THE PRIVACY SACRIFICE FOR THE EASE OF TECHNOLOGY

STATE V. MIXTON, 478 P.3D 1227 (ARIZ. 2021).

*Alicia Pearson**

TABLE OF CONTENTS

I. INTRODUCTION

With technology continually advancing at a rapid speed, society continues to adapt and embrace new technological revolutions—but at what cost? Each technological advancement requires the individual to make an ultimate decision: adapt and embrace or reject and resist. To adapt and embrace allows for ease in today's society, where smartphones and smartwatches convert multiple devices into one, providing for functionality with the tap of a screen. Technology has expanded the boundaries of society where this functionality has become "such a pervasive and insistent part of daily life."[1] To reject and resist such ease

* J.D. Candidate, May 2023, Rutgers Law School—Camden. This Comment is dedicated to the marginalized groups in society that I had the honor of providing healthcare to as a Registered Nurse working in a busy inner-city emergency room in Philadelphia. These are the groups of society that continue to disproportionately bear the burden of state-imposed disrespect when it comes to privacy.

1. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (citation omitted).

in turn burdens the individual, who then struggles to participate in modern society.

While society continues to adapt and embrace technological advancements, are the federal and state constitutions that safeguard society's privacy keeping up? Can society rest easy knowing that constitutional provisions have been future-proofed? The quick answer seems to be no. It has been suggested, for example, that the Supreme Court of the United States only recently "began the process of future-proofing the Fourth Amendment" in *Carpenter v. United States*.[2] In that case, the Court was forced to reckon with the digital age and determine how the Fourth Amendment could fit within.[3] While the Court was able to reframe the Fourth Amendment, it essentially revealed "its fractured soul."[4] It is clear that "[t]he constitutional path forward is unclear and no single Fourth Amendment theory controls."[5] Despite the law of privacy remaining convoluted, the Court was able "to bring the Fourth Amendment into the digital future and protect against growing technologically enhanced police surveillance powers."[6] However, that was only the beginning.

In *State v. Mixton*,[7] the Supreme Court of Arizona reckoned with the digital age and confirmed how convoluted the path of privacy law truly is. The court held:

> [N]either the Fourth Amendment to the United States Constitution nor article 2, section 8 of the Arizona Constitution requires law enforcement officials to secure a search warrant or court order to obtain IP addresses or subscriber information voluntarily provided to [internet service providers] as a condition or attribute of service.[8]

The court further held that, "[t]he Fourth Amendment does not apply to IP addresses or subscriber information under the third-party doctrine, and this information is not a 'private affair' under the Private Affairs Clause" of article II, section 8.[9] The court determined that privacy was to be sacrificed for the ease of technology.

---

2. Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/.
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. 478 P.3d 1227 (Ariz. 2021).
8. *Id.* at 1245.
9. *Id.*

II. STATEMENT OF THE CASE

An internet service provider ("ISP") "is a company that provides individuals with access to the internet."[10] The ISP then "assigns a string of numbers, called an IP address, to a customer's modem to facilitate access to the internet."[11] While a user does not control or own an IP address, it is "always attached, 'like a "return address," to every "envelope" of information exchanged back and forth by computers that are actively communicating with each other over the internet.'"[12] "When a computer accesses a website, the IP address tells the website where to transmit data."[13] Standing alone, an IP address does not reveal the identity of an internet user but rather only reveals the "user's approximate geographic location, such as a neighborhood, and the user's ISP."[14] The ISP on the other hand possesses the subscriber's information and "maintains records and information, such as the name, address, and telephone number associated with an IP address."[15]

In 2016, an undercover detective posted an online ad seeking users interested in child pornography.[16] The detective was contacted by the username "tabooin520" who requested to be added to a group messaging chat on an application called "Kik."[17] Once added, the username sent images and videos of child pornography via the group chat and also to the detective.[18] On behalf of the request by the detective, federal agents with Homeland Security Investigations "served a federal administrative subpoena authorized under federal law on Kik to obtain tabooin520's IP address."[19] The IP address was provided to the detective who then used publicly available databases to determine that Cox Communications was the ISP for the IP address.[20] Federal agents with Homeland Security Investigations "then served another federal administrative subpoena on Cox for the subscriber information associated with the IP address."[21] Cox Communications complied and disclosed the subscriber information which included the name, street address, and phone number of the

10. *Id.* at 1229.
11. *Id.*
12. *Id.* (quoting United States v. Jean, 207 F. Supp. 3d 920, 928–29 (W.D. Ark. 2016), *aff'd* 891 F.3d 712 (8th Cir. 2018)).
13. *Id.*
14. *Id.*
15. *Id.* at 1230.
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.*
21. *Id.*

subscriber, William Mixton.[22] The detective then used this information to obtain a search warrant for Mixton's residence.[23] Upon execution of the warrant, a cell phone, external hard drive, laptop, and desktop computer were seized and searched which revealed photos and videos of child pornography.[24] The search also revealed messages, photos, and videos that Mixton sent to the detective under the username "tabooin520."[25]

William Mixton "was indicted on twenty counts of sexual exploitation of a minor under fifteen years of age."[26] His motion to suppress the subscriber information and all evidence seized, "on the grounds that [both] the Fourth Amendment to the United States Constitution and article 2, section 8 of the Arizona Constitution require[d] a warrant or court order to obtain his IP address and ISP subscriber information," was unsuccessful.[27] The jury convicted him on all counts, and he appealed.[28]

On appeal, a split decision from the court of appeals affirmed his convictions and sentences.[29] The court held that "although Mixton lacked a reasonable expectation of privacy under the Fourth Amendment, the Arizona Constitution required a search warrant to obtain his ISP subscriber information, and the federal third-party doctrine did not apply to the Arizona Constitution."[30] "[A]lthough the State obtained Mixton's ISP subscriber information in violation of the Arizona Constitution, suppression of the information was unnecessary because the good-faith exception to the exclusionary rule applied, as no precedent prohibited the search, controlling law deemed the search reasonable, and law enforcement reasonably relied on existing precedent."[31] The Supreme Court of Arizona granted review.[32]

III. BACKGROUND

A. Federal Privacy

"The Fourth Amendment protects '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.* (citations omitted).
31. *Id.*
32. *Id.*

searches and seizures.'"[33] It "was designed to protect individuals against 'arbitrary invasions by governmental officials.'"[34] Traditionally, the Supreme Court has evaluated the Fourth Amendment's search and seizure "through a lens of 'common-law trespass.'"[35] "[T]he Court has recognized that the Fourth Amendment protects people, not just places, when an individual 'seeks to preserve something as private' and that expectation is 'one that society is prepared to recognize as reasonable.'"[36] "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[37]

1. Third-Party Doctrine

The Third-Party Doctrine[38] is "an analytical construct used to differentiate between information a person seeks to preserve as private, and information that, because he shares it with others, is not treated as private."[39] Under this doctrine, "a person has no expectation of privacy in information he voluntarily discloses to third parties, even if there is an assumption it will be used only for a limited purpose."[40] "[B]ecause it is no longer private, the government may obtain such information from a third party without triggering the Fourth Amendment's protections."[41]

Carpenter v. United States[42] "created a 'narrow' exception to the third-party doctrine, requiring the government to obtain a search

33. *Id.* at 1231 (alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018)).

34. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2213).

35. *Id.* (quoting United States v. Jones, 565 U.S. 400, 405 (2012)).

36. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2213).

37. *Id.* (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

38. Federal appellate courts have held that IP addresses and ISP subscriber information are not protected by the Fourth Amendment because both categories of information fall within the "third-party doctrine" exception. *Id.* (collecting cases).

39. *Id.*

40. *Id.*; *see also* United States v. Miller, 425 U.S. 435, 440 (holding no reasonable expectation of privacy in bank records); Smith v. Maryland, 442 U.S. 735, 742 (holding no reasonable expectation of privacy in numbers dialed on home telephone). The Court emphasized the fact that defendants knowingly conveyed this information to a third party. *Mixton*, 478 P.3d at 1231. However, the Court also "considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Id.* at 1232 (quoting *Carpenter*, 138 S. Ct. at 2219 (citation omitted)); *cf.* Katz v. United States, 389 U.S. 347, 350–53 (holding that the warrantless monitoring of telephone conversations from a public telephone booth violated the Fourth Amendment).

41. *Mixton*, 478 P.3d 1227.

42. 138 S. Ct. 2206 (2018).

warrant for CSLI."[43] In that case, "officers accessed cellphone data, commonly known as cell-site location information ("CSLI"), to reveal a suspect's movements over the course of 127 days."[44] The Court focused on the fact that CSLI is "generated continuously without a user's affirmative act,"[45] explaining that "CSLI is generated by a cellphone whenever it receives a text, email, call, or when an app seeks to refresh data."[46] The Court deemed this evidence to be "detailed, encyclopedic, and effortlessly compiled."[47] It provided the government with "near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[48] Due to the fact that such data was compiled effortlessly and continuously, the Court held that a "'detailed chronicle of a person's physical presence compiled every day, every moment, over several years' implicated privacy concerns far exceeding those in *Smith* and *Miller*."[49]

B. State Privacy

"The Arizona Constitution provides that '[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law.'"[50] This section is known as the "Private Affairs Clause," and was adopted from the Washington State Constitution.[51] "Passage of Arizona's Private Affairs Clause preceded the Fourteenth Amendment's incorporation of the Fourth Amendment, but it 'is of the same general effect and purpose as the Fourth Amendment to the Constitution of the United States.'"[52] Arizona's Constitution is "more explicit than its federal counterpart in safeguarding the fundamental liberty of Arizona

43. *Mixton*, 478 P.3d 1232; *see also Carpenter*, 138 S. Ct. at 2210, 2220. However, since Carpenter's narrow holding, "every federal appellate court addressing the issue has affirmed that the Fourth Amendment's warrant requirement does not reach IP addresses and ISP subscriber information." *Mixton*, 478 P.3d at 1232–33 (collecting cases).

44. *Mixton*, 478 P.3d at 1232.

45. *Id.*

46. *Id.*

47. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2216).

48. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2218).

49. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2220); *see also* United States v. Miller, 425 U.S. 435, 440 (1976) (holding no reasonable expectation of privacy in bank records); Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding no reasonable expectation of privacy in numbers dialed on home telephone).

50. *Mixton*, 478 P.3d 1227, 1234–35 (alteration in original) (quoting ARIZ. CONST. art. 2, § 8).

51. *Id.* at 1235.

52. *Id.* (quoting Turley v. State, 59 P.2d 312, 316 (Ariz. 1936)).

citizens."[53] By its terms, it broadly protects an "expansive realm of 'private affairs.'"[54]

However, despite the differences in language, since statehood, the Private Affairs Clause has been interpreted to serve "the same general effect and purpose as the Fourth Amendment," and therefore is meant to preserve and protect the same rights that the Fourth Amendment is meant to protect.[55] Despite this interpretation, Arizona courts retain the right "to give such construction to [the state's] own constitutional provisions as [the court] think[s] logical and proper," notwithstanding the parallels to the Federal Constitution.[56] The Arizona Supreme Court has recognized the "value in uniformity with federal law when interpreting and applying the Arizona Constitution"[57] and has emphasized that the court has "yet to expand the Private Affairs Clause's protections beyond the Fourth Amendment's reach, except in cases involving warrantless home entries."[58]

Due to the fact that "private affairs" is not defined within the Arizona Constitution, the Arizona Supreme Court has looked to its "natural, obvious, and ordinary meaning," while focusing on such a meaning that would have existed at the time the Constitution was adopted.[59] The court considers various definitions and looks to the history of the passage of the Private Affairs Clause.[60] The clause "was taken verbatim from the

53. *Id.* (quoting State v. Ault, 724 P.2d 545, 549 (Ariz. 1986)).

54. *Id.* Compare with the Constitution of the United States' Fourth Amendment that "protects a finite index of enumerated items— 'persons, houses, papers, and effects.'" *Id.*; *see also* Timothy Sandefur, *The Arizona "Private Affairs" Clause*, 51 ARIZ. STATE L.J. 723 (2019) ("[D]espite repeatedly acknowledging that the Arizona Constitution can and should protect a broader range of rights than the federal Constitution, [Arizona courts] have largely failed to give effect to that principle and have so far developed virtually no significant protections of private affairs that differ from federal protections.").

55. *Mixton*, 478 P.3d at 1235.

56. *Id.* (quoting *Turley*, 59 P.2d at 316–17 (Ariz. 1936)).

57. *Id.* ("Although this court, when interpreting a state constitutional provision, is not bound by the Supreme Court's interpretation of a federal constitutional clause, those interpretations have 'great weight' in accomplishing the desired uniformity between the clauses." (quoting State v. Casey, 71 P.3d 351, 354 (Ariz. 2003))).

58. *Id.* "[T]he Clause expressly protects *both* 'private affairs' *and also* the home, indicating that it should protect a significantly broader set of substantive rights." Sandefur, *supra* note 54, at 723. However, "courts have largely neglected the linguistic and historical differences between the state and federal provisions." *Id.* This has hence resulted in Arizona citizens being forced to live with such inconsistency. *Id.* "Their courts, while giving lip service to the idea that the state constitution is more protective than federal law, apply it no more broadly in practice. At the same time, Washington case law that interprets language identical to the Arizona Clause *does* provide stronger protections than federal law." *Id.*

59. *Mixton*, 478 P.3d at 1235–36.

60. *Id.* at 1236.

Washington Constitution,[61] and the records of the Arizona constitutional convention contain no material addressing its intent."[62] Despite the silence in the constitutional convention record regarding intent, there are several "objections to extending state constitutional protections in other contexts beyond those recognized under the federal Constitution at the time."[63]

The Arizona Supreme Court has a "longstanding approach in applying the reasonable expectation analysis[64] to determine how to apply the Private Affairs Clause, and the central inquiry remains whether an asserted interest is private."[65]

IV. THE COURT'S REASONING

The court recognized "the utility in uniform state and federal criminal rules, procedures, and standards," and emphasized that "[t]he nature of cybercrime squarely implicates these interests and militates in favor of uniform federal and state search and seizure standards."[66] The court first looked to federal precedent, which it declined to depart from, and then reviewed state precedent, which it also declined to depart from. The court held, "[t]he unanimous federal court authority and the clear consensus of state courts, finding no privacy interest in IP addresses and ISP subscriber information, have affirmed their respective jurisdiction's popular consensus on this point as reflected in their laws permitting

61. *Id. Compare* WASH. CONST. art. I, § 7, *and* ARIZ. CONST. art. 2, § 8.

62. *Mixton*, 478 P.3d at 1236 (quoting Hart v. Seven Resorts Inc., 947 P.2d 846, 851 (Ariz. 1997)).

63. *Id.*

64. *See* State v. Lietzau, 463 P.3d 200 (Ariz. 2020); State v. Hernandez, 417 P.3d 207 (Ariz. 2018); State v. Jean, 407 P.3d 524 (Ariz. 2018); State v. Adair, 383 P.3d 1132 (Ariz. 2016); State v. Peoples, 378 P.3d 421 (Ariz. 2016); State v. Guillen, 223 P.3d 658 (Ariz. 2010) (en banc); State v. Peters, 941 P.2d 228 (Ariz. 1997) (en banc); Mazen v. Seidel, 940 P.2d 923 (Ariz. 1997) (en banc); State v. Jones, 917 P.2d 200 (Ariz. 1996) (en banc); State v. DeWitt, 910 P.2d 9 (Ariz. 1996) (en banc); State v. Apelt, 861 P.2d 634 (Ariz. 1993) (en banc); State v. Moorman, 744 P.2d 679 (Ariz. 1987); State v. Lucero, 692 P.2d 287 (Ariz. 1984) (en banc); State v. Fisher, 686 P.2d 750 (Ariz. 1984) (en banc); State v. Girdler, 675 P.2d 1301 (Ariz. 1983) (en banc); State v. Harding, 670 P.2d 383 (Ariz. 1983) (en banc); State ex rel. Ekstrom v. Justice of Court of State of Ariz. In and For Kingman Precinct No. 1, 663 P.2d 992 (Ariz. 1983) (en banc); State v. Jeffers, 661 P.2d 1105 (Ariz. 1983) (en banc); State v. Sanchez, 627 P.2d 676 (Ariz. 1981) (en banc); State v. Morrow, 625 P.2d 898 (Ariz. 1981) (en banc); State v. Jarzab, 599 P.2d 761 (Ariz. 1979) (en banc); State v. Walker, 579 P.2d 1091 (Ariz. 1978) (en banc); State v. Myers, 570 P.2d 1252 (Ariz. 1977) (en banc); State v. Cobb, 566 P.2d 285 (Ariz. 1977) (en banc); State v. Dugan, 555 P.2d 108 (Ariz. 1976) (en banc); State v. Miller, 520 P.2d 1115 (Ariz. 1974) (en banc); State v. Childs, 519 P.2d 854 (Ariz. 1974) (en banc) (all applying the "reasonable expectation of privacy" analysis).

65. *Mixton*, 478 P.3d at 1239.

66. *Id.* at 1242.

access to this information without court authorization."[67] It is the legislature who responds to the people—their wills and moral values.[68] Here, the federal and state laws reflected the views of citizens regarding the privacy interests in IP addresses and ISP subscriber information.[69] Both federal and state legislatures authorized law enforcement officials to obtain this information via subpoena, not a warrant.[70]

A. The Court's Reasoning with Federal Jurisprudence

Using *Carpenter* as a guidepost, and collectively consulting federal appellate court cases that pre-dated it, the court uniformly held "that the Fourth Amendment does not protect IP addresses and ISP subscriber information because such information falls within the exception created by the 'third party doctrine.'"[71] The court looked to the theory behind the holdings in *Smith v. Maryland*[72] and *United States v. Miller*,[73] where the focus was not on the act of sharing the information but rather the nature of the information or documents that were sought.[74] The court then looked to the Ninth Circuit's interpretation of "the de minimis privacy interests implicated in the non-content information generated by an IP address."[75] The Ninth Circuit stated:

> When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the

67. *Id.* at 1239 (citations omitted).
68. *Id.*
69. *Id.*
70. *Id.* at 1239, 1242 (noting the power of the "state to issue administrative subpoenas for subscriber information and other non-content service provider records based on a showing that 'the information likely to be obtained is relevant to an ongoing criminal investigation'" (quoting ARIZ. REV. STAT. § 13-3018(A), (C) (2023))).
71. *Id.* at 1231.
72. 442 U.S. 735 (1979).
73. 425 U.S. 435 (1976).
74. *Mixton*, 478 P.3d at 1232; *see also Smith*, 442 U.S. at 742 (holding that a defendant did not have a legitimate expectation of privacy in the numbers he dialed on his phone); *Miller*, 425 U.S. at 440 (holding that a defendant did not have a legitimate expectation of privacy in checks, deposit slips and statements from the bank because those documents were business records).
75. *Id.*

> basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith*[76] and *Katz*[77] drew a clear line between unprotected addressing information and protected content information that the government did not cross here.[78]

The court then analogized the subscriber information and IP addresses to the bank records and dialed telephone numbers that an individual voluntarily provides to third parties.[79] The court held, "an internet user voluntarily provides subscriber information and IP addresses to third-party ISPs and servers," but that such information did "not reveal the substance or content of the internet user's communication any more than the information affixed to the exterior of a mailed item."[80] To support this proposition, the court looked to nineteenth century precedent where the United States Supreme Court "held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties."[81]

The court confirmed that even after *Carpenter*, the federal appellate courts did not depart from prior precedent that did not allow the Fourth Amendment's warrant requirement to reach IP addresses and ISP

---

76. *See Smith*, 442 U.S. at 742 (holding that a defendant did not have a legitimate expectation of privacy in the numbers he dialed on his phone).

77. *See* Katz v. United States, 389 U.S. 347, 350–53 (1967) (holding that the warrantless monitoring of telephone conversations from a public telephone booth violated the Fourth Amendment).

78. *Mixton*, 478 P.3d at 1232 (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

79. *Id.*

80. *Id.* The statute "prohibits companies from disclosing 'contents of a communication,' but they may turn over non-content information like IP addresses, phone numbers, and physical addresses in response to a subpoena." *Id.*; *see* 18 U.S.C. § 2701.

81. *Mixton*, 478 P.3d at 1232 (quoting *Forrester*, 512 F.3d at 511).

subscriber information.[82] Despite not being bound by it, the Supreme Court of Arizona was persuaded by the federal appellate courts' interpretations and declined to depart from them.[83] The court sought to provide consistency to its citizens by providing "further predictability and stability of the law" and felt such could be accomplished by embracing the federal interpretations of federal constitutional provisions.[84]

Regardless, the nature of the information obtained in *Carpenter* was nothing like the information obtained here. Therefore, the Supreme Court of Arizona did not have to consult appellate cases and could have decided the issue by distinguishing *Carpenter*. "'IP addresses . . . are widely and voluntarily disseminated in the course of normal use of networked devices,' reveal only the approximate geographical location of a subscriber, and do not divulge the content of a user's communication."[85] "ISP subscriber information includes only data the subscriber voluntarily provides the ISP—typically the subscriber's name, address, and phone number."[86] The court stressed that while internet activity is necessary for "participation in a modern society," "internet users retain a measure of autonomy in masking their online activities."[87] The court stressed that the nature of an IP address and ISP subscriber information is fundamentally different from the CSLI in *Carpenter* because "CSLI is generated without an affirmative act by cell phone users."[88] The court emphasized this difference and focused on what the individual had to do, or cease doing, in order to continue participating in a modern society.[89] The cell phone user could only avoid having CSLI generated by "ceasing cell phone use entirely," while the internet user could avoid exposing the IP address and hence the ISP subscriber information by "masking their online activities."[90] The Supreme Court of Arizona emphasized the fact

82. *Id.* at 1232–33; *see, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (holding that IP addresses are outside the scope of *Carpenter* and hence subject to the third-party doctrine); United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (holding that post-*Carpenter*, ISP subscriber information falls within the scope of the third-party doctrine); *see also* United States v. Wellbeloved-Stone, 777 F. App'x 605, 607 (4th Cir. 2019) (per curiam) (declining to revisit *Bynum*'s holding that the Fourth Amendment did not protect subscriber information post-*Carpenter*); United States v. VanDyck, 776 F. App'x 495, 496 (9th Cir. 2019) (memorandum) (declining to revisit *Forrester*'s holding that the Fourth Amendment did not protect IP addresses and ISP subscriber information post-*Carpenter*).

83. *Mixton*, 478 P.3d at 1233.

84. *Id.*

85. *Id.* (quoting United States v. Weast, 811 F.3d 743, 748 (5th Cir. 2016)).

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

that internet users can take measures to mask their online activities if desired to make them private.[91] "[U]sers can anonymously access the internet via public and private services, such as public libraries and public WiFi networks at private businesses, or mask their online movements through proxy services like virtual private networks ("VPN")."[92] Therefore, if such measures are taken, the user's IP address could not be traced back to the user.[93]

The court rejected Mixton's theoretical argument that the government could use the IP address to trace an internet user's browsing history.[94] The court held that, not only was the argument based on an "unproven assumption," but there was no allegation that the State even made any derivative use of Mixton's IP address.[95] Rather, the sole issue before the court was "the constitutionality of the State's use of a federal administrative subpoena to obtain an IP address and ISP subscriber information" which was the only relevant authority conferred by the federal statute.[96] The court declined to hold that IP addresses and ISP subscriber information "implicate[d] the privacy interests embodied in the de facto omnipresent surveillance generated by 'detailed, encyclopedic' CSLI information."[97] The Supreme Court of Arizona held that "just as every federal court has held—the Fourth Amendment does not, in light of *Carpenter*, require a search warrant to obtain IP addresses and ISP subscriber information."[98]

B. The Court's Reasoning with the State's Jurisprudence

The court was first tasked with defining "private affairs" because the Arizona Constitution failed to define the phrase.[99] "In short, notably absent from the records of the constitutional convention is any objection to state use of a subpoena to obtain a business record to facilitate a legitimate criminal investigation of a corporate customer."[100] The court found that historical deliberations supported the view that the clause "militate[d] in favor of state access to certain corporate records held by third parties to aid criminal investigations."[101] As a result, the court held

91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.* at 1234.
96. *Id.*
97. *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).
98. *Id.*
99. *Id.* at 1234–35.
100. *Id.* at 1236.
101. *Id.* at 1237.

that the Private Affairs Clause did not protect IP addresses and ISP information and hence a warrant was not required to access it.[102]

The court refused to "discern the scope of the Private Affairs Clause in a vacuum," and instead emphasized how the reasonable expectation of privacy test was used to determine what protections the clause afforded to the people.[103] The court was troubled by the concept of "privacy," specifically as it related to "persons who transmit information to third parties, such as corporate entities, who are free to collect, maintain, and make collateral commercial use of it."[104] As a result, the court held that "any definition of 'privacy' must logically entail consideration of the nature of the information, and whether and how it is shared with others."[105] The definition of "privacy" must also include a reasonableness assessment of the asserted privacy interest "to determine whether it is, in fact, private."[106] The court held that a privacy interest can only exist "if the nature and use of the information is consistent with what is reasonably conceived as being private."[107] As a result, "the Private Affairs Clause protects a privacy interest in an IP address and ISP subscriber information only if society is prepared to accept such an expectation of privacy as reasonable."[108]

The court emphasized that "the technological reality" belied any such claim that a reasonable expectation of privacy existed in internet activity.[109] Inherent risks of using the internet include the ability to track and target the user. The very fact that websites are public and accessible through public search engines and that an internet user's online activity is tracked by third parties and then used to create targeted advertisements further supports this proposition.[110] "An investigation of third-party collection and use of internet users' activity revealed that numerous companies track online activity through the top 100 visited websites."[111] "Website operators also collect data on, and analyze, internet users' activities."[112] "For example, websites can use 'browser

102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.* at 1238.
108. *Id.*
109. *Id.*
110. *Id.*; *see also* Alicia Shelton, *A Reasonable Expectation of Privacy Online "Do Not Track" Legislation*, 45 U. BALT. L. F. 35, 41 (2014).
111. *Mixton*, 478 P.3d at 1238 (citing Andrew Couts, *Top 100 Websites: How They Track Your Every Move Online*, DIGITAL TRENDS (Aug. 30, 2012), http://www.digitaltrends.com/web/top-100-websites-how-are-they-tracking-you/).
112. *Id.*

fingerprinting' programs to gather 'innocuous bits of information, such as a browser's version number, plug-ins, operating system, and language, [so that] websites can uniquely identify ('fingerprint') a browser and, by proxy, its user.'"[113] Apps also have the ability to track users through website access.[114] "Websites also often employ 'cookies' that allow them to track internet users' browsing habits."[115] The court summarized that,

> [I]n this age of information sharing and inter-connectivity, "[m]ost of us understand that what we do on the [i]nternet is not completely private." Our "ubiquitous and pervasive internet use" that is "internet-connected, cloud-dependent, and app-reliant for personal communications, all manner of commercial transactions, 24-7 entertainment, and universal positional tracking," makes it hard to believe that anyone still retains "this largely antiquated notion" of "anonymity in their internet use."[116]

The court emphasized that if internet users are troubled by this truth, it is the legislature, not the courts that should "curtail use of such data."[117]

The court was unpersuaded by Mixton's argument that he had a reasonable expectation of privacy in his IP address and ISP subscriber information.[118] The court concluded that no reasonable expectation of privacy could exist when there is such "widespread and pervasive collection, analysis, and sharing of detailed internet activity, including website visitation" by third parties.[119] The court ultimately held that "when a person discloses non-content information to a third party, even under the earnest but misguided belief that the third-party will safeguard the information, such information sharing is fundamentally inconsistent with any notion of privacy and he forfeits a reasonable expectation of privacy in that information."[120]

---

113. *Id.* (alteration in original) (quoting Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 294–95 (2012)); *see also Privacy Mythbusting #4: I Can't be Identified Just by Browsing a Website. (If Only!)*, DUCKDUCKGO (July 11, 2017), https://spreadprivacy.com/browser-fingerprinting/.

114. *Mixton*, 478 P.3d at 1238.

115. *Id.* (citing *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 268 (3d Cir. 2016)).

116. *Mixton*, 478 P.3d at 1238 (alteration in original) (quoting State v. Mixton, 447 P.3d 829, 847 (Ariz. Ct. App. 2019)).

117. *Id.*

118. *Id.* at 1238–39.

119. *Id.* at 1238.

120. *Id.* at 1239.

The court further rejected the notion that IP addresses and ISP information revealed any type of intimate details regarding an individual's life.[121] Instead the court focused on the public nature of the information. The fact that an internet user's online activities are "routinely" released for other purposes negates any possibility of privacy.[122] The very nature of an IP address makes it similar in character to the return address an individual places on an envelope and deposits in the mail.[123] Furthermore, "IP addresses and ISP records belong to the third-party provider, not the subscriber."[124] Hence, they are not a "private affair."[125] The court concluded that,

> [A]n IP address and subscriber information are not "private affairs" under the Private Affairs Clause because the nature of the information is inconsistent with privacy: an internet user's expectation of privacy in such non-content information is unreasonable in light of the nature of the information; it is voluntarily shared with third parties; and such third parties own, and often engage in pervasive legal derivative use of, it.[126]

This is not to say that *any* information given to a third party then becomes that of the third party. This is only saying that use of a website that then creates an IP address does not create a property interest in that IP address. By virtue, the IP address is the ISP's because without an ISP, no IP address would exist because the user would not have access to the internet.

"[A]n IP address does not provide the state with an illicit view into an internet user's private affairs because, absent a warrant, the state is prohibited from examining the substance or content of a user's communications."[127] Theoretically, the only information the State could acquire through an IP address regarding an internet user's online activities "is the information a user discloses to a website and which the website subsequently chooses to publicize."[128] The court stressed that by

---

121. *Id.*
122. *Id.*
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.* at 1240.
127. *Id.*
128. *Id.*; *see, e.g.*, Kelly Weill, *Edits to Wikipedia Pages on Bell, Garner, Diallo Traced to 1 Police Plaza*, POLITCO (Mar. 13, 2015, 5:28 AM), https://www.politico.com/states/new-york/city-hall/story/2015/03/edits-to-wikipedia-pages-on-bell-garner-diallo-traced-to-1-police-plaza-087652 (explaining that reporters determined internet users at New York

virtue of voluntarily providing non-content information to a third-party provider, internet users do not have a reasonable expectation of privacy in the IP address or ISP subscriber information under the Arizona or Federal Constitution.[129] Both the third-party doctrine and the court's holding under the Arizona Constitution applied to non-content information—the contents of a communication were still protected.[130]

Despite the split in state courts regarding the applicability of the third-party doctrine, the court did not find persuasive Mixton's desire that it follow Washington's precedent but rather distinguished the cases he relied upon.[131] The court then looked to other state court holdings related to the third-party doctrine and found that, of the six that considered the issue, all[132] but one[133] determined that there was no reasonable expectation of privacy in an IP address and ISP subscriber information.[134]

The court also rejected Mixton's argument that the third-party doctrine would eradicate an internet user's right to anonymous speech.[135] The court held that an "assertion of a right to speak anonymously does not extend to anonymous distribution of illicit material without legal consequence."[136] There was a reason that the agents obtained the subpoena to gather the information. Mixton's "anonymous speech" was illicit child pornographic material—not something that either Arizona's Constitution or the Federal Constitution would protect. "Neither the federal administrative subpoena here, nor any provision under Arizona

---

Police Department headquarters edited Wikipedia pages because Wikipedia published the IP addresses of unregistered editors).

129. *Mixton*, 478 P.3d at 1240.

130. *Id.*

131. *Id.* at 1241. The court emphasized that Washington has not rejected the third-party doctrine but instead "examines the scope of its state constitution's protections on a case-by-case basis," and has not addressed the question as to "whether its constitution requires a warrant or court order to obtain an IP address and ISP subscriber information." *Id.* The Washington Constitution requires the court to determine "whether the State unreasonably intruded into the defendant's 'private affairs.'" *Id.* (quoting State v. Gunwall, 720 P.2d 808, 814 (Wash. 1986)). To determine whether the search was unconstitutional or not, the court considers the type of information revealed by the records and historically the type of protection afforded to such information in the past. *Id.*

132. *See* Radner v. State, 932 N.E.2d 755, 761–62 (Ind. Ct. App. 2010); State v. Leblanc, 137 So.3d 656, 661–62 (La. Ct. App. 2014); State v. Mello, 27 A.3d 771, 776–77 (N.H. 2011); State v. Delp, 178 P.3d 259, 264–65 (Or. Ct. App. 2008); State v. Simmons, 27 A.3d 1065, 1069–70 (Vt. 2011).

133. *See* State v. Reid, 945 A.2d 26, 33–37 (N.J. 2008) (holding that although there is a state constitutional right to privacy in ISP subscriber information, disclosure is allowed without notice to the subscriber and with a grand jury subpoena).

134. *Mixton*, 478 P.3d at 1242–43.

135. *Id.* at 1243.

136. *Id.*

law, would permit the state to acquire an IP address or subscriber information for a reason unrelated to a criminal investigation, and no federal or Arizona constitutional provision protects the anonymous distribution of child pornography."[137] Furthermore, he did not attempt to make his submission to the detective anonymous.[138] He did "not plausibly endeavor to elude identification."[139] "[H]e used a pseudonym as his personal identifier on his Kik account, he conveyed data files to others using his actual IP address."[140] Again he took no affirmative action to make his submission private. He completed no action that would have signified to anyone that he sought a reasonable expectation of privacy when he sat on his home desktop computer and sent an undercover detective child pornographic material from a username that could be linked to him.

"[A]n IP address functions as a return address for any internet-based computer activity."[141] Therefore, his use of a username was similar to him mailing a letter with his return address scribbled in the top left-hand corner.[142] "[A] letter sender is afforded no constitutional protections to the information on the outside of the envelope."[143] Privacy cannot be afforded if one knowingly discloses its origins.[144] If he truly wanted to protect his privacy and create a reasonable expectation of privacy, he could have used "publicly available computers, publicly available WiFi networks, or VPNs to mask his IP address."[145]

Despite Mixton's argument that the use of a subpoena is subject to abuse, the court determined that such argument was speculative as there was proper grounds to issue the subpoena.[146] The federal subpoena only allowed "an agency district director or special agent to obtain IP address and ISP subscriber information based upon an articulable belief that the information is relevant to investigation of a child-exploitation crime."[147] Obtaining any content-based information was not authorized by the

137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.* "Although we embrace the principle of anonymous speech and recognize its inestimable contribution to our liberty, authoring an essay under the pseudonym 'Publius' does little to preserve the author's anonymity if the exterior of the envelope containing the essay reads 'From the Office of Alexander Hamilton.'" *Id.*
145. *Id.*
146. *Id.* at 1244.
147. *Id.*

subpoena and remained subject to the warrant requirement.[148] Here, the state obtained Mixton's non-content information that included his IP address and ISP subscriber information "with a valid federal administrative subpoena, and could similarly have done so under Arizona law."[149]

The court ultimately held that "neither the Fourth Amendment to the United States Constitution nor article 2, section 8 of the Arizona Constitution requires law enforcement officials to secure a search warrant or court order to obtain IP addresses or subscriber information voluntarily provided to ISPs as a condition or attribute of service."[150] IP addresses and ISP subscriber information are not protected by the Fourth Amendment because of the third-party doctrine, and furthermore, are not considered a "private affair" under the Private Affairs Clause.[151] As a result, such information was lawfully obtained by the state via a valid federal administrative subpoena.[152]

V. AUTHOR'S ANALYSIS

In *Mixton*, the Arizona Supreme Court continued down the convoluted path of privacy. The court's analysis further identifies the struggles to be reckoned with as technology continues to challenge an individual's reasonable expectation of privacy.

The court correctly identifies that an individual has no reasonable expectation of privacy in an IP address or ISP subscriber information. "If you really feel that what you're doing online is that valuable to [the] government . . . , then you probably shouldn't be leveraging the Internet."[153] While it is not completely hopeless, regardless of how a user seeks to "overhaul" how online activities are conducted, there are no guarantees of privacy.[154] Use of the internet—also known as "cyberspace," the "infobahn," the "information superhighway," or the "World Wide Web"[155]—carries with it the inherent risk of exposure. No individual can have a reasonable expectation of privacy in something that by the very nature of its character is meant to expose. The very

148. *Id.*
149. *Id.*
150. *Id.*
151. *Id.*
152. *Id.*
153. Mark Smirniotis, *What Is a VPN and What Can (and Can't) It Do?*, N.Y. TIMES: WIRECUTTER (Mar. 3, 2021), https://www.nytimes.com/wirecutter/guides/what-is-a-vpn/.
154. *Id.*
155. *Internet*, THESAURUS.COM, https://www.thesaurus.com/browse/internet (last visited Aug. 17, 2023).

nature of the various terms used to describe the internet demonstrates that it is a large and highly trafficked area. Therefore, any individual that seeks privacy when using the internet should be said to have an *unreasonable* expectation of privacy.

Here, the Arizona Supreme Court concludes that Mixton should have had effective barriers to the intrusion.[156] The court suggests that he could have used public WiFi or accessed his home internet via VPN.[157] Therefore, only if Mixton had taken such measures should he have been granted a reasonable expectation of privacy. It logically makes sense that if such affirmative actions are taken a greater expectation of privacy exists. However, the question then arises: what if a user has a reasonable expectation of privacy in online activities, but is unaware that an IP address exists and that it could be traced back to him? In that case, the user could have his privacy invaded via a technological advancement that he is not aware of. Does it make a difference whether the user is informed or not? In the future, should the court consider whether or not the user is aware of the technological advancement? Can an individual have a reasonable expectation of privacy in something that he does not know exists? Or does that tie into the affirmative action, where only informed technology users are granted a reasonable expectation of privacy? If that is the case, then a reasonable expectation of privacy is not available to everyone. With the technological advancements that reach an individual on a daily basis, it cannot be said that the individual can competently remain abreast of the latest innovations. It is impossible to stay that informed. Should it be required that users are informed? If not, are they preyed upon because of their ignorance? Should the courts create a blanket exception that use of technology renders a reasonable expectation of privacy in anything obtained from it? Thereby, putting all individuals on equal footing, and truly and properly providing *everyone* with the privacy granted to them by the democracy they live in.

On one hand, consumers "trust" that technology can support them on a daily basis and believe that it is safe—but at what cost does this come? What do we unknowingly expose ourselves to by using technology? If we are not technologically aware, but still benefit from the use of technology, can it be said that we knowingly expose information? Do we ultimately sacrifice any privacy to use the internet? It appears that despite what society wants to believe, that answer is yes.

While the court correctly identifies that a citizen has no reasonable expectation of privacy in an IP address or ISP subscriber information, its analysis is flawed. No one, regardless of the affirmative actions taken,

156. *See generally* State v. Mixton, 478 P.3d 1227 (Ariz. 2021).
157. *Id.* at 1243.

has a reasonable expectation of privacy in an IP address or ISP subscriber information. By focusing on the affirmative actions that the individual *should have* taken in order to be granted a reasonable expectation of privacy, the court discreetly labels this individual as "common."

The court's analysis suggests that while the "common" individual has *no* reasonable expectation of privacy, perhaps the technologically savvy individual *may*—and most likely does—have a reasonable expectation of privacy in that same IP address and ISP subscriber information. Such a suggestion contravenes the protections that both the Fourth Amendment and Arizona Constitution grant to "the people"[158] of the United States and the "person[s]"[159] of the State of Arizona. These protections are afforded to *all* individuals, regardless of education or knowledge. Therefore, the court's insinuation that only informed persons in the State of Arizona could have a reasonable expectation of privacy in an IP address and ISP subscriber information only continues to further enhance the divide between the rich and the poor—to continue the disenfranchisement of the underprivileged. While "presidential candidates and the media generally attribute growing inequality to policies adopted by Congress and presidents, and to larger forces like automation . . . the . . . [courts] deserve[] a sizable share of the blame."[160] In theory, all individuals are equal when weighed on the scales of justice. "Justices of the Supreme Court and of many state courts take oaths to 'do equal justice to the poor and to the rich.'"[161] However, as the State of Arizona here demonstrates, that is not the case. The court's analysis effectively demonstrates "how the law discriminates in its level of protection for the rich and the poor."[162]

---

158. *Id.* at 1231.

159. *Id.* at 1234.

160. Adam Cohen, *Supreme Inequality: The High Court Has Been Siding with the Rich Against the Poor Since Nixon*, WASH. POST: OUTLOOK (Apr. 8, 2020), https://www.washingtonpost.com/outlook/2020/04/08/high-court-has-been-siding-with-rich-against-poor-since-nixon/.

161. *Equal Justice for the Poor, Too; Far Too Often, Money—or the Lack of It—Can Be the Deciding Factor in the Courtroom, Says Justice Goldberg, Who Calls for a Program to Insure Justice for All Americans*, N.Y. TIMES (Mar. 15, 1964), https://www.nytimes.com/1964/03/15/archives/equal-justice-for-the-poor-too-far-too-often-moneyor-the-lack-of.html.

162. Yevgeny Shrago, *The Fourth Amendment and Income Inequality*, HARV. L. & POL'Y REV. HLPR BLOG (Apr. 22, 2011), https://journals.law.harvard.edu/lpr/2011/04/22/the-fourth-amendment-and-income-inequality/. A three-judge panel of the Ninth Circuit held that police officer placement of a GPS tracker on a suspect's car without a warrant did not violate his Fourth Amendment rights "because he had no reasonable expectation of privacy for the underside of a car parked in his driveway." *Id.* The court reasoned that,

Many court decisions "define expectations of privacy in a way that makes people who are less well-off more likely to experience warrantless, suspicionless government intrusions."[163] The Supreme Court for example "has stressed that the Fourth Amendment is less likely to be implicated when a reasonable person would have taken more steps to ensure the privacy of the area searched."[164]

> Instead of declaring that one's living space and belongings are automatically entitled to constitutional protection—a conclusion that would seem to follow from the Fourth Amendment's explicit mention of "houses" and "effects"—the Court has signaled that the reasonableness of privacy expectations in such areas is contingent upon the existence of "effective" barriers to intrusion.[165]

"In other words, one's constitutional privacy is limited by one's actual privacy."[166] "That stance ineluctably leads to the conclusion that Fourth Amendment protection varies depending on the extent to which one can afford accoutrements of wealth such as a freestanding home, fences, lawns, heavy curtains, and vision- and sound-proof doors and walls."[167]

> [I]f a neighborhood child could place the tracker, so could the cops. Chief Judge Kozinski vehemently disagreed with the panel's "wayward child" standard, pointing out that such a rule gives one expectation of privacy for those wealthy enough to afford enclosed garage parking and another for those reduced to parking on the street. Chief Judge Kozinski accused the panel (and implicitly the entire judiciary) of "unselfconscious cultural elitism" for failing to understand the divergent situation.

Id. (quoting United States v. Pineda-Moreno, 617 F.3d 1120 (9th Cir. 2010)).

163. Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 400 (2003).

164. *Id.*

165. *Id.* at 400–01.

166. *Id.* at 401. "[P]eople who live in public spaces . . . and people who have difficulty hiding or distancing their living space from casual observers . . . are much more likely to experience unregulated government intrusions." *Id.* "[W]elfare workers may conduct warrantless, suspicionless inspections of benefit recipients' homes for the purpose of detecting welfare fraud." *Id.* at 402. "[A]djoining apartments may be searched even when only one of them is listed in the warrant, so long as the 'objective' facts make distinguishing between the two difficult, something that would never happen with two freestanding houses or even most well-designed (i.e., more expensive) apartments." *Id.* at 403. "[A] mobile vehicle—regardless of whether it is *likely* to move before a warrant can be obtained and regardless of whether it *is* a home—is associated with a lesser expectation of privacy than a house." *Id.* at 404. Under "container jurisprudence," "while consent to search a car clearly permits police to search a brown paper bag on the car floor, 'it is very likely unreasonable' to believe that the same consent would authorize search of a locked briefcase in the trunk, dictum that speaks for itself." *Id.*

167. *Id.* at 401.

"[T]he poor person's Fourth Amendment rights pale against the wealthier person's."[168] Such action or lack thereof sends a direct message to the poor: "they are unworthy of the government's respect."[169] "'Respect' is in part about status or esteem. Each person feels respected when he is treated as significant and of equal worth with every other person. Groups too struggle for equal status. But respect is also about inclusion, about being considered full members of the wider political community."[170]

Common suggestions on how to protect digital privacy include securing accounts, protecting web browsing, and using antivirus software.[171] However, most of these suggestions are not free or readily known to all individuals. Also, even if the individual decides to invest in such products or services, there are no guarantees that privacy is even effectively granted through their use.

Specifically with regards to web browsing, some commercially available privacy products "automatically direct[] [the user] to the secure version of a site when the site supports that, making it difficult for an attacker — especially [while] on public Wi-Fi at a coffee shop, airport, or hotel — to digitally eavesdrop on what [the user is] doing."[172] It is also suggested that a virtual private network is useful if a user frequently connects to public Wi-Fi because it adds an extra layer of security when browsing the internet.[173] "It can also provide some privacy from [the] Internet service provider and help minimize tracking based on [the user's] IP address."[174] However, all internet activity "still flows through the VPN provider's servers," therefore by using a VPN, the user is choosing to trust that company over the ISP to not store or sell the user's data.[175] While this "type of secure connection is a worthwhile investment for anyone who wants to wrap their data in an extra layer of privacy and security . . . . [it] is not a magic bullet for Internet security and . . . [will not make the user] anonymous online."[176]

Normally, the internet connection and data it carries goes from the user's computer to the "local Wi-Fi or network router, then bounces on through [the] ISP's network and off to the destination server . . .

168. *Id.* at 403.
169. Andrew E. Taslitz, *Respect and the Fourth Amendment*, 94 J. CRIM. L. & CRIMINOLOGY 15, 24 (2003).
170. *Id.* at 27.
171. Thorin Klosowski, *How to Protect Your Digital Privacy*, N.Y. TIMES: PRIV. PROJECT, https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy (last visited Aug. 17, 2023).
172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*
176. Smirniotis, *supra* note 153.

eventually returning with the requested data."[177] Theoretically, at any point along the way, someone could observe the data's journey from point of origin to destination.[178] However, with a VPN connection, all data found in the "Internet traffic between [the user's] computer and the VPN server" is encrypted, thus preventing another user from monitoring, viewing, or modifying any of that data.[179]

> Beyond the VPN server . . . [the user's] traffic mixes with traffic from other people on the same VPN—someone monitoring the connection to the destination server could see that [the user's] traffic came from the VPN server, but would [not] be able to know it was destined for [the user's] computer or device.[180]

When compared to individual websites, ISPs "have a much broader reach" when it comes to behaviors and types of information the ISP can "technically and legally" track and collect.[181] However, "few ISPs are transparent about how much information about their customers they store and for how long, instead relying on broad disclosures in their fine print."[182] An internet user's ISP at a minimum keeps track of every IP address assigned to the user for six to eighteen months.[183] "ISPs mostly use these records to respond to specific law enforcement requests, often to catch truly awful criminals. But no protections are in place to guarantee that it [is] the only way ISPs use these logs."[184]

In theory, because the user's data is encrypted as it passes through the ISP, a VPN will prevent the ISP from monitoring or logging that data traffic, and at best, the ISP would only "see gibberish passing" through to the VPN server.[185] However, regardless of this level of alleged security that a VPN could provide, there is no guarantee that a VPN could protect against government tracking.[186]

An individual's reasonable expectation of privacy should not depend on the affirmative actions of that individual. In other words, every individual should be provided the same privacy interests. There should not be varying degrees of privacy governed by an individual's ability to implement barriers. A person should not have to justify why he should

177. *Id.*
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.*
186. *Id.*

be given the same privacy interest that was afforded to his neighbor. The courts claim that every person is equal in the eyes of the law, or that every person is equal and granted the same rights under the constitutions, whether federal or state. While this is the "expressed statement" and illusion that the government sets forth, it is not what is being practiced. If the United States as a whole—which includes both the federal and state courts—wants to truly provide every person with adequate privacy, then such a right should be implemented. Courts should not dabble in adjusting privacy rights based on the facts before them—determining whether a six-foot fence affords a greater expectation of privacy than the five-foot fence. In order to halt this disparity of treatment, courts need to adjust their analysis. A reasonable expectation of privacy is something that should be afforded to everyone. Therefore, the homeless person on the streets should be afforded the same reasonable expectation of privacy as the wealthy person living on an island, surrounded by a moat and twenty-foot-high brick walls. Neither the United States Constitution nor the Arizona Constitution provide for a sliding scale of privacy. It is time that the courts adjust the analysis to determine whether something an individual expects to remain private is something that society as a whole—both rich and poor—can conclude is a reasonable expectation. It is time that the courts truly see all individuals as equal when standing before them. Everyone deserves the equal justice that is promised by the very documents that govern the states and country that they reside in.

> Respect requires recognizing that group identity is at the core of individual identity. The state must, therefore, embrace salient groups as equal partners in creating and implementing criminal justice policy. Group voices must be heard. But individuals must also be treated as unique, judged for what they do rather than what group they belong to. There is thus a healthy tension between group and individualized justice. Moreover, each citizen and his group must feel that the state intrudes upon their freedoms only when there is ample and trustworthy evidence of individual wrongdoing. Furthermore, all branches of government must recognize their constitutional obligation to express respect for citizens while enforcing the law.[187]

187. Taslitz, *supra* note 169, at 28.

VI. CONCLUSION

The Arizona Supreme Court properly held, "neither the Fourth Amendment to the Constitution of the United States nor article 2, section 8 of the Arizona Constitution requires law enforcement officials to secure a search warrant or court order to obtain IP addresses or subscriber information voluntarily provided to ISPs as a condition or attribute of service."[188] The State properly obtained the information with a valid federal subpoena and as such, the court affirmed Mixton's convictions.[189]

There is no reasonable expectation of privacy in an internet user's IP address or ISP subscriber information. Not for anyone—rich or poor. One cannot acquire a reasonable expectation in such information by implementing barriers. The affirmative action of the person is not something that is to be taken into consideration when effecting a reasonable expectation of privacy analysis. To allow such inquiry into the analysis would allow for "certain marginalized groups in our society [to] disproportionately bear the burden of state-imposed disrespect."[190] When there are differences, such as rich versus poor, "which group's view prevails will be a question of political morality."[191] However, "it will always be the case that examining minority viewpoints will better inform an otherwise unduly constricted constitutional analysis."[192]

Therefore, because both rich and poor are governed by the same constitutions and hence afforded the same rights, neither have a reasonable expectation of privacy while using the internet in the IP address or ISP subscriber information. Both groups do, however, have a reasonable expectation that, by living in today's society, they can expect to sacrifice a privacy interest by using the internet. By engaging in such use, there is no preservation of privacy. Each citizen must decide to either enjoy the ease that technology provides by sacrificing privacy; or refrain from participating in a modern society and enjoy the reasonable expectation of privacy that comes with it. Everyone has the choice, but as a word of caution—choose wisely.

188. State v. Mixton, 478 P.3d 1227, 1244 (Ariz. 2021).
189. *Id.* at 1244–45.
190. Taslitz, *supra* note 169, at 30.
191. *Id.*
192. *Id.*

***

***

Volume 75 Fall 2023 Issue 5

Rutgers University Law Review

Rutgers Law School