many different smart watches that connect to these smart phones. In 2018, wearables, such as smart watches and fitness trackers, were expected to gross $6.4 billion with a projected growth of 10% from 2017.\textsuperscript{45} Smart watches connect with smart phones, share information with the phone, and allow the wearer to access most applications, functions, and notifications from the phone.\textsuperscript{46} Some watches are able to generate their own data, including personal health data.\textsuperscript{47}

While the tech giants create the devices, third-party developers are responsible for creating the millions of applications users can download. As of the second quarter of 2019, there are over 2.46 million apps to choose from in the Google Play online store and almost 1.9 million in the Apple Store.\textsuperscript{48} Apps may access a variety of personal data from a user’s phone, including contacts and location.\textsuperscript{49} Depending on the app, the user may be able to choose how much data to share with the app.\textsuperscript{50} The app often sends this data back to the developer for storage and review.\textsuperscript{51}

Smart home devices—including smart speakers—have increased in popularity and accessibility in recent years. While smart speakers were expected to bring in only $3.2 billion in revenue for 2018, that was a projected increase of 64% from 2017.\textsuperscript{52} Google and Amazon are leading the way with their smart speakers.\textsuperscript{53} These speakers go inside homes or businesses and connect with many different devices. As of October 2019, Google offers five types of these devices—Nest Hub, Nest Hub

\textsuperscript{45} Wood, supra note 12.  
\textsuperscript{46} Apple Watch Series 5, APPLE, [https://perma.cc/X5P2-YURP] (last visited Oct. 4, 2019).  
\textsuperscript{47} Fitbit trackers are equipped with heart rate, activity, and sleep tracking. Our Technology, FITBIT, [https://perma.cc/ST5K-EUAH] (last visited Oct. 4, 2019).  
\textsuperscript{49} About Privacy and Location Services in iOS 8 and Later, APPLE SUPPORT (Sept. 2, 2019), [https://perma.cc/ML34-8FN6].  
\textsuperscript{50} Id.  
\textsuperscript{52} Wood, supra note 12.  
\textsuperscript{53} Erika Rawes, Google Home vs. Amazon Echo, DIGITAL TRENDS (Sept. 30, 2019), [https://perma.cc/REZ3-8FC6].
Max, Home Mini, Home, and Home Max. Each of these devices vary in size, with the Home Hub including a display screen. These devices utilize Google Assistant to listen and respond to voice commands via a Wi-Fi connection. The Google Home App allows you to control and manage all of your devices. This includes allowing you to add or remove third-party services and view or delete commands. According to Google, their Home devices work with a variety of applications and technologies for entertainment, energy efficiency, and security purposes. This includes connecting with televisions, appliances, plug-ins, lights, thermostats, and many other devices.

Similarly, Amazon produces the Amazon Echo in several models. The Echo and Echo Dot are classic speakers, while the Echo Show and Echo Spot include a display. These devices are controlled by Amazon Alexa, a virtual assistant that functions like Google Assistant. Alexa works by constantly listening for her “wake word” which initiates a response to subsequent commands. Amazon also has an Alexa app that allows you to manage your settings and review or delete previous commands. Alexa works with a variety of devices,

55. See supra note 54 (detailing the different sizes of devices and features).
60. Id.
63. Alexa and Alexa Device FAQs, AMAZON, [https://perma.cc/W46A-U8L9] (last visited Feb. 24, 2019). The default wake word is “Alexa,” but users can set a custom wake word through the Alexa app. Id.
64. Id.
2020 WIRE(LESS) TAPPING 853

much like the Google Home. Additionally, it allows you to place calls, order things from Amazon, and install or create your own Alexa “skills.”

Skills are programmable tasks and apps that users can personalize and control with their voice.

Amazon continues to expand its line of products by offering headphones and car components that have Alexa built in.

Smart speakers are only the tip of the iceberg for smart home devices. Other smart home devices had an anticipated gross revenue of $4.6 billion for 2018, achieving a 36% projected growth from 2017. These devices run the gamut from thermostats, lightbulbs, outlets, security cameras, utility usage monitors, locks, vacuum cleaners, and appliances. Such devices use an internet connection to pair with other devices, like Google Home or Amazon Alexa.

C. Service Providers

Along with the data gathered by various device features, service providers constantly track a device’s location. The smartphone’s features and apps work together with service providers to create a comprehensive map of a device owner’s location. A smartphone constantly “pings” these towers to obtain service and use location services. As the technology improves, the ability to narrow the phone’s location down to a smaller radius

65. Id.; Google Home: Works With, supra note 59.
66. See Alexa and Alexa Device FAQs, supra note 63.
67. See Kevin Webb, These Were the 25 Most Popular Alexa Skills of 2018, According to Amazon, BUS. INSIDER (Dec. 30, 2018), [https://perma.cc/MC8Q-NR2F].
68. Amazon Echo and Alexa Devices, supra note 61.
69. Johnny Wood, This Is the Future of Tech in the US, WORLD ECON. F. (Sept. 7, 2018), [https://perma.cc/5N3N-NJQS].
70. See Alexa and Alexa Device FAQs, supra note 63; Google Home: Works With, supra note 59.
71. See Alexa and Alexa Device FAQs, supra note 63; Google Home: Overview, supra note 58.
73. See id. at 6.
74. See id. at 10.
increases.\textsuperscript{75} This accuracy improves if multiple towers are used to triangulate the phone’s location.\textsuperscript{76} This information is then kept with the phone’s service provider.\textsuperscript{77}

**D. Privacy Policies**

With the mass amounts of data gathered on consumers, technology companies realize the necessity of privacy. Each company has a privacy page on their website that lists the various protections they provide for their users.\textsuperscript{78} Apple’s privacy page boasts that “[y]our personal data belongs to you, not others.”\textsuperscript{79} However, Apple further clarifies that the phrase means that Apple does not sell your data to third parties.\textsuperscript{80} Apple, along with the other technology companies, can and will turn over your data to law enforcement. In fact, technology companies even have online guides for legal requests including subpoenas, search warrants, and court orders.\textsuperscript{81} Apple’s Legal Process Guidelines is a fourteen-page document that describes how to serve process and what information is available from Apple.\textsuperscript{82} Law enforcement does utilize the legal process to obtain users’ data from technology companies, and the companies do comply. Several technology companies publish biannual Transparency Reports that detail the legal requests they

\textsuperscript{75} See Phil Locke, Cell Tower Triangulation—How It Works, WRONGFUL CONVICTIONS BLOG (June 1, 2012), [https://perma.cc/VD88-FQV5].

\textsuperscript{76} Id.

\textsuperscript{77} See Webb, supra note 67; Melissa Locker, U.S. Cell Carriers Are Probably Still Selling Your Real-Time Phone Location Data, FAST COMPANY (Jan. 9, 2019), [https://perma.cc/R7D7-6BS4]. In January 2019, journalists uncovered that major service providers were selling user’s location data to third parties. Joseph Cox, I Gave a Bounty Hunter $300. Then He Located Our Phone, VICE (Jan. 8, 2019), [https://perma.cc/92QR-R5FQ]; Locker, supra note 77.


\textsuperscript{79} Privacy, APPLE, supra note 78.

\textsuperscript{80} Id.; Privacy Policy, APPLE, [https://perma.cc/VFQ5-VX2U] (last visited Oct. 4, 2019).


\textsuperscript{82} Privacy: Legal Process Guidelines, supra note 81.
receive and the amount that are responded to. Three prominent technology companies received a combined total of 110,444 requests in 2017. Of those requests, 73,963 were responded to by the companies, resulting in a 66.9% response rate.

Table 1:

<table>
<thead>
<tr>
<th>Company</th>
<th>Total Requests for 2017</th>
<th>Requests Responded To</th>
<th>Response Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>8,929</td>
<td>7,113</td>
<td>79.7%</td>
</tr>
<tr>
<td>Amazon</td>
<td>3,697</td>
<td>2,779</td>
<td>75.2%</td>
</tr>
<tr>
<td>Google</td>
<td>97,818</td>
<td>64,071</td>
<td>65.5%</td>
</tr>
<tr>
<td>Total</td>
<td>110,444</td>
<td>73,963</td>
<td>66.9%</td>
</tr>
</tbody>
</table>

II. THE PATH TO CARPENTER

As the Fourth Amendment encounters new technology and shifting policy stances, the doctrine becomes more nuanced and convoluted. The original purpose of the Fourth Amendment was to limit the government’s power to engage in extensive searches and seizures. To accomplish this, the Fourth Amendment prohibits unreasonable searches and seizures of “persons, houses, papers, and effects.” As a threshold matter, courts determine whether the Fourth Amendment applies to a search or seizure by evaluating if the police trespassed on a textually


84. See infra Table 1.

85. See id.

86. This data was compiled from the sources listed in supra note 83.


88. U.S. CONST. amend. IV.
protected area,\textsuperscript{89} or if the defendant had a reasonable expectation of privacy.\textsuperscript{90}

\section*{A. The Ebb and Flow of the Fourth Amendment Standards}

Under the trespass standard, the police must trespass on one of the four constitutionally protected areas: persons, houses, papers, or effects.\textsuperscript{91} The first two categories are relatively straightforward; however, papers and effects are somewhat of a grey area. To provide more clarity, courts draw from property and common law when determining whether a trespass has occurred.

\textit{Boyd v. United States} was one of the first cases to provide an in-depth evaluation of the trespass doctrine.\textsuperscript{92} In \textit{Boyd}, the government alleged that the defendants failed to pay duties on imported goods.\textsuperscript{93} The government obtained a subpoena requiring the defendants to produce documents relating to the importation of the goods.\textsuperscript{94} On Fourth Amendment grounds, the Supreme Court made two prominent assertions. First, the Fourth Amendment applies to a person’s property unless the government can indicate a possessory right in the object under property law.\textsuperscript{95} However, exceptions were noted, primarily that property law requirements did not exist for contraband.\textsuperscript{96} Second, the Court confirmed the sanctity of private papers and the contents thereof.\textsuperscript{97} The opinion quoted language from the English case \textit{Entick v. Carrington}:

\begin{quote}
Papers are the owner’s goods and chattels; they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the
\end{quote}

\begin{footnotes}
\textsuperscript{89} United States v. Jones, 565 U.S. 400, 404-05 (2012).
\textsuperscript{92} Boyd v. United States, 116 U.S. 616, 622 (1886).
\textsuperscript{93} \textit{id.} at 617-18.
\textsuperscript{94} \textit{id.} at 618.
\textsuperscript{95} \textit{See id.} at 623-24.
\textsuperscript{96} \textit{id.} at 624.
\end{footnotes}
laws of England be guilty of a trespass, yet where private papers are removed and carried away the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.\textsuperscript{98}

This case, along with historical documentation, indicates that the Founders had a more liberal view of property rights in mind when the Constitution and Bill of Rights were ratified.\textsuperscript{99} Drawing from Whig concepts and John Lock’s views, property not only included tangible objects, but intangible things such as rights, thoughts, and expressions.\textsuperscript{100} James Madison echoed these sentiments in his essay entitled \textit{Property}.\textsuperscript{101} There he wrote that “man is said to have a right to his property, he may be equally said to have a property in his rights.”\textsuperscript{102} An overarching theme was that expression of the self was included in the term property.\textsuperscript{103} This was further evidenced in the seminal article \textit{The Right to Privacy} by Charles Warren and Louis Brandeis.\textsuperscript{104} After creating this “right to privacy,” Warren and Brandeis asserted that such a right encompasses one’s personality,\textsuperscript{105} and that only publication by the author himself forgoes such a right.\textsuperscript{106}

Despite the broad protections under the trespass view during the 1800s and early 1900s, the protections began to constrict with \textit{Olmstead v. United States}.\textsuperscript{107} There, the Court applied the trespass standard to determine whether wiretapping a phone line that ran between the defendant’s house and business constituted a “search” under the Fourth Amendment.\textsuperscript{108} The Court held that the Fourth Amendment was not applicable in

\textsuperscript{98} Boyd, 116 U.S. at 627-28.
\textsuperscript{99} Cloud, supra note 97, at 49-50.
\textsuperscript{100} Id. at 43-48.
\textsuperscript{101} Id. at 47-50; Madison’s essay \textit{Property} was published in the National Gazette on March 29, 1792. It can be found in 6 James Madison, \textit{The Writings of James Madison}, 101 (Gaillard Hunt ed., 1906).
\textsuperscript{102} Cloud, supra note 97, at 48.
\textsuperscript{103} See id. at 49-50.
\textsuperscript{104} Samuel D. Warren & Louis D. Brandeis, \textit{The Right to Privacy}, 4 Harv. L. Rev. 193, 194-95, 205 (1890).
\textsuperscript{105} Id. at 205-96.
\textsuperscript{106} Id. at 198-200.
\textsuperscript{108} Id. at 455-57.
such a situation because the police were intercepting electronic signals from a line outside of the defendant’s home.109

It is in this context that a new standard emerged in *Katz v. United States*.110 There, the defendant used a public telephone booth, which the government had attached a listening and recording device to.111 The defense framed the questions for the Court as: was the phone booth a constitutionally protected area and “[w]hether physical penetration of a constitutionally protected area is necessary” for a Fourth Amendment violation?112 The Court rejected these issues, stating “the Fourth Amendment protects people, not places.”113 The issue was reframed broadly as “whether the search . . . complied with constitutional standards.”114

In the majority opinion, Justice Stewart alluded to the idea of a reasonable expectation standard.115 The test was more fully elucidated by Justice Harlan in his *Katz* concurrence.116 This standard was both subjective and objective. Step one asked if the person had “an actual (subjective) expectation of privacy.”117 Step two then evaluated if that “expectation [was] one that society [was] prepared to recognize as ‘reasonable.’”118 Over the years, the test eventually became more condensed, primarily focusing on the second prong.119

The Court was clear that the reasonable expectation of privacy test supplements the trespass analysis rather than fully replacing it.120 To further complicate matters, the reasonable expectation of privacy standard paved the way for the emergence of the third-party doctrine. Less than a decade after *Katz*, the Court determined that “a person has no legitimate

---

109. *Id.* at 466. But see *Silverman v. United States*, 365 U.S. 505, 511-12 (1961) (holding the insertion of a microphone into the air ducts of a home was a search under the Fourth Amendment).


111. *Id.* at 348.

112. *Id.* at 349-50.

113. *Id.* at 351.

114. *Id.* at 354.


116. *Id.* at 360-61 (Harlan, J., concurring).

117. *Id.* at 361.

118. *Id.* (emphasis added).


120. *Id.* at 2267-68 (internal citations omitted).
expectation of privacy in information he voluntarily turns over to third parties.\textsuperscript{121} Thus, allowing the government to search documents that one furnishes to a third-party without a warrant.\textsuperscript{122}

In \textit{United States v. Miller}, the government obtained the defendant’s bank statements without a warrant.\textsuperscript{123} The Court reasoned that negotiable instruments are not private communication, and the bank created and kept these documents for business purposes.\textsuperscript{124} In reaching such a conclusion, the Court rejected \textit{Boyd} and found that the bank owned the “business records;” therefore, the defendant could not assert a privacy right in property they did not own.\textsuperscript{125} In \textit{Smith v. Maryland}, the Court used a pen register to determine the numbers dialed from a phone without a warrant.\textsuperscript{126} Here, the Court applied the reasonable expectation of privacy test and held there was no search because the defendant “voluntarily conveyed” the information and “assumed the risk.”\textsuperscript{127}

As the Court has encountered cases that address modern technology, it has grappled with the interplay between the Fourth Amendment and third-party doctrine. In her concurrence in \textit{United States v. Jones}, Justice Sotomayor stated that “it may be necessary to reconsider [the third-party doctrine],” as it is “ill suited for the digital age.”\textsuperscript{128} Additionally, the reasonable expectation test has received substantial criticism. The major critique is deciding if the Court should evaluate this prong on a normative or empirical basis.\textsuperscript{129} A normative application would ask what privacy rights we should recognize, while an empirical application would ask what privacy rights we actually do have.\textsuperscript{130} The normative and empirical models both present one

\footnotesize{121. Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976) (finding that the third-party doctrine still applied “even if the information is revealed on the assumption that it will be used only for a limited purpose”).

122. Carpenter, 138 S. Ct. at 2216.

123. Miller, 425 U.S. at 437-38.

124. Id. at 442-43.

125. Id. at 440-41.

126. Smith, 442 U.S. at 737.

127. Id. at 744-45 (internal quotations omitted).


129. Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting); Id. at 2246 (Thomas, J., dissenting).

130. Id. at 2265 (Gorsuch, J., dissenting).}
major flaw: who should actually be making policy decisions and interpreting societal values? Under either model, courts and judges will be making these decisions, when in reality, the legislature likely has a better understanding of what we think or want to be considered as private. Additionally, the empirical model may lead to conflict as someone will still have to interpret and decide what privacy rights we do have. For example, Justice Gorsuch points out that many citizens believe that our privacy rights decrease as the severity of the crime increases. In reality, the Fourth Amendment applies the same regardless of the crime.

In 2011, the trespass doctrine made a return in Jones. Prior to Jones, the Court ruled on United States v. Knotts, and applied the reasonable expectation of privacy test. In Knotts, the government placed a tracking “beeper” inside a container in the defendant’s car. The Court declined to find a privacy interest because the location of the car and its final destination were “voluntarily conveyed to anyone who wanted to look.” However, the Court noted that the tracking in Knotts was confined to one specific trip, and the outcome or principles may be different for long-term tracking. That held true when the Court encountered Jones. In Jones, the government installed a GPS on the defendant’s car and tracked his location for twenty-eight days. But Jones was distinguishable from Knotts because the government attached the GPS directly to Jones’s car, whereas in Knotts the tracking device was put into a third

131. Id.
132. Id. See Rousso v. State, 239 P.3d 1084, 1095 (Wash. 2010) (en banc) (“It is the role of the legislature, not the judiciary, to balance public policy interests and enact law.”); Ganttt v. Sentry Ins., 824 P.2d 680, 687 (Cal. 1992) (“[P]ublic policy’ as a concept is notoriously resistant to precise definition, and that courts should venture into this area, if at all, with great care and due deference to the judgment of the legislative branch, ‘lest they mistake their own predilections for public policy which deserves recognition at law.’”).
133. Carpenter, 138 S. Ct. at 2265 (Gorsuch, J., dissenting).
134. Id.
137. Id. at 278.
138. Id. at 281-82.
139. See id. at 283-84.
140. Jones, 565 U.S. at 403.
141. Id.
party’s container before being placed in Knotts’s vehicle.\textsuperscript{142} The car in Jones was legally owned by the defendant’s wife; however, Justice Scalia drew from the principals of bailment to find that the car was the defendant’s.\textsuperscript{143} Because the car constituted the defendant’s property, the Court found that the installation of the GPS constituted a trespass on a textually protected area, and therefore, a Fourth Amendment search occurred.\textsuperscript{144}

**B. The Carpenter Majority**

With the reemergence of the trespass doctrine in Jones, objections towards the applicability of the reasonable expectation of privacy and third-party doctrines, and the Court requiring warrants for cell phone searches in the search incident to arrests context a few years prior in Riley v. California,\textsuperscript{145} Carpenter v. United States seemed to be the perfect opportunity for the Court to greatly expand Fourth Amendment protections for cell phones and technology. When the Carpenter opinion was released, it was evident that the Court barely scratched the surface on what needed to be done to protect citizens’ Fourth Amendment rights in the digital age. Instead, the Court added in yet even more nuance and confusion to the already complicated mix.

In Carpenter, the government subpoenaed two wireless carriers seeking the defendant’s cell-site location information (CSLI).\textsuperscript{146} That information enabled the government to triangulate the defendant’s location.\textsuperscript{147} Chief Justice Roberts, writing for the majority, preliminarily noted that CSLI and cell phone records have a “unique nature.”\textsuperscript{148} He also observed that a cell phone is “almost a ‘feature of human anatomy’”\textsuperscript{149} that is taken almost everywhere and is capable of acting as “an intimate

\textsuperscript{142} Knotts, 460 U.S. at 278.
\textsuperscript{143} Jones, 565 U.S. at 404 n.2 (“If Jones was not the owner he had at least the property rights of a bailee.”).
\textsuperscript{144} Id. at 404-05.
\textsuperscript{145} Riley v. California, 573 U.S. 373, 401 (2014). The court prohibited warrantless searches of a cell phone seized incident to arrest. Id.
\textsuperscript{147} Id. at 2212-13.
\textsuperscript{148} Id. at 2217.
\textsuperscript{149} Id. at 2218.
window into a person’s life,” by revealing their “familial, political, professional, religious, and sexual associations.”

While the reasonable expectation of privacy standard was used, the majority refused to apply the third-party doctrine for which the government advocated. Applying the third-party doctrine in this case would have been “a significant extension of [the third-party doctrine] to a distinct category of information.” The rejection of the third-party doctrine stemmed from the government’s failure “to appreciate that there are no comparable limitations on the revealing nature of CSLI.” This decision turned on two factors: the presence of location information and a lack of voluntary conveyance. The Court reasoned that there was no voluntary conveyance because cell-phone usage is so pervasive that it is almost necessary for one to own a cell phone, and CSLI data is obtained with minimal affirmative actions by the cell phone owner—all that is required is turning on the phone.

In sum, Chief Justice Roberts found that the comprehensive and revealing amount of data, which can be obtained retroactively and often collected without any affirmative action on the owner’s part created a privacy interest that could not be overcome by the third-party doctrine. Implicit in the opinion, is the idea that some data or information alone may not require a warrant, but when aggregated, the nature of the data transforms to the point that a warrant is required. However, no further guidance was provided.

The majority ultimately held that obtaining CSLI data requires probable cause and a warrant. But the majority

150. Id. at 2217.
151. Carpenter, 138 S. Ct. at 2217 (internal quotations omitted).
152. Id. at 2216-17.
153. Id. at 2219.
154. Id.
155. See id. at 2219-20.
156. Carpenter, 138 S. Ct. at 2220.
157. Id. at 2223.
158. See Sabrina McCubbin, Summary: The Supreme Court Rules in Carpenter v. Unites States, LAWFARE (June 22, 2018), [https://perma.cc/ZCF6-C4GT]; see Amy Howe, Opinion Analysis: Court Holds That Police Will Generally Need a Warrant for Sustained Cellphone Location Information, SCOTUSBLOG (June 22, 2018), [https://perma.cc/2B9R-ASFZ].
159. See Carpenter, 138 S. Ct. at 2221.
explicitly clarified that Carpenter does not: (1) express a view on “real-time CSLI or ‘tower dumps’;” (2) disturb the application of the third-party doctrine to “conventional surveillance techniques and tools;” (3) “address other business records that might incidentally reveal location information;” or (4) impact investigation techniques used for national security. Furthermore, Carpenter does not limit application of other exceptions to the warrant requirement, like the prospect of warrantless access to CSLI data if the facts give rise to an exigent circumstance.

On the merits, the Court held that the government’s subpoena request constituted a “search” within the meaning of the Fourth Amendment. The Court noted that its decision was a narrow one, but the convoluted reasoning left unanswered questions which prompted four dissents. Concerns from the dissenters generally focused on two key areas. First, the dissenters expressed concerns that the Court added yet another nuance to the Fourth Amendment’s application. These concerns stemmed from the majority calling out CSLI as a “distinct category of information” without providing further guidance for future issues. This was important as it was the majority’s deciding factor for whether the third-party doctrine applied. Second, the dissenters called out the majority for alluding to instances where warrantless searches of distinct information may be acceptable without providing further guidelines.

C. The Carpenter Dissents

This narrow majority opinion did little in reconciling the Fourth Amendment, the third-party doctrine, and modern technology. As a result, it prompted several dissents. Justice Kennedy criticized the Carpenter decision for “fail[ing] ‘to

160. Id. at 2220.
161. Id. at 2223.
162. Id. at 2220.
163. Id.
164. Carpenter, 138 S. Ct. at 2234 (Kennedy, J., dissenting).
165. Id. (internal quotations omitted).
166. Id. at 2220.
167. Id. at 2234 (Kennedy, J., dissenting).
provide clear guidance to law enforcement’ and courts on key issues raised by its reinterpretation of Miller and Smith. For example, he wrote the majority failed to discuss how to determine if something is a “distinct category of information” and how much information is required to obtain a search warrant. Justice Kennedy concludes by stating that the proper outcome would have “interpret[ed] accepted property principles as the baseline for reasonable expectations of privacy” and remanding the case.

In a second dissent, Justice Thomas suggested reframing the question to focus on “whose property was searched” rather than if a search occurred. Although Justice Thomas relied on property principles, he disagreed with Justice Kennedy’s use of such principles in the context of a reasonable expectation analysis. Justice Thomas preferred to read the Fourth Amendment literally, which would wholly reject the Katz test. That test, he wrote, has “no plausible foundation in the text of the Fourth Amendment” and “confuses the reasons for exercising the protected right with the right itself.”

Justice Alito penned a third dissent that also focused heavily on property law principles. First, he agreed with Justice Kennedy that the defendant did not own the CSLI records under a strict property law analysis. Second, Justice Alito added that even under the Katz test and third-party doctrine, the defendant “lack[ed] any meaningful property-based connection” to the CSLI records held by the service providers.

In a fourth dissent, Justice Gorsuch took a different approach. Although he disfavored keeping the third-party doctrine on “life support,” he fundamentally shared the

168. Id. (quoting Riley v. California, 134 S. Ct. 2473, 2491 (2014)).
169. Carpenter, 138 S. Ct. at 2234 (Kennedy, J., dissenting).
170. Id. at 2235.
171. Id. (Thomas, J., dissenting) (emphasis in original).
172. Id. at 2236.
173. Id.
175. Id. at 2240 (quoting THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 78 (2008)) (internal quotations omitted).
176. Id. at 2259-60 (Alito, J., dissenting).
177. Id. at 2260.
178. Id.
majority’s view that the rationale behind the third-party doctrine is wrong. Accordingly, Justice Gorsuch proposed three options: keep the third-party doctrine and “live with the consequences,” ask only if there is “a reasonable expectation of privacy” in data held by third parties,” or do something different. After dismissing options one and two on the grounds that they, respectively, would leave government unchecked, Justice Gorsuch instead focused on his third option. His proposed solution would incorporate traditional property principles, like bailment, while also allowing the legislature to step in and help clarify ownership and privacy issues with data. Justice Gorsuch wrote that his proposal could increase Fourth Amendment protections, comply with a textual interpretation of the Fourth Amendment, reduce “judicial intuition,” and incorporate state law.

III. A RETURN TO OLD IDEALS FOR NEW TECHNOLOGY

As previously indicated, modern technology poses two key issues for the Fourth Amendment. First, technology is developing at an exponential rate while the law is several steps behind. This creates a “Fourth Amendment lag.” The lag increases if a case makes it on the Supreme Court’s docket. Another critical issue is how to reconcile the third-party doctrine with advancing, interconnected technology. While the Carpenter Court declined to apply the third-party doctrine to location data, it kept the doctrine “on life support.” This suggests that the third-party doctrine can still apply to devices that do not track the user’s location. If true, the government could potentially obtain all of the data from a user’s smart home.

179. Carpenter, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).
180. Id. at 2262, 2264.
181. Id. at 2264, 2266-67.
182. See id. at 2267-70.
183. See id. at 2268-70.
184. Richards, supra note 87, at 1448 (internal quotations omitted).
185. See id. at 1456-57, 1465, 1488.
186. Id. at 1482-83.
187. Carpenter, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).
device—like an Amazon Alexa or Google Home that obtains data from a multitude of other smart devices.

*Carpenter* failed to create a workable standard that can apply to current and future technology. Justice Gorsuch described three paths from which we can choose.\(^\text{188}\) Path one would continue to apply the third-party doctrine, leaving mass amounts of private information exposed. Path two would have judges apply the *Katz* test, giving them a lot of discretion and potentially acting as the third-party doctrine in disguise. Path three would propose a new solution. Given the examples illustrated in the preceding paragraph, the third path is the best option.

States, and especially Arkansas, can provide its own citizens adequate protection under their own constitutions. Through judicial federalism, states can interpret their constitutions more broadly than the United States Constitution.\(^\text{189}\) As states begin to interpret constitutional provisions differently than the federal courts, such as the Fourth Amendment,\(^\text{190}\) there is evidence indicating that the Supreme Court may follow suit. In three instances—adoption of the exclusionary rule,\(^\text{191}\) allowing warrantless probable cause arrests,\(^\text{192}\) and permitting warrantless entries into homes—\(^\text{193}\) the Supreme Court looked to state laws and trends when formulating their opinions.\(^\text{194}\)

Evidence suggests that Arkansas and other states might use judicial federalism to depart from the third-party doctrine. One 2006 study conducted a fifty-state survey of how each state applied Fourth Amendment principles.\(^\text{195}\) At that time, thirty-

---

\(^{188}\) Id. at 2262.


two states had diverged or gave reason to suspect they might diverge from the Supreme Court’s interpretation of the Fourth Amendment. 196 Eleven of these states rejected the third-party doctrine. 197 The study classified Arkansas as a state that might reject the third-party doctrine. 198

The Fourth Amendment of the Arkansas Constitution has identical language to the Fourth Amendment of the United States Constitution. 199 Because of this, Arkansas originally took the stance that it would not deviate from the Supreme Court’s interpretation of the Fourth Amendment. 200 In 2000, that view changed in State v. Sullivan with the Arkansas Supreme Court writing, “there is nothing that prevents this court from interpreting the U.S. Constitution more broadly than the United States Supreme Court, which has the effect of providing more rights.” 201 Despite that language, the Supreme Court declined to construe Arkansas’ constitutional provisions differently than the United States Constitution. 202

Since Sullivan, the Arkansas Supreme Court has thematically focused its judicial review on the Arkansas Constitution rather than the United States Constitution, particularly in the context of pretextual arrests and warrantless consent searches. 203 By interpreting the State’s Fourth Amendment differently, Arkansas courts can provide citizens

---

196. Id.
197. Id.
198. Id.
199. Compare U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”), with ARK. CONST. art. 2, § 15 (“The right of the people of this State to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue, except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.”).
with comparatively more protections than its federal counterparts while evading federal review.\textsuperscript{204}

In \textit{Sullivan}, the defendant was stopped for a traffic violation and arrested when narcotics were found in his possession.\textsuperscript{205} On remand, the court held that pretextual arrests are unreasonable and therefore subject to the exclusionary rule.\textsuperscript{206} It reasoned that Arkansas precedent historically viewed pretextual arrests as unreasonable.\textsuperscript{207}

Next, consider consent searches. In \textit{Griffin v. State}, officers engaged in a nighttime warrantless search of Griffin's shed and car before gaining his consent.\textsuperscript{208} The Court held this search invalid because officers must give an individual the opportunity to reject a warrantless search before conducting the search.\textsuperscript{209} Two key factors impacted the Court's reasoning and ultimate decision to depart from federal standards. First, Arkansas required police officers to comply with "rigorous standards" to obtain a warrant for a nighttime search.\textsuperscript{210} Second and more importantly, similar issues regarding actual consent during knock-and-talk searches were frequenting dockets across several states.\textsuperscript{211}

Only a few months after \textit{Griffin}, in \textit{Jegley v. Picado}, the Arkansas Supreme Court struck down an Arkansas statute that criminalized sodomy.\textsuperscript{212} In \textit{Jegley}, the Court established the right to privacy as a fundamental right accorded to citizens in the Arkansas Constitution.\textsuperscript{213} The Court reasoned that more than eighty statutes referenced privacy, which the Court viewed as "a public policy . . . supporting a right to privacy."\textsuperscript{214} The

\textsuperscript{204} See Henderson, \textit{supra} note 195, at 375 (discussing the Supreme Court's opinion that any state relying on its constitution "immunizes its decision from review by [the] Court").

\textsuperscript{205} \textit{Sullivan I}, 340 Ark. 315, 318-B, 16 S.W.3d at 551-52.


\textsuperscript{207} \textit{Id}.


\textsuperscript{209} \textit{Id}. at 800, 67 S.W.3d at 590.

\textsuperscript{210} \textit{Id}. at 793, 67 S.W.3d at 585.

\textsuperscript{211} \textit{Id}. at 801, 67 S.W.3d at 591 (Brown, J., concurring).

\textsuperscript{212} Jegley v. Picado, 349 Ark. 600, 636-38, 80 S.W.3d 332, 353-54 (2002).

\textsuperscript{213} \textit{Id}. at 630-32, 80 S.W.3d at 349-50.

\textsuperscript{214} \textit{Id}. at 628-29, 80 S.W.3d at 347-48.
Court concluded by stating that “Arkansas has a rich and compelling tradition of protecting individual privacy.”\textsuperscript{215}

\textit{Jegley} played a key role when Arkansas deviated from federal precedent again in \textit{State v. Brown}.\textsuperscript{216} There, the police obtained the homeowner’s consent to search her house but failed to inform her of her right to refuse consent.\textsuperscript{217} Relying on \textit{Jegley}, the Court reasoned that there is a sacrosanct zone of privacy around a person’s home, and that “Arkansas has clearly embraced a heightened privacy protection for citizens in their homes against unreasonable searches and seizures.”\textsuperscript{218} The \textit{Brown} opinion not only expanded citizens’ rights in the consent context, it also explained that Arkansas courts will deviate from federal precedent “when the result is patently wrong and so manifestly unjust that a break becomes unavoidable.”\textsuperscript{219}

Although these cases provide an overview of when Arkansas will deviate from federal interpretation, Arkansas courts may decline to deviate if there is a “difficulty in balancing interests and setting rules.”\textsuperscript{220} Given this framework, it seems likely that Arkansas would reject the third-party doctrine so long as a workable test replaces it. The technology discussed in Section I essentially gives the police warrantless access to all of a user’s data and information through the third-party doctrine,\textsuperscript{221} which, in effect, reduces Fourth Amendment rights “to nearly nothing.”\textsuperscript{222} Surely that is a result that an Arkansas court could find “patently wrong and so manifestly unjust.”\textsuperscript{223}

\textbf{IV. HOW TO APPROACH UNDER THE TRESPASS THEORY}

In the closing remarks of his \textit{Carpenter} dissent, Justice Gorsuch chastised the defense for failing to argue the

\begin{itemize}
\item \textsuperscript{215} \textit{Id.} at 632, 80 S.W.3d at 349-50.
\item \textsuperscript{217} \textit{Id.} at 464-65, 156 S.W.3d at 725.
\item \textsuperscript{218} \textit{Id.} at 469-70, 156 S.W.3d at 729.
\item \textsuperscript{219} \textit{Id.} at 473, 156 S.W.3d at 731.
\item \textsuperscript{220} \textit{See} \textit{State v. Harris}, 372 Ark. 492, 500, 277 S.W.3d 568, 575-76 (2008) (declining to extend heightened privacy protections to vehicles).
\item \textsuperscript{221} \textit{See} discussion supra Section I.
\item \textsuperscript{222} \textit{Carpenter} v. United States, 138 S.Ct. 2206, 2262 (Gorsuch, J., dissenting).
\item \textsuperscript{223} \textit{Brown}, 356 Ark. at 473, 156 S.W.3d at 731.
\end{itemize}
applicability of state laws or the trespass standard despite Jones and Florida v. Jardines providing notice of the Court’s willingness to hear such arguments. Additionally, the majority opinion reminds us that “the analysis is informed by the historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted.” Thus, by arguing the trespass standard in data cases and including historical and state property laws in the analysis, defendants may be able to successfully bypass the reasonable expectation of privacy doctrine and the accompanying third-party doctrine. Such an approach may have more success at the state level, but the Carpenter decisions seems to indicate that the approach will not automatically fail at the federal level. This section will evaluate potential arguments rooted in property law that can establish a textually protected interest in data.

A. Protected Category

Like the United States Constitution, the Arkansas Constitution protects persons, houses, papers, and effects. Data stored on servers and microchips does not neatly fit into any of these categories. Drawing from federal historical perspectives, certain types of data—such as texts, emails, documents, etc.—could fall into the category of expressive or content property that the Founders held sacred. Other data must be deemed to be a paper or an effect. Case law indicates that demonstrating a possessory interest may fulfill this requirement.

224. Carpenter, 138 S.Ct. at 2272 (Gorsuch, J., dissenting).
225. Id. at 2213-14. (majority opinion).
227. See supra Section III.
228. See Brown, 356 Ark. at 469-70, 156 S.W.3d at 728-29 (describing the evolution and extent of Arkansas constitutional protections).
229. See supra Part II(a).
230. See supra note 144 and accompanying text.
B. Ownership

Ownership of property requires an owner to exercise dominion and control over property while also having an intent to own. Other property rights such as free alienability and the right to exclude all others may also help to define ownership. At first blush, it may seem that users do not possess these rights in the context of their data, as companies may also exert dominion and control over the data. For example, companies may use an individual’s data for advertising, to improve user experience, and may even share the data with third parties. But when evaluating user accessibility, most companies allow users some control over their data. Google, for instance, allows users to download a copy of all of their data, delete or modify saved data, and also place certain restrictions on what third-parties may use or obtain. Such capabilities seem to establish dominion and control over the data collected.

Data users also have a right to exclude all others from accessing their data. Data management tools aside, most devices allow users to choose how much data they share with other applications and companies. Apple either discloses what companies they may share your data with or requires you to accept data sharing with other entities—usually in the form of a pop-up notification that requires you choose to “accept” or “decline” the company’s policy. The ability of users to delete gathered data or provide encryptions also excludes the companies or providers from accessing the data. Finally, a user’s data is freely alienable. Most companies allow users to determine how much data they want to share, and with whom. Data may, for example, be shared with another technology company, a private party, or law enforcement.

232. See id.
233. See discussion supra Parts I(b), (d).
234. Privacy Policy, Google, supra note 78.
236. See Google, supra note 78.
237. See supra Part IV(b).
238. See supra Section I.
Furthermore, Apple uses differential learning to improve its services. Differential learning uses data patterns from all users as opposed to a user’s personal data. Users reserve their data privacy as “[d]ifferential privacy transforms the information shared with Apple before it ever leaves the user’s device such that Apple can never reproduce the true data.” Therefore, in these cases, the company or third parties do not have access to the user’s personal data. This would eliminate many third-party doctrine concerns. Because the company does not receive “clear data” or any user identifications, the user maintains dominion and control over their data. It also follows that users can choose whether to share their data with others or not, meeting the freely alienable and right of exclusion elements. Companies that employ differential learning give users a stronger argument that users “own” their data.

Case law illustrates that exclusive possession may not be required to establish a property right in the data. Consider home ownership where a family may all live in one house and have authority to consent to a search of the house despite all family members not being listed on the deed. By contrast, in rental situations, a landlord may not consent to a search of a tenant’s space. The Supreme Court has held that effective consent by non-owners, other than landlords, relies on “‘common authority’ over the premises... [and] rest[s] on ‘mutual use of the property’ by one ‘having joint access or control for most purposes.’” Thus, a spouse may consent to searches of the

240. Id.
241. Id.
242. See supra Part IV(b).
243. See, e.g., Bruce v. State, 367 Ark. 497, 502-03, 241 S.W.3d 728, 731-32 (2006) (finding wife had authority to consent to search of home); Grant v. State, 267 Ark. 50, 56-57, 589 S.W.2d 11, 14 (1979) (holding the stepfather could consent to search of stepson’s bedroom despite the stepson paying rent); Washington v. State, 251 Ark. 487, 492, 473 S.W.2d 157, 160 (1971) (finding the warrantless search valid where a regular occupant of the apartment let the police in).
home, but a visitor may not. Application of this doctrine to the data context, a company most likely lacks “joint access or control” over the user’s data. Accordingly, a company cannot consent to turn over a user’s data without a search warrant. However, even if a company possessed joint or apparent authority over the data, the company would be wise to institute a policy of refusing consent and requiring officers to obtain a warrant.

Although traditional property law indicates that users have an ownership interest in their data, a different analytical approach may be preferable. In his Carpenter dissent, Justice Thomas suggests that companies’ terms of service may establish property rights in data. While Carpenter’s contracts with Sprint and MetroPCS did not give Carpenter ownership over the location data, Justice Thomas stated that “such provisions could exist in the marketplace” and cited Google’s terms of service. This could shift the onus to technology companies to include this simple phrase to protect their customers. However, this could restrict the company’s ability to utilize users’ data.

C. Bailment

Bailment is “delivery of personalty for some particular purpose, or on mere deposit, upon a contract, express or implied, that after the purpose has been fulfilled it shall be redelivered to the person who delivered it, or otherwise dealt with according to his directions.” In Arkansas, there are three key elements to

246. See id.
247. Grant, 267 Ark. at 55, 589 S.W.2d at 13-14.
248. See id.
250. Id.
251. Terms of Service: Your Content in Our Services, GOOGLE, [https://perma.cc/Y4M8-BR9L] (last updated Oct. 25, 2017). “Some of our services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.” Id.
establish bailment: (1) actual delivery to the bailee, (2) acceptance by the bailee, and (3) sole and temporary custody by the bailee. If these elements are met, any issues with the company still being in possession of the data are bypassed.

Assuming that a user's data is their property, most devices and settings allow technology companies to periodically obtain and store user data on their servers or cloud. This would constitute actual delivery. Because the technology companies establish this process, acceptance of the user's data is implied. Whether a company has sole and temporary control over data could present an issue. Most companies allow users to access, modify, and delete their stored data to some extent. In Arkansas, a bailor must part control with their property to establish a bailment. But consider the purpose of the bailment: users turn over their data for storage and safe keeping or to improve their services.

If a user stores information with a company for safe keeping, an analogy can be drawn to a safety deposit box. Safety deposit boxes can be a form of bailment between the bank and the patron who rents the box. There is nothing stopping a safety deposit box owner from accessing the contents of his box multiple times a day. If he does so, his bailment would still continue to exist. Similarly, a user would not

---


254. See supra Part IV(b).

255. See supra Part I(a).


257. See supra Parts I(a), IV(b).

258. Tedder v. Blackmon's Auctions Inc., 274 Ark. 241, 243-44, 623 S.W.2d 516, 517-18 (1981) (finding no bailment between owner and auctioneer where owner was present during the auction and was free to take the vehicles at any time).


jeopardize their bailment by accessing their data or cloud contents.

Furthermore, this analogy also helps defeat other potential concerns, such as third-party access. A safety deposit box requires a key for access. Such a key is usually possessed by the owner and the bank. Perhaps the bank had to store the safety deposit box at another location—would this give the new location or entity access to its contents? Large technology companies often use third-party servers to store mass amounts of data. However, when they do so, the company encrypts the data. Like a safety deposit box, a special key is needed to unencrypt the data. Thus, some required method of protection—such as encryption or password—utilized by either the user or company before the data is sent to the Cloud or a third party could work to defeat third-party claims to the information.

Bailment provides an extra layer of protection due to its quasi-contract-property law nature. Because contract principles are present in bailment law, a company can further define the terms of the bailment through agreements with users. Such agreements could come in the forms of terms and conditions or privacy policies. Conceivably, a company could disclose that it will, for example, use data to improve your services or store your data in a remote server owned by a different company and still preserve the bailment, thus, still providing users’ data with Fourth Amendment protections.

262. See Liability for Loss of Contents, supra note 260.
263. See id.
264. See Ivan Widjaya, How Do Large Companies Store and Manage Digital Information?, CLOUD BUS. REV. (Apr. 11, 2018), [https://perma.cc/M2YL-R5LB].
265. See Cloud Encryption: Using Data Encryption in the Cloud, BUSINESS.COM (July 3, 2018), [https://perma.cc/7MYC-VW3V].
266. See A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?, SURVEILLANCE SELF-DEFENSE, [https://perma.cc/753C-PAVN] (last updated Nov. 29, 2018); Michael Grothaus, Apple Should Borrow These 4 Privacy Features from the Competition, FAST COMPANY (Jan. 31, 2019), [https://perma.cc/3TLM-XTCW].
267. See Bailments, supra note 256, § 30.
D. Role of State Legislature

While Arkansas may be willing to depart from federal precedent for Fourth Amendment cases, attorneys must make their state law arguments using a sparse collection of case law. To make up for lack of case law, attorneys will have to rely on persuasive authority. Alternatively, the Arkansas legislature could enact laws that give Arkansans a possessory right in their data. Other states have enacted such legislation on a variety of other topics. For example, Alaska limits how DNA may be collected and analyzed, while also giving the people property rights in their DNA.268

This approach would not automatically solve all Fourth Amendment issues regarding data. Instead, it assumes that a positive law model—as advocated for by Justice Gorsuch—is in place. Under a positive law model, government action would be in violation of the Fourth Amendment if the governmental agent, when “stripped of [his] official authority,” was acting in a manner that was tortious, criminal, or in violation of another law.269 Neither Arkansas nor federal courts have expressly adopted a positive law model. However, by enacting legislation creating a property right in data, Arkansas defendants would then have the green light to begin making such arguments.

V. CONCLUSION

Fourth Amendment jurisprudence has long struggled with how to properly integrate new technology and the legal issues it brings into the doctrine. Defining citizens’ rights through a property law analysis was one of the early approaches. Though this approach is not perfect, it creates the most flexible framework for Fourth Amendment analysis. Additionally, the concept of judicial federalism paired with property law derived from state law allows states to take the reins in defining Fourth Amendment rights in the Cloud.


Arkansas property law can preserve a user’s interest and privacy in data despite the user sharing such data with technology companies, through the Cloud, or with other devices. In applying case law, a user’s data exhibits the elements of ownership necessary for a property interest. Where the law may be lacking or subject to debate, the law of bailment can serve as a workaround to the third-party doctrine. Such a framework can work for various devices and data that have unique storage and sharing capabilities. Furthermore, the Arkansas legislature can step in and create a statutory property right in data to allow defendants to make positive law arguments. Finally, this framework is one that can, presumably, apply to most conceivable future technology without requiring great deviation.