ARIZONA SUPREME COURT
ORAL ARGUMENT CASE SUMMARY

STATE v. WILLIAM MIXTON,
CR 19-0276-PR
247 Ariz. 212 (App. 2019)

PARTIES:

Petitioner/Cross-Respondent: The State of Arizona, Attorney General's Office

Respondent/Cross-Petitioner: William Mixton

FACTS:

In 2016, while investigating child exploitation, an undercover detective from the Tucson Police Department posted an advertisement on an online forum targeting users interested in child pornography. A user who identified himself as "tabooin520" responded and asked the detective to be added to a group chat on a messaging application, Kik Interactive Inc. ("Kik"). Soon after, the user sent images and videos of child pornography to the group chat and individually to the detective.

Working in collaboration with federal Homeland Security Investigations agents, the detective requested that the agents serve an administrative subpoena on Kik. Once they had done so, Kik gave the agents the user's IP address. The detective used this IP address to determine the user's internet service provider ("ISP"), available through public information. The federal agents served another subpoena on the ISP, requesting subscriber information for the IP address provided by Kik. The ISP disclosed Mixton's name, street address, and phone number. With this information, the detective obtained and executed a search warrant for the address where Mixton lived. During the search, police seized a cell phone, external hard drive, laptop computer, and desktop computer, all of which contained photos and videos of child pornography. The seized media included the messages, photos, and videos sent to the detective.

A grand jury, having been apprised of the evidence, indicted Mixton on twenty counts of sexual exploitation of a minor under fifteen years of age. Before trial, Mixton unsuccessfully moved to suppress the subscriber information and all evidence consequently seized from his home. The superior court heard oral argument and denied the motion. At trial, a jury convicted Mixton on all twenty counts, and the court imposed consecutive seventeen-year sentences for each count. Mixton timely appealed.

The Court of Appeals issued a 2-1 opinion upholding the convictions and sentences. Writing for the Majority, Judge Eppich noted that the Fourth Amendment of the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Because a search occurs when a reasonable expectation of privacy is violated, law enforcement officers usually must obtain a warrant supported by probable

cause. However, the Majority determined that Mixton had no recognizable Fourth Amendment privacy interest in his subscriber information or IP address. The Majority noted that in general, the Fourth Amendment does not protect information that a person reveals to a third party who then reveals it to the state, "even if the information is revealed [to the third party] on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *See United States v. Miller*, 425 U.S. 435, 443 (1976) (government's warrantless acquisition of customer's bank records held by bank did not violate Fourth Amendment); and *Smith v. Maryland*, 442 U.S. 735, 744-45 (1979) (warrantless collection of subscriber's phone calls did not violate Fourth Amendment). Therefore, under the "third party doctrine," law enforcement did not need a court-issued warrant to obtain the information.

The Majority continued its analysis under the Arizona Constitution. Article II, § 8 provides: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." The Majority then concluded that as a matter of first impression that the constitutional "private affairs" language gave Mixton a reasonable expectation of privacy, and therefore police could not use an administrative subpoena to obtain the information.

The Majority then examined whether the "good-faith" exception to the exclusionary rule applied. It determined that law enforcement officers were operating in good faith, and therefore A.R.S. § 13-3925(B) did not require the suppression of the evidence, and it affirmed Mixton's convictions and sentences.

In an opinion concurring in part, Judge Eckerstrom believed that the information was protected under the United States Fourth Amendment as determined in *Carpenter v. United States*, 138 S.Ct. 2206 (2018). In that case, the court found that an individual has a legitimate expectation of privacy in "cell-site location information" which is information collected from towers operated by cell phone service providers that connect to cellular telephones. The judge therefore believed that following *Carpenter*, law enforcement officers were required to secure a court-issued search warrant to acquire the IP address.

Judge Espinosa concurred in part, agreeing that no Fourth Amendment violation under the United States Constitution occurred in this case, and even if there was a violation, it would have been cured under both the federal and Arizona "good-faith" exceptions to the exclusionary rule.

However, he dissented, opining that there is no constitutional protection for ISP subscriber information under either the United States Constitution or the Arizona Constitution. He advised, "modern society is now internet-connected, cloud-dependent, and app-reliant for personal communications, all manner of commercial transactions, 24-7 entertainment, and universal positional tracking. Everyone utilizing cell phones, electronic tablets, laptop computers, smartwatches, and even modern automobiles... is subject to pervasive tracking 'cookies,' unseen meta-data in copiously shared photos and files, and constant geo-location." Therefore, because the third-party identifying information is widely accessible, a person has no reasonable expectation of privacy in the IP address.

ISSUES:

Petition for Review: Did the two-judge majority of the court of appeals err when it declared that article II, § 8 of the Arizona Constitution protects a right to privacy in an internet protocol ("IP") address and internet subscriber information, and held that federal agents investigating the electronic transmission of child pornography violated this novel constitutional right when they acquired this information—which revealed only Mixton's identity—through federally-authorized subpoenas?

Cross-Petition for Review: In light of *Carpenter v. United States*, 138 S.Ct. 2206 (2018), and the unique privacy interests at stake in this case, does the Fourth Amendment protect such information without application of the third-party doctrine?

DEFINITIONS:

Administrative subpoena: (Sometimes known as a "desk subpoena.") This is a written request for information by law enforcement officers that does not require the actions of a grand jury or a judge. If law enforcement officers have probable cause, they can also obtain information using a grand jury subpoena, a search warrant issued by a judge, or a court order.

IP address: Residential internet customers typically connect to the internet through an ISP. Each time a customer connects, the ISP assigns a unique identifier, known as an IP address, to the customer's computer terminal. Depending on the ISP, a customer's IP address can change. ISPs generally retain IP address information for one to three months. IP addresses are also conveyed to websites that an internet user visits, and administrators of websites can see the IP addresses of visitors to their sites. However, site administrators do not possess information linking a given IP address to a particular person. That information is held by the ISPs. *See United States v. Christie*, 624 F.3d 558, 563 (3d Cir. 2010).