PRIVACY RIGHTS — FEDERAL WIRETAP ACT — SIXTH CIRCUIT FINDS NO REASONABLE EXPECTATION OF PRIVACY IN ORAL COMMUNICATIONS TRANSMITTED VIA POCKET DIAL. — *Huff v. Spaw*, 794 F.3d 543 (6th Cir. 2015).

The Federal Wiretap Act[1] (Title III of the Omnibus Crime Control and Safe Streets Act of 1968), which governs when interception of oral and wire communications is permissible,[2] was not drafted with pocket dials[3] in mind. This statute aims to prevent unlawful government interceptions of private individuals' communications, while simultaneously empowering law enforcement agents to deploy wiretap technologies in legitimate ways.[4] Yet Title III's application also reaches some communications intercepted by private parties.[5] Recently, in *Huff v. Spaw*,[6] the Sixth Circuit held that an individual whose pocket dial was intercepted and recorded by a private party enjoyed no reasonable expectation of privacy and therefore could receive no civil remedy under Title III. Though this conclusion accords with precedent, it may clash with privacy expectations by allocating contemporary privacy risks in unexpected ways. A better standard would reflect private citizens' daily reliance on technology and balance the apportionment of responsibility by also taking into account the reasonableness of the defendant's actions.

In fall 2013, James Huff (Huff), his wife Bertha Huff, and his colleague Larry Savage traveled to Italy for a business conference.[7] Huff was chairman of the Kenton County Airport Board (Board), which manages the Cincinnati/Northern Kentucky International Airport (CVG).[8] After a meeting at the conference, Huff and Savage adjourned to an outdoor balcony at the hotel and discussed CVG personnel matters — including possible replacement of CVG's CEO.[9] Sometime during this conversation, Huff called Carol Spaw, a senior

---

[1] Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012), 47 U.S.C. § 605 (2012)). Except as specifically provided, *see* 18 U.S.C. § 2511, the statute makes it unlawful to "intentionally intercept[] . . . any wire, oral, or electronic communication," *id.* § 2511(1)(a).

[2] *See* Gelbard v. United States, 408 U.S. 41, 47–52 & nn. 6–10 (1972) (summarizing Title III's legislative history and emphasizing privacy interests at stake in regulating interception of wire and oral communications).

[3] A pocket dial ("butt dial") is "the accidental placement of a . . . call while . . . [the] phone is in the owner's pocket." *Pocket Dialing*, WIKIPEDIA, http://en.wikipedia.org/wiki/Pocket_dialing [http://perma.cc/8TS9-LKZ2].

[4] *See Gelbard*, 408 U.S. at 48.

[5] Indeed, the text refers to "any person" — not just state actors. 18 U.S.C. § 2511(1).

[6] 794 F.3d 543 (6th Cir. 2015).

[7] *Id.* at 545.

[8] *Id.*

[9] *Id.*

executive assistant to CVG's CEO who also served as a liaison to the Board.[10] Unable to reach her, Huff hung up and placed his iPhone in his jacket pocket.[11] Savage then reached Spaw using his own cellphone, after which the men continued to discuss CVG personnel matters for the better part of an hour, attended another meeting, and then returned to their respective hotel rooms, where Huff met his wife, Bertha, and recounted his conversation with Savage.[12] Unbeknownst to Huff, his iPhone had dialed Spaw's office line soon after he had put the phone in his pocket.[13] Spaw had answered and said "hello"; receiving no reply, Spaw enlisted a coworker to discern what the men were discussing.[14] Spaw grew concerned that the men were unlawfully discriminating against the CEO and started to take notes until approximately eighty-six minutes into the transmission, when she began using a company iPhone to record the call.[15] At eighty-nine minutes, Huff realized that a pocket dial had occurred.[16] After the transmission ended, Spaw typed up her notes, hired a company to improve the recording, and shared this information with others on the Board.[17]

In late 2013, the Huffs filed a complaint against Spaw in the United States District Court for the Eastern District of Kentucky, alleging intentional interception, disclosure, and use of wire and oral communications in violation of Title III.[18] The trial court entered summary judgment for the defendant.[19] Since an "oral communication" receives Title III protection only if it was made with an objectively reasonable expectation that it would not be intercepted, the court's determination that, as a matter of law, Huff had no such expectation meant that no Title III violation could have occurred.[20]

---

[10] *Id.* Spaw was located in Kentucky, and Huff sought help making a dinner reservation. *Id.* at 545, 547.

[11] *Id.* at 545.

[12] *Id.* at 545–46.

[13] *Id.* at 545.

[14] *Id.* at 546.

[15] *Id.*

[16] *Id.* Huff testified that he ended the call immediately, but cellphone records indicated the transmission lasted for two more minutes. *See id.*

[17] *Id.*

[18] The Huffs' complaint alleged violations of 18 U.S.C. § 2511(1)(a), (b), (c), and (d) and requested both a declaratory judgment and a civil damages remedy. *See* Verified Complaint with Jury Demand at 5–7, 10, Huff v. Spaw, 995 F. Supp. 2d 724 (E.D. Ky. 2014) (No. 2:13-cv-00212). The Huffs also filed privacy claims under Kentucky state law. *See id.* at 7–9.

[19] *See Huff*, 995 F. Supp. 2d at 726. The court emphasized that — given the ubiquity of pocket dials and the Huffs' awareness of this risk — the plaintiffs lacked a reasonable expectation of privacy in the call. *See id.* at 732.

[20] *Id.* at 731–32, 734. Because Huff was aware of the risk of pocket dials, the court found that "he knew he was carrying a device that was capable of giving a third party audible access to his conversations without him ever knowing" and so had no reasonable expectation of privacy while carrying his phone. *Id.* at 732.

The Sixth Circuit partially affirmed the district court. Writing for the unanimous panel, Judge Boggs[21] found that James Huff lacked a reasonable expectation of privacy to support his Title III claim, but reversed and remanded to determine whether Spaw's actions represented an interception of Bertha Huff's oral communications in contravention of Title III.[22] The court began[23] its analysis with the text of Title III,[24] which establishes that "a person engages in protected oral communication only if he exhibited 'an expectation of privacy that is both subjectively and objectively reasonable.'"[25] Given the statute's substantial similarity to the "reasonable-expectation-of-privacy" test articulated in Justice Harlan's concurrence in *Katz v. United States*,[26] which courts use to determine whether Fourth Amendment protection applies,[27] the court drew upon *Katz*'s two-pronged standard to assess the Title III claims.[28] Under the *Katz* test, for a person to have a reasonable expectation of privacy, she must have "exhibited an actual (subjective) expectation of privacy and . . . the expectation [must] be one that society is prepared to recognize as [objectively] 'reasonable.'"[29]

Recognizing that "the division of labor between these two parts is ill-defined in the Title III context,"[30] the court invoked Sixth Circuit precedent to clarify the test. Notably, the Sixth Circuit[31] "limit[ed] the subjective part to the issue of whether a person *held an internal belief* in an expectation of privacy from interception."[32] It asserted that any inquiry into internal belief — the subjective prong of the test — was

---

[21] Judge Boggs was joined on the panel by Judge Cook and District Judge Quist, sitting by designation from the Western District of Michigan.

[22] *Huff*, 794 F.3d at 552, 554. The Sixth Circuit also determined that, because Bertha Huff "made statements in the privacy of her hotel room, was not responsible for exposing those statements to an outside audience, and was . . . unaware of the exposure, she exhibited an expectation of privacy." *Id.* at 554.

[23] As a threshold matter, the court found that it had jurisdiction, even though Title III does not have extraterritorial reach, because the relevant location was Covington, Kentucky, where Spaw "used a device to acquire the contents of [the] conversations." *Id.* at 547.

[24] Title III defines an "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2) (2012).

[25] *Huff*, 794 F.3d at 548 (quoting Dorris v. Absher, 179 F.3d 420, 425 (6th Cir. 1999)).

[26] 389 U.S. 347 (1967).

[27] *See id.* at 361 (Harlan, J., concurring). *Katz* held that law enforcement officers who intercepted an individual's phone conversation by attaching an electronic recording device to the exterior of the phone booth from which he placed his call had engaged in a "search" for purposes of Fourth Amendment analysis because the government's activities "violated the privacy upon which [the individual] justifiably relied." *Id.* at 353 (majority opinion).

[28] *See Huff*, 794 F.3d at 548–49.

[29] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[30] *Huff*, 794 F.3d at 549.

[31] The court distinguished its application of *Katz* from other courts' approaches, but ultimately concluded that its analysis was functionally equivalent. *See id.* at 549–50.

[32] *Id.* at 549 (citing Dorris v. Absher, 179 F.3d 420, 425 (6th Cir. 1999)).

properly subsumed by objective analysis of whether an individual "exhibited" an expectation of privacy.[33] The only relevant inquiries under Title III, then, come from the objective prong of the test: whether a person "*exhibit[ed]* an intention to keep statements private" and whether the person's expectation was reasonable.[34]

The court found that Huff did not "exhibit" the requisite privacy expectation.[35] Invoking Fourth Amendment "plain view" doctrine,[36] it determined that Huff "exposed" his communications through the pocket dial in a way that belied a protected privacy interest.[37] Critically, such exposure need not be intentional; it "can be the inadvertent product of neglect," akin to when a "homeowner neglects to cover a window with drapes."[38] Huff's failure to take affirmative action to secure his phone after terminating the call was thus dispositive. He should have known that pocket dials might allow others to intercept communications.[39] Since he did not take steps to prevent such interceptions, such as locking the phone or using a downloadable application that blocks pocket dials, he lacked a reasonable expectation of privacy.[40]

It is understandable that the Sixth Circuit applied *Katz*'s two-pronged Fourth Amendment test in a Title III suit involving two private parties; indeed, both legislative history and jurisprudential practice suggest that this is the legally proper analysis.[41] But the reasonable-expectation-of-privacy test initially emerged in a very different relational and technological context. *Katz*'s standard aimed to protect privacy interests against illicit state searches and seizures under the Fourth Amendment, not interception of a communication by another

---

[33] *See id.* at 549–50 ("[T]he only relevant inquiries are the two objective subparts: (1) whether a person exhibited an expectation of privacy and (2) whether that expectation was reasonable." *Id.* at 550.).

[34] *Id.* at 550. The court assessed the Huffs' privacy interests independently. *Id.*

[35] *Id.*

[36] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[O]bjects, activities, or statements that [a person] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

[37] *See Huff*, 794 F.3d at 550 ("Because James Huff placed the pocket-dial call to Spaw, he exposed his statements to her and therefore failed to exhibit an expectation of privacy [in them].").

[38] *Id.*

[39] The court highlighted Huff's acknowledged familiarity with the risk of pocket dials, which he admitted at his deposition. *See id.* at 552.

[40] *Id.* Having made this determination concerning James Huff, the court distinguished Bertha Huff's privacy expectations and reversed the district court's holding as it pertained to her, remanding only this portion of the suit for further proceedings. *See id.* at 552–56.

[41] Title III's statutory history indicates congressional intent to align the definition of "oral communications" with the constitutional standards from *Katz*. *See* S. REP. NO. 90-1097, at 60 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2178. Other courts have conducted similar analyses. *See Huff*, 794 F.3d at 548.

private individual.[42] And the *Katz* doctrine developed at a time when private individuals did not routinely carry powerful computers in their pockets.[43] In light of such revolutionary technological developments, the Supreme Court itself has indicated a willingness to revisit core doctrine. Most recently, the Court found longstanding precedent inapplicable given the personal privacy interests implicated by and the sheer ubiquity of the modern cell phone.[44]

Rather than take up the Court's invitation to reevaluate precedent from an earlier era, *Huff* relied on the traditional *Katz* plain view doctrine. In applying this standard to citizen–citizen interceptions, *Huff* may allocate risks in a way that creates tensions with both societal privacy expectations and the challenges that modern technologies pose. Especially in light of ongoing technological development, a better standard for Title III suits between private parties would balance responsibility between the individuals on both sides of the line.

Though importing *Katz*'s Fourth Amendment test might be quite productive in many Title III suits, it is not clear that *Huff* is such a case. In a more typical suit involving state interception of communications, the relationship between a wiretapping state agent and a wiretapped party mimics the dynamics of a standard government search-and-seizure case.[45] In such contexts, a court must balance law enforcement exigencies and public-safety concerns against the privacy interests of a citizen plaintiff.[46] In contrast, because *Huff* involved private-party interception, direct parallels to a Fourth Amendment search-and-seizure case are less obvious. In this sort of citizen–citizen case, public safety is not part of the calculus, and the current doctrine does not offer an obvious variable to weigh against a plaintiff's privacy interests.[47] Accordingly, analogous application of the *Katz* standard across both

---

[42] The Fourth Amendment has long been understood to protect individuals against *government* intrusions. *See, e.g.*, Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

[43] *Cf.* Matt Rosoff, *Your Phone Is More Powerful than the Computer in the Spaceship NASA Launched This Week*, BUS. INSIDER (Dec. 6, 2014, 10:01 AM), http://www.businessinsider.com/your-phone-is-more-powerful-than-the-orion-computer-2014-12 [http://perma.cc/M8EK-3GMG].

[44] Riley v. California, 134 S. Ct. 2473, 2484–85 (2014) (declining to extend permissive search precedent to the search of data on cell phones, in large part because "phones are based on technology nearly inconceivable just a few decades ago," *id.* at 2484); *see also* United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring) (describing seemingly settled Fourth Amendment precedent as "ill suited to the digital age," *id.* at 957).

[45] *See, e.g.*, Kee v. City of Rowlett, 247 F.3d 206, 208, 211 & n.6 (5th Cir. 2001); Dorris v. Absher, 179 F.3d 420, 423–25 (6th Cir. 1999).

[46] *Cf.* Terry v. Ohio, 392 U.S. 1, 18 n.15 (1968) (discussing how, in the context of a government search, "the Fourth Amendment governs all intrusions by agents of the public upon personal security, and . . . the scope of the particular intrusion, *in light of all the exigencies of the case*, [is] a central element in the analysis of reasonableness" (emphasis added)).

[47] Whether extant statutory and regulatory constraints on government law enforcement efforts are adequate to protect privacy interests is beyond the scope of this analysis.

government–citizen and citizen–citizen Title III suits may not best serve all involved parties.

In *Huff*, the seminal question comes from *Katz*'s objective prong: did Huff exhibit a reasonable expectation of privacy, regardless of his intentions?[48] To demonstrate this expectation, he would have needed to act affirmatively to prevent the harm that occurred.[49] The court reached this conclusion by analogizing to Fourth Amendment plain view doctrine,[50] equating a failure to draw blinds (and prevent a police officer from peering in and witnessing a crime) to a failure to lock an iPhone (and prevent the device from making a call that allows an unintended audience to document a conversation). This stance assumes the default setting in a physical space (open blinds/no privacy expectation) is parallel to the default here (unlocked phone/no privacy expectation). Viewed this way, a failure to "opt in" by actively securing a phone is a failure to manifest an (objective) expectation of privacy.

However, *Huff*'s application of the objective-expectation prong, bolstered by plain view doctrine, may be incongruous with societal expectations in a world where many individuals carry phones in their pockets. Even if pocket dials are a known risk, it does not automatically follow that the frequency of an occurrence signals a societal consensus that the burden is unequivocally on a user to secure her phone via a lock code or an application — or else sacrifice any reasonable expectation of privacy. The Sixth Circuit's analogy to plain view doctrine forecloses analysis of how society would expect the individuals on both sides of the line to act. The doctrine may consequently place a heavier burden than society might expect on a plaintiff seeking relief under the Title III, section 2320 private right of action.

To mitigate these issues, the citizen–citizen Title III suit may call for a more nuanced analysis in which the *Katz* standard acts as the initial step in a balancing test.[51] A court might first apply its understanding of *Katz* to assess subjective and objective reasonableness, with this conclusion forming the weight of a plaintiff's privacy interests on one side of the scale. If the plaintiff could establish that an alleged interceptor willingly took affirmative steps such that she was not merely a passive recipient,[52] then the court could independently assess

---

[48] *See Huff*, 794 F.3d at 548.

[49] *Id.* at 549.

[50] *See id.* at 550–52.

[51] Other domains, like tort negligence, use balancing tests to equitably assess risk and allocate burden. The BPL formula (comparing a prospective burden against the probability and cost of a prospective injury) is a well-known example. *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

[52] The definition of "interception" here does not depart from the definition used in other Title III suits, which requires intentionality by the defendant. *See* 18 U.S.C. § 2511(1)(a) (2012). Under the statute, "'intercept' means the aural or other acquisition of the contents of any wire, electron-

the subjective and objective reasonableness of the defendant's conduct. At this stage, the court could balance the defendant's case against the plaintiff's interests. The court would properly consider (1) any reasonable belief on the defendant's part that the interception was necessary to avoid a greater harm and (2) any inequity from imposing liability on the recipient of a pocket dial, who did not ask to be called. This approach could resolve citizen–citizen claims in a way that better coheres with the values on both sides of *Katz*'s original framework.[53]

Without a broader doctrinal shift or more precise, case-specific direction, *Huff*'s approach may raise as many questions as it answers. In *Huff*, the court believed it was simple to specify the concrete actions sufficient to exhibit a reasonable expectation of privacy: the plaintiff would have needed to take precautionary steps by downloading an application or locking the phone. However, what if Huff had locked his phone (objectively exercising an interest in privacy) and then unlocked it by putting his hand in his pocket and inadvertently touching the fingerprint ID surface, such that it opened and initiated a pocket dial? It is not at all clear whether this sequence would establish Huff's expectation of privacy (making Spaw potentially liable for illegal wiretapping, since she willingly recorded the call) — or whether any antecedent reasonable step that Huff took would be irrelevant in light of the subsequent chain of events. Without a more comprehensive framework, what constitutes an "exhibition" of a privacy expectation remains murky, and it is not clear that the modern individual could in fact "exhibit" such an expectation at all times.[54] A balancing test, of course, would not avoid this issue entirely, yet could still offer fairer outcomes because the defendant's actions would be a counterweight to the plaintiff's privacy interests.

Although *Huff*'s approach allows courts to adapt as technologies develop, its omission of overarching standards comes at the cost of clear guidance for today's courts. For instance, even as courts may extract from *Huff* that an individual must affirmatively act to secure her privacy interests, it is not apparent what an individual sporting an

---

ic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

[53] An alternate test for private communications might appear to incentivize private lawsuits — perhaps to an undesirable extent — and create administrability challenges for courts. However, the plaintiff would still bear the burden of proving an affirmative interception by the defendant, and the knowledge that a court would balance the plaintiff's interests in a fact-specific way should deter frivolous suits. Though courts would need to select between two doctrinal approaches, a decision framework that is not without tradeoffs, the relatively narrow context in which courts would deploy this doctrine should lower any inherent administrability hurdles.

[54] *See* William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 38–40 (2001) (stressing the "eternal vigilance," *id.* at 40, required when "even the slightest exposure of an item to the public can defeat a privacy claim," *id.* at 38).

Apple Watch or other wearable technology must do to demonstrate a reasonable expectation of privacy. Would she be expected to read and internalize a user manual and flawlessly execute any available privacy limits all of the time or else forfeit any privacy right? In addition to a lack of notice and predictability, there seems to be some risk that increasingly complex technologies will afford privacy protections only for those who are savvy enough to understand them at a sufficiently high level to take appropriate action. Especially since analysis of private causes of action informs more general Fourth Amendment jurisprudence,[55] *Huff*'s privacy ramifications for future suits involving different technologies are far-reaching.[56] For now, courts may already be toeing the line of affording privacy only to those with technical facility.[57] To the extent that society is not prepared to accept such an outcome as reasonable, the Sixth Circuit's holding in *Huff* may align with precedent and yet remain normatively problematic.

---

[55] The Court has often looked to privacy-related causes of action to inform its conception of reasonable expectations of privacy in the Fourth Amendment context. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 951 (2012) (emphasizing that the Court has defined the "reasonable expectation of privacy" as "an expectation 'that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society'" (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1998))); Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, . . . the surveillance is a 'search' and is presumptively unreasonable without a warrant."); Florida v. Riley, 448 U.S. 445, 451 (1989) (plurality opinion) ("Any member of the public could legally have been flying over Riley's property . . . and could have observed Riley's greenhouse.").

[56] As technology evolves, even companies that tout easy-to-use products publish long and complicated user manuals. *See, e.g.*, APPLE INC., APPLE WATCH USER GUIDE (2015), http://manuals.info.apple.com/MANUALS/1000/MA1708/en_US/apple_watch_user_guide.pdf [http://perma.cc/3N7Z-AH8X] (ninety-six-page user manual for Apple Watch).

[57] See, for instance, *United States v. Ganoe*, 538 F.3d 1117 (9th Cir. 2008) (discussed in *Huff*, 794 F.3d at 551), in which a user did not turn off the file-sharing function on peer-to-peer software (LimeWire). The Ninth Circuit applied the plain view doctrine to deny the user's privacy claim: "[T]o argue that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access . . . is like saying that he did not know enough to close his drapes." *Id.* at 1127.