No. _____

IN THE

Supreme Court of the United States

MARK STANFORD KATZMAN,

Petitioner

v.

THE PEOPLE OF THE STATE OF MICHIGAN,

Respondent

On Petition for Writ of Certiorari
To the Supreme Court of Michigan

PETITION FOR WRIT OF CERTIORARI

NOEL ERINJERI
Counsel of Record
ROCKIND LAW
36400 WOODWARD AVE., STE. 210
BLOOMFIELD HILLS, MI 48304
(248)-208-3800

QUESTION PRESENTED

Whether the Fourth Amendment permits the police to undetectably impersonate the owner of a phone via text message, and arrest another person by means of the ruse.

TABLE OF CONTENTS

APPENDIX

LIST OF PRIOR PROCEEDINGS

1. *People v. Mark Katzman*
   Oakland County (Mich.) Circuit Court
   Case# 2017-263-755-FH
   Trial/Verdict: June 7, 2018
   Sentenced: July 24, 2018

2. *People v. Mark Katzman*
   Michigan Court of Appeals
   Case# 345173
   Judgment: October 3, 2019
   Reported: 946 NW 2d 807 (2019)

3. *People v. Mark Katzman*
   Michigan Supreme Court
   Case# 160596
   Judgement: May 8, 2020
   Reported: 942 NW 2d 36 (2020)

TABLE OF AUTHORITIES

PETITION FOR A WRIT OF CERTIORARI

Petitioner Mark Stanford Katzman respectfully petitions for a writ of certiorari to review the Michigan Supreme Court's denial of leave to appeal the judgment of the Michigan Court of Appeals.

OPINIONS BELOW

The Michigan Supreme Court's denial of leave to appeal (Pet. App. 1a) is reported at 942 NW 2d 36 (2020). The Michigan Court of Appeals decision (Pet. App. 2a) is reported at 946 NW 2d 807 (2019).

JURISDICTION

The Michigan Supreme Court denied leave to appeal on May 8, 2020. (Pet. App. 1a.) This Court has jurisdiction pursuant to 28 U.S.C. § 1257(a).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment states in its relevant part that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]"

STATEMENT OF THE CASE

I. FACTUAL HISTORY

The facts are not in dispute. Mark Katzman was convicted of two counts of Delivery of Cocaine Under 50 Grams, which stemmed from an investigation of one Jessica Engisch by the Narcotics Enforcement Team (NET) of the Oakland County (Michigan) Sherriff's Department. During a series of undercover buys, Engisch made reference to a person named "Mark," who was her connection for various narcotics. On April 18, 2017, pursuant to a search warrant, the police searched Engisch's residence, arrested her, and seized her cell phone.

The next day, while Engisch was in jail, NET Detective Eric Buckberry was at the Sherriff's Department while another officer was examining the phone. A text message from a contact named "Mark" came in to Engisch's phone that said "Call me when ur (sic) up." Posing as Engisch, Det. Buckberry immediately responded to Mark by text, saying "Come by whenever you want." Detective Buckberry did not discuss his use of the phone with Ms. Engisch or otherwise seek her permission, nor did the warrant authorize such use.

Detective Buckberry and several other officers then staked out Engisch's residence, including two uniformed officers in a marked car. When Mark arrived, the uniformed officers detained him, and brought him to speak with Detective Buckberry. With the uniformed officers still present, Detective Buckberry read the Miranda warning and told Mr. Katzman that he was investigating the sale of cocaine to Jessica Engisch, and confirmed that his name was Mark. Mr. Katzman

confessed to delivering cocaine to Engisch on two occasions, and was arrested. Later that day, Katzman made a second confession at the Oakland County Jail during an interrogation by two other NET detectives. Based on those confessions and various lab reports, defendant was charged and convicted of two counts of Delivery of Cocaine.

II. PROCEEDINGS BELOW

A. Trial Court Proceedings

Petitioner waived his preliminary examination and filed a Motion to Suppress Evidence in the Oakland County Circuit Court (Hon. Rae Lee Chabot) asking that Katzman's statements to police (and all related evidence) be suppressed, arguing that:

1. The police's warrant to search Engisch's phone did not allow the police to use the phone;
2. By causing a fraudulent message to appear on Katzman's phone, the police had committed a trespass upon Katzman;
3. Katzman had a reasonable expectation of privacy in the contents of his own phone and his communications with Ms. Engisch; and
4. That all of the above violated Katzman's rights against unreasonable search and seizure as defined by the Fourth Amendment of the federal constitution and Article I, Section 11 of the Michigan Constitution.

Judge Chabot disagreed, holding that:

> "I think the police have the right to take whatever the[y] find under the search warrant and **explore**[1] it for the purposes that the search warrant was. I really don't think there's any reasonable expectation of privacy in such a setting." (emphasis added)

During a bench trial on June 7, 2018, defendant renewed his request to suppress the evidence. Judge Chabot declined to do so and found the defendant guilty of both counts. Katzman was sentenced to one year of probation on July 24, 2018.

B. Appellate Proceedings

Petitioner appealed by right to the Michigan Court of Appeals. Following briefing and oral arguments, the Michigan Court of Appeals issued a published opinion on October 3, 2019, affirming the trial court's denial of Petitioner's motion to suppress.

Petitioner then applied to the Michigan Supreme Court for leave to appeal. The Michigan Supreme Court denied such leave without oral argument on May 8, 2020. This petition for a writ of certiorari timely follows, pursuant to this Court's order of March 19, 2020 (extending the filing deadline for petitions for certiorari in light of the COVID-19 crisis).

REASONS FOR GRANTING THE PETITION

Are the traditional rights against search and seizure applicable in the digitial world? As technology advances ever more quickly, the law, often as not, tries desperately to keep up. In this case, the conclusion of the trial court and the Michigan Court of Appeals that a search warrant for one phone allowed the police to

---

[1] Petitioner notes that "explore" is a synonym for "search." Sgt. Buckberry's conduct went far beyond mere "exploration."

do much more than search—it allowed the police to use that phone to impersonate its owner (without the owner's consent) via text message in order to seize another citizen.

The constitutional danger is clear—there was no way to know that Petitioner was communicating with the police, as opposed to his associate. Because of the nature of modern communications, to allow such conduct is to give the government *carte blanche* to invade every facet of our digital lives. Petitioner therefore urges this Court to further refine its Fourth Amendment jurisprudence to apply to the Digital Age.

At least four states have considered the Fourth Amendment issues that are implicated when the police impersonate co-defendants (or other associates of the defendants) via text message. In the instant case, the Michigan Court of Appeals found that the defendant lacked standing to challenge the search of Engisch's phone. The New Jersey Superior Court (Appellate Division) held in *State of New Jersey v. Hreha*, A-2744-19T3 (2020) (unpublished case) that the defendant also lacked standing to make a Fourth Amendment challenge to the search of another person's phone, and that the police impersonation was "of no moment." Id. at 20. The Oregon Court of Appeals held in *State of Oregon v Carle,* 337 P. 3d 904 (2014), that "defendant had no reasonable expectation of privacy in the digital copy of the text message that police found on Duane's [the person impersonated] phone." *Id.* at 911. Finally, the Washington Supreme Court found for the defendant in *State of Washington v. Hinton*, 319 P. 3d 9 (2014) but made the decision based on Article I,

Section 7 of the Washington Constitution, without addressing the federal Fourth Amendment. *Id.* at 12.

This Court should adopt the holding of the Washington Supreme Court to the issue of police impersonation via text message:

> "Forcing citizens to assume the risk that the government will confiscate and browse their associates' cell phones tips the balance too far in favor of law enforcement at the expense of the right to privacy." Id. at 17.

To the extent that the Michigan, New Jersey, and Oregon cases hold the opposite, jurisprudence on the topic is evolving in a positively Orwellian direction—**it requires citizens to assume that any electronic communication is potentially a fraudulent communication from the government.**

Whether examined under the "reasonable expectation of privacy" analysis of *U.S. v. Katz,* 389 U.S. 347 (1967); or the more recent "trespass" analysis of *U.S. v. Jones,* 565 U.S. 400 (2012), this cannot be.

I. By causing a fraudulent message to appear on Katzman's phone, the police trespassed upon Katzman's digital property.

The renewed use of the "trespass test" when analyzing search and seizure issues is a relatively recent development. In *U.S. v. Jones,* 565 U.S. 400 (2012), the government placed a Global Positioning System (GPS) tracker on a suspect's vehicle without obtaining a proper warrant. The *Jones* court held:

> "It is important to be clear about what occurred in this case: **The Government physically occupied private property for the purpose of obtaining information.** We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted. (*Id.* at 404-5) (emphasis added)

In the current case, the government did the same thing—by causing a fraudulent message to appear on Katzman's phone, they occupied Katzman's (digital) private

property. The fact that the property in question happened to be his phone instead of his home or vehicle does not alter the fact of the trespass: "With all [modern cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Riley v. California*, 573 U.S. 373 (2014).

In the opinion below, Michigan Court of Appeals rejected the concept of a digital trespass, reasoning that

> "the text message amounted to an electronic communication that did not occupy an actual physical presence on defendant's personal property. Because the text message that defendant received from law enforcement did not constitute a physical trespass on his effect, defendant's reliance on *Jones* is misplaced. The proper inquiry is whether defendant had a reasonable expectation of privacy. See id., 411[2] ("Situations involving the transmission of electronic signals ...[are] subject to" the reasonable expectation of privacy test." (Pet. App. 6a).

The Michigan Court of Appeals excerpt from Jones is somewhat strained. Here is what *Jones* actually had to say about the topic (as opposed to the Michigan Court of Appeals summary of what Jones said):

> The concurrence faults our approach for "present[ing] particularly vexing problems" in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. Post, at 9. We entirely fail to understand that point. **For unlike the concurrence, which would make *Katz* the exclusive test, we do not make trespass the exclusive test.** Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.
>
> In fact, it is the concurrence's insistence on the exclusivity of the Katz test that needlessly leads us into "particularly vexing problems" in the present case. [...] **It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.**" *Jones* at 412. (emphases added)

[2] Referring to *Jones*.

In other words, the Michigan Court of Appeals read that passage of Jones to mean that this Court had established a bright-line rule that electronic transmission of signals was subject only to Katz's reasonable expectation of privacy analysis. On the contrary, a complete reading of that section of *Jones* makes it clear that a) the application of either test to electronic signals is still an open question, at least before this Court; and b) that neither Katz's reasonable expectation of privacy test nor Jones's trespass test predominates over the other. "[A]s we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Jones* at 409 (emphasis original).

In short, the Michigan Court of Appeals misread *Jones*. Then, based on that misreading, it refused to apply the trespass analysis to the facts of this case. That is an error that this Court should now correct.

To be sure, the police did cause a physical alteration to Katzman's phone when they sent the fraudulent message, at a micro level. By causing the text message data to appear in Katzman's phone's microchips, and certain pixels to be displayed on the screen, they remotely trespassed upon the phone by manipulating it without Katzman's consent. In other words, there was an underlying *physical* trespass in the physical world.

Conceptually, however, it makes more sense to consider the phone as Katzman's *digital* private property. Just as in the physical world, a citizen has cognizable property interests in the part of his life that is online, upon which the state may not trespass. Consider a hypothetical situation: the police search

Engisch's residence pursuant to a valid search warrant, where they discover her personalized stationery and a key to Katzman's house. Writing a note to Katzman and forging Engisch's signature, they use the key to surreptitiously enter Katzman's house and leave the note on his kitchen table, luring him into a sting. If the police's actions in this example violate the Fourth Amendment in the physical world (and they do), their actions in this case must also be illegal in a digital context.

So far as Petitioner is aware, the idea of a "digital trespass" has not been adopted in any Court. But while the argument may be novel, it is a natural consequence of how we think (and act) in our online lives. A citizen's phone, text message conversations, social media accounts, and the like are considered to be under one's exclusive control, in the same way as one's home or vehicle. And just like the home, a person has the right to exclude outsiders from any or all of those virtual "spaces." When the police surreptitiously enter those spaces for their own purposes without consent, they have trespassed upon that space.

This is not a radical expansion of trespass theory:

> "Trespass law has never been confined to when a person physically intrudes on another's private property—it is sufficient that the trespasser has physical or legal control over the intrusion. For example, at common law, a trespass by livestock was an almost strict liability tort by the livestock owner—if Smith's cow went onto Jones's property and injured Jones, Smith could be liable even if he was not negligent in confining the cow and never set foot on Jones's land. Trespass cases due to pollution are common; in many of these cases the trespasser never set foot on the contaminated land. If an undirected animal or cloud of pollution interacting with another's property can be a trespass, it is hard to imagine why a directed wireless signal interacting with another's property would be any less of a trespass."
>
> Hannah Cook, (Digital) Trespass: What's Old Is New Again 94 Denv. L. Rev. Online 1 (February 23, 2017), available at SSRN: https://ssrn.com/abstract=2923211

In other words, what makes something a trespass is not whether it happens in a particular place or to a particular item, or even if it's accomplished by a particular person. Phrased simply, a trespass occurs when one's exclusive control of his property is violated. That is what happened here, and that is what the Fourth Amendment is meant to guard against—and this Court should read its precedent in *Jones* broadly enough to do so.

II. Katzman had a reasonable expectation of privacy in his own phone.

In addition to trespassing on Katzman's phone, the police violated Katzman's reasonable expectation of privacy in **his own phone** when they sent the fraudulent message from the police station.

In the opinion below, the Michigan Court of Appeals disagreed, holding that

> "Here, consent is irrelevant because the police officers had a valid search warrant for Engisch's cell phone. Furthermore...the police officers here did not use defendant's cell phone at all. (Pet. App. 5a, fn 3).

In this footnote, the Court of Appeals makes two mistakes. First of all, while the police may have had a search warrant for Engisch's phone, they had no such warrant for Katzman's phone. More importantly, the police did use Katzman's phone—by causing the fraudulent message to appear there, they manipulated Katzman into an arrest, and ultimately a confession.

Consider situations where a defendant sells drugs to an undercover officer, or makes incriminating statements over the phone (i.e., a voice call), either to an officer or to a known associate (with a police officer listening with the associate's knowledge, but not the defendant's). In that case, the defendant assumes the risk

that his associate will betray him, or that the person he is talking to is not who he says he is. In either case, though, the distinction from the case at bar is that someone *besides the police* has surrendered their privacy interest—either the defendant himself, by speaking to an unknown party; or the associate, by agreeing to cooperate with the police. In the present case, the police commandeered Engisch's phone without consulting with anyone, and impersonated her in a way that was undetectable.

That this undetectable impersonation is of someone known to the defendant is the critical point, because of the nature of online communications. Consider a fairly standard scenario, in which the police pose as a minor in order to ferret out pedophiles or purveyors of child pornography. While the police are still concealing their identities, the target of the investigation has the opportunity to refuse to break the law at the behest of a stranger. But impersonating a friend and known associates subverts that opportunity—it is axiomatic that we speak differently, act differently, and react differently when we are among friends.

Long ago, this Court has recognized this distinction in a very similar context. In *Gouled v. U.S.,* 255 U.S. 298 (1921), a business associate of the defendant pretended to make a friendly visit to the defendant's house, at the direction of government agents. The associate secretly removed documents from Gouled's home office, which were used to prosecute him. This Court held that

> [W]hether entrance to the home or office of a person suspected of crime be obtained by a representative of any branch or subdivision of the Government of the United States by stealth, or through social acquaintance, or in the guise of a business call, and whether the owner be present or not when he enters, any search and seizure subsequently and secretly

> made in his absence, falls within the scope of the prohibition of the Fourth Amendment[.] Id. at 306.

A century later the police have perpetrated a similar ruse. Only instead of using Jessica Engisch, the person, the police used "Jessica Engisch," the cell phone account, to enter illegally Katzman's phone. If anything, the instant case is worse than *Gouled,* since the police had the willing participation of neither Katzman nor Engisch. While police technology may have become more sophisticated, the constitutional principle (and its violation) remain the same.

In fact, given the state of technology, the police do not even need a person's phone in order to impersonate him—they could simply hack into his email, instant messenger service, etc., by "spoofing" and use the resulting communications against a co-defendant. By the Michigan Court of Appeal's logic (shared by the appellate courts in Oregon in New Jersey), this is perfectly acceptable. But carrying that logic to its conclusion, if the police impersonated a defendant's doctor, or his priest, or his wife; and by that deception obtained incriminating statements, there would be no Fourth Amendment violation. Such an absurd result should not be countenanced.

Rather, Petitioner urges this Court to adopt the reasoning of the Washington Supreme Court in *Hinton.* While *Hinton* was decided under Washington state law, Petitioner submits that the Fourth Amendment generally, and *Katz* specifically, compels the same result at the federal level:

> "Given the realities of modern life, the mere fact that an individual shares information with another party and does not control the area from which that information is accessed does not place it outside the realm of article I, section 7's[3] protection. [...] The risk that one to whom we impart private information will disclose it is a risk we 'necessarily assume whenever we

[3] Washington's version of the Fourth Amendment

> speak.' **But that risk should not be automatically transposed into an assumed risk of intrusion by the government."** *(Hinton*, 319 P. 3d at 15-16) (emphasis added)

The *Hinton* court concluded that

> Unlike a phone call, where a caller hears the recipient's voice and has the opportunity to detect deception, there was no indication that anyone other than Lee possessed the phone, and Hinton reasonably believed he was disclosing information to his known contact. [...] Forcing citizens to assume the risk that the government will confiscate and browse their associates' cell phones tips the balance too far in favor of law enforcement at the expense of the right to privacy. Id. at 16.

In short, while the police are sometimes allowed to use deceptive tactics, the target of such tactics should have a fair chance of detecting that deception, and a fair chance to back out.

The opinion below held that "Once defendant sent the initial text message to Engisch's cell phone, he no longer had an expectation of privacy in the text message exchange." (Pet. App. 5a.) However, the message exchange in question was initiated when Katzman texted Engisch "call me when [you're] up." Katzman's expectation of privacy in his message did not terminate when he sent them—it terminated when the message was received by Engisch. To analogize to the physical world, one's expectation of privacy in a mailed letter does not terminate when the letter is deposited in the recipient's mailbox. It terminates when the recipient actually opens the letter. If the police take the letter out of the mailbox before the recipient reads it, they have violated the *sender's* reasonable expectation of privacy. By interposing himself in the middle of what was supposed to be a private conversation, Detective Buckberry violated *Katzman's* expectation of privacy even though Buckberry was using Engisch's phone. This is because (as stated before) Katzman thought was communicating with Engisch, not a stranger.

The distinction is subtle, but important. If Engisch had turned over her phone to the police and allowed them to use it, Katzman would be out of luck. Likewise, if Katzman had revealed incriminating information to someone that he knew was *not* Engisch, there would be no constitutional violation. The Michigan Court of Appeals implies the distinction is irrelevant. If allowed to stand, the practical result would be that every citizen would have to assume every single digital communication (text, email, social media, etc.) might not be from the putative sender, but a fraudulent communication from the government.

Such a dystopia was not possible before electronic communications became ubiquitous. Written communications could be identified as forgeries by the handwriting. Telephone impersonators could be identified by their voice. And even with media that lent themselves to the possibility of such fraud (such as telegrams), it was not economical or practical for the police to employ deceptive tactics in that way. Nowadays, however, such intrusion by the police is (technically speaking) a trivial matter. But just because police can do something doesn't mean that they should—and this Court should faithfully apply the Fourth Amendment and hold that they can't.

III. Katzman has standing to challenge this violation of his Fourth Amendment rights.

The Michigan Court of Appeals merged the reasonable expectation of privacy question with the question of standing, holding that since Katzman did not have a reasonable expectation of privacy in Engisch's phone, he had no standing to challenge the fraudulent message. (Pet. App. 5a). The Court of Appeals missed the

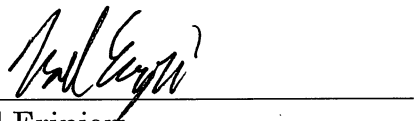
mark, in that Defendant-Appellant is not asserting his Fourth Amendment rights over Engisch's phone, but over his own. As the police both committed a digital trespass and violated his reasonable expectation of privacy in his phone, and his message, it necessarily follows that he has standing to claim the protection of the Fourth Amendment.

CONCLUSION

Defendant-Appellant urges this Court to conclude that the police cannot exceed the scope of their search warrant and abuse their authority in this way. The Court should reaffirm an ancient principle and apply it to a new technology—a search warrant only permits a search, nothing more. The petition for a writ of certiorari should be granted.

September 25, 2020

Respectfully submitted,



Noel Erinjeri
Counsel of Record
ROCKIND LAW
36400 Woodward Ave., Ste. 210
Bloomfield Hills, MI 48304
248-208-3800