No. 11-817

IN THE

Supreme Court of the United States

STATE OF FLORIDA,

Petitioner,

v.

CLAYTON HARRIS,

Respondent.

On Writ of Certiorari to
The Supreme Court of Florida

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF THE RESPONDENT

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
KHALIAH BARNES
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

August 31, 2012

QUESTION PRESENTED

Whether an investigative technique that law enforcement asserts reliably identifies the presence of contraband is sufficient to satisfy the probable cause requirement of the Fourth Amendment and thereby allows routine warrantless searches.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1]

EPIC has participated as *amicus curiae* before this Court and many other courts in matters concerning new challenges to Fourth Amendment protections. *See*, *e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012); *NASA v. Nelson*, 131 S. Ct. 746 (2011); *Tolentino v. New York,* 131 S. Ct. 1387 (2011); *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010); *Herring v. United States*, 555 U.S. 135 (2009); *Hiibel v. Sixth Judicial Circuit of Nev.*, 542 U.S. 177 (2004); *In re US for Historical Cell Site Data*, 747 F. Supp. 2d 827 (2010), *appeal docketed*, No. 11-20884 (5th Cir. Dec. 14, 2011); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2005); and, *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004).

At issue in this case is whether an alert by a narcotics detection dog, absent additional evidence of reliability, is sufficient to establish probable cause for

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

the warrantless search of a vehicle. As the outcome in this case may also implicate the use of investigative techniques that encroach upon electronic privacy, EPIC supports the judgment of the Florida Supreme Court, and urges the Court to reconsider the viability of the "sui generis" analysis, *see United States v. Place*, 462 U.S. 696 (1983), that would effectively place many similar techniques outside the scope of the Fourth Amendment. The police are now deploying a wide range of techniques, functionally similar to the canine sniff at issue in this case, that raise substantial concerns about the future application of the Fourth Amendment. As Justice O'Connor cautioned in *Arizona v. Evans*, "[t]he police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." 514 U.S. 1, 17-18 (1994) (O'Connor, J., concurring). In making this assessment, the Court should consider the reliability of the technique, the impact upon privacy, and the purpose of the Fourth Amendment.

SUMMARY OF THE ARGUMENT

When a new investigative technique is used in an attempt to identify a hidden substance, flag a possible threat, or gather evidence, the government should bear the burden of establishing its reliability. Otherwise, impermissible searches will result. This problem is particularly acute with search techniques – call them "electronic canine sniffs" – that implicate privacy.

The Court has previously considered whether an alert from a detection dog is itself a search, but it has not determined whether such an alert is sufficiently reliable to establish probable cause for a search. There is a clear need now to look more closely at techniques that purport to reliably detect only contraband. Since the decision in *Illinois v. Caballes*, 543 U.S. 405 (2005), forensic sciences have come under increased scrutiny. Scientific experts and legal scholars have urged more extensive evaluation of new investigative techniques, and the development of national standards, in order to support legal conclusions.

The rapid development of new investigative techniques poses a significant threat to electronic privacy and the rights of individuals. Many techniques may turn out to be useful, but all investigative techniques should be subject to close scrutiny by the courts. The "perfect search," like the "infallible dog," is a null set.

ARGUMENT

I. The Government's Burden of Reliably Establishing Probable Cause Is Essential to the Preservation of Electronic Privacy

This case presents a key Fourth Amendment concern: what evidence is necessary to establish the reliability of a method used to support a finding of probable cause? This question follows from the long and complicated history of searches enabled by drug detection canines. The Court assumed in *United States v. Place*, 462 U.S. 696 (1983), that the use of a trained dog "does not expose noncontraband items that otherwise would remain hidden from public view." *Id.* at 707. The Court reaffirmed that view in *Illinois v. Caballes*, 543 U.S. 405 (2005), but Justice Souter observed in dissent that "[a]t the heart both of *Place* and the Court's opinion today is the proposition that sniffs by a trained dog are *sui generis* because a reaction by the dog in going alert is a response to nothing but the presence of contraband." *Id.* at 410-11 (Souter, J., dissenting). As Justice Souter stated, and *amicus* EPIC believes to be true for a broad class of new investigative techniques, "[t]he infallible dog, however, is a creature of legal fiction." *Id.* at 411.

The deployment of electronic investigative techniques raises concerns very similar to the use of the detection dog in this case. A warrantless search conducted subsequent to an "alert" from a detection dog or similar technique will implicate Fourth Amendment interests. An unreliable and untested technique could generate false positives, alerts where there is no contraband present, which would lead to

invasive searches of innocent individuals. There are several examples of recently developed techniques that an agent might use in an attempt to detect contraband, but these techniques should not be used without testing and verification.

Imagine that the officer in this case did not rely on an "alert" by Aldo, the drug-detection dog, but instead on an "alert" by a new spectroscopic device used to identify unique chemical signatures from a distance. *See*, *infra* at Part III.B.1. Would the Court assume that information generated by such a device was reliable? Could the Court find that probable cause existed to search defendant's truck absent such proof? Imagine, alternatively, that the officer relied on an "alert" by a device that could peer under a person's clothing and observe and record images that would not otherwise be viewable by the police. Could the officer rely on that alert without first establishing the effectiveness of the device? And what of the substantial privacy intrusion that would result if such searches were routinely permitted without the accountability that the Fourth Amendment requires? *See*, *infra* at Part III.B.2. Similarly, imagine the agents use a network device to intercept private communications that they believe may contain evidence of illegal conduct. Such a technique could conceivably scan and record millions of private messages to find a needle in the digital haystack. Could the agent use the intercepted communications without first establishing the accuracy of the technique used to identify the illegal communications? *See*, *infra*, at Part III.B.3. Because the answer to all of these questions is clearly *no*, the

Court should uphold the decision of the Florida Supreme Court and require independent evidence of reliability where an officer uses an investigative technique to establish probable cause or otherwise justify an unwarranted search.

II. A Probable Cause Finding Under the Fourth Amendment Should Be Established Based on Reliable Evidence

In prior cases involving the use of narcotics detection dogs, this Court has held that probable cause was not required to conduct a "sniff test" in certain public spaces. *See Illinois v. Caballes*, 543 U.S. 405 (2005) (exterior of a vehicle during a traffic stop); *United States v. Place*, 462 U.S. 696 (1983) (luggage at an airport). These decisions were characterized as *sui generis* based on the Court's conclusion that a canine sniff "discloses only the presence or absence of narcotics, a contraband item." *Caballes*, 543 U.S. at 409. However, Justice Souter cautioned in *Caballes* that "[w]hat we have learned about the fallibility of dogs in the years since *Place* was decided would itself be reason to call for reconsidering *Place's* decision against treating the intentional use of a trained dog as a search." *Id.* at 410 (Souter, J., dissenting).

As the facts of this case show, many investigative techniques do not reliably indicate the presence of a contraband substance. The Fourth Amendment protects individuals against such "unreasonable searches and seizures," and this Court has held that procedural requirements, such as proof of probable cause, help ensure that individual rights are not violated.

A. The Fourth Amendment Protects Individual Privacy by Prohibiting Unreasonable Searches and Seizures

The Fourth Amendment protects individuals against "government intrusion[s] that upse[t] an . . . 'expectation of privacy' that is objectively 'reasonable.' " *Bond v. United States*, 529 U.S. 334, 340 (2000) (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). An individual has a reasonable expectation of privacy when (1) that individual manifests a subjective expectation of privacy, and (2) society recognizes that expectation as "reasonable." See *Katz* 389 U.S. at 360-61 (Harlan, J., concurring). To conduct investigations in such circumstances, law enforcement officials must first obtain a warrant supported by probable cause or invoke an exception to the Fourth Amendment's warrant clause. See Orin Kerr, *Searches and Seizures in the Digital World*, 119 Harv. L. Rev. 531, 547 (2005).

The Court has ruled that a dog sniff test conducted in certain public areas does not constitute an unreasonable search under the Fourth Amendment. *See Place*, 462 U.S. 696; *Caballes*, 543 U.S. 405. However, since the ruling in *Caballes*, the reliability of investigative techniques and forensic methods has been widely criticized. *See infra* Part III.A. In addition, legal scholars have raised significant concerns about the potential applicability of the "contraband exception" to the search of digital media. *See*, *e.g.*, Scott J. Glick, *Virtual Checkpoints and Cyber-Terry Stops: Digital Scans to Protect the Nation's Critical Infrastructure and Key Resources*, 6 J. Nat'l Sec. L. & Pol'y 97 (2012); Timothy C.

MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. Mem. L. Rev. 299 (2010); Mark E. Smith, *Going to the Dogs: Evaluating the Proper Standard for Narcotic Detector Dog Searches of Private Residences*, 46 Hous. L. Rev. 103 (2009); Daniel L. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 Ga. L. Rev. 1 (2005).

The Court previously addressed the use of new investigative techniques designed to detect the presence of contraband in *Kyllo v. United States*, 533 U.S. 27 (2001). The Court found that a search occurs where a device enables the Government "to explore details of the home that would previously have been unknowable without physical intrusion." *Id.* at 40. Justice Scalia, writing for the Court, also noted that the issue before the Court was somewhat broader, "[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.* at 34.

The same is true of investigative techniques that reveal the contents of a private space without establishing a traditional predicate for a search based on probable cause. The unreliability of a canine sniff not only implicates warrantless searches that produce contraband, but also warrantless searches of innocuous "persons, houses, papers, and effects." U.S. Const. amend. IV. Like the thermal-imaging device in *Kyllo*, a canine sniff cannot be classified as investigative tool that only reveals the presences or absence of contraband. *See* Cecil J. Hunt, II, *Calling in the Dogs: Suspicionless Sniff Searches and*

Reasonable Expectations of Privacy, 56 Case W. Res. L. Rev. 285, 335 (2005).

A canine sniff test could produce a false alert, for example, in the presence of an innocent person based on the scent of trace drug particles that exist on a substantial portion of the United States currency. *See id.* at 315 (*citing United States v. Carr*, 25 F.3d 1194, 1215 (3d Cir. 1994) (Becker, J., concurring in part and dissenting in part)) The Eleventh Circuit recently noted that "as much as 80 [percent] of currency in circulation has drug residue." *United States v. $242,484.00*, 351 F.3d 499, 511 (11th Cir. 2003), *vacated on other grounds by reh'g en banc*, 357 F.3d 1225 (11th Cir. 2004). Therefore, even those who are innocent of any criminal activity face a substantial likelihood that a trained drug-sniffing dog will alert to the presence of contraband, in the form of drug residue on their currency, and thereby subject them to an invasive governmental search.

Even in the absence of tainted currency, innocent individuals face the threat of other false positives from detection dogs. Allowing probable cause to be established based upon the use of an unreliable investigative technique, such as a narcotics-detection dog or other allegedly 'infallible' search, "is . . . highly problematic because it is an exception that threatens to swallow the rule . . . that all government searches are presumptively unreasonable unless accompanied by a warrant or covered by a particular and limited exception." Hunt, *supra* at 335. This exception could leave the public "at the mercy of advancing technology" as Justice Scalia warned in *Kyllo*. 533 U.S. at 36.

B. In Order to Establish Probable Cause Based on the Use of an Investigative Technique, a Court Should Consider Whether the Technique Is Reliable

The Court has made clear in the past that an assertion of probable cause may not rest upon "mere conclusory statement[s]" that lack "any basis at all for making a judgment regarding probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983) (citing *Nathanson v. United States*, 290 U.S. 41 (1933)). Rather, the officers seeking to establish probable cause must establish a "fair probability that contraband or evidence of a crime will be found in a particular place" based on the "totality of the circumstances analysis." *Gates*, 462 U.S. at 238. A reviewing magistrate must have "[s]ufficient information [to] allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Id.* at 239. The reliability of the source of information is a "highly relevant" factor in determining whether the probable cause requirement has been satisfied. *Id.* at 230. *See Safford Unified School Dist. No. 1 v. Redding*, 557 U.S. 364, 371 (2009); *Arizona v. Evans*, 514 U.S. 1, 16 (1995) (O'Connor, J., concurring).

III. New Investigative Techniques Should Be Used Based on Research, Testing, and Data Indicating Reliability

The development of new investigative techniques is important for effective law enforcement, but these techniques should be constantly evaluated to determine their reliability. Forensic science has been widely criticized in recent years because of a lack of clear standards and credible research to

support technical conclusions. *See* National Research Council of the National Academies, *Strengthening Forensic Science in the United States: A Path Forward* 2 (2009) [hereinafter National Academy Report]. There have been some efforts to improve these procedures, including the development of standard-setting groups by the Federal Bureau of Investigation ("FBI") and others. *See*, *e.g.*, Fed. Bureau of Investigation, U.S. Dep't of Justice, *Scientific Working Group on Dogs and Orthogonal Detection Guidelines*, 8 Forensic Science Comm. (Oct. 2006).[2]

Still, the rapid deployment of new investigative techniques has outpaced the ability to develop appropriate standards to ensure reliability and effectiveness. A lack of clear standards for the use of detection dogs, for example, highlights the need for additional evidence to support a finding of probable cause. Without this evidence, courts risk encouraging unreliable and ineffective law enforcement techniques as well as weakening constitutional privacy protections, as searches will occur regardless of whether evidence is found.

New techniques that have recently been developed by federal agencies to detect contraband and seize illegal communications present similar problems to the detection dogs in this case. Examples include Terahertz Wave Reflection Spectroscopy, *see infra* Part III.B.1, Millimeter Wave and Backscatter

---

[2] *Available at* http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2006/standards/2006_10_standards01.htm.

X-Ray (airport body scanners), *see infra* Part III.B.2, and message interception software ("Carnivore"). *See infra* Part III.B.3. A decision to reverse the Florida Supreme Court, as applied to these digital search techniques, could unleash a new generation of "electronic canine sniffs" that would operate largely beyond Fourth Amendment review.

A. The National Academy of Sciences and Other Experts Have Raised Significant Concerns About the Lack of Reliable Standards for Investigative Techniques

Amicus EPIC's concerns about the outcome in this case arise in large part because of a growing scientific and legal consensus about the need to assess the reliability and impact of new investigative techniques. As Senator Patrick Leahy explained at the commencement of a series of recent hearings on forensic science before the Senate Judiciary Committee, "there is agreement that we must dedicate resources to basic foundational research into the validity of forensic disciplines and the methods they employ, and that we must agree on basic standards." *Improving Forensic Science in the Criminal Justice System: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2012) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary).

A 2008 Report by the National Academy of Sciences identified several of significant problems in forensic science, including "the potential danger of giving undue weight to evidence and testimony derived from imperfect testing and analysis" and the subsequent "admission of erroneous or misleading

evidence." National Academy Report at 4. The National Academy Report, issued after the Court's decision in *Illinois v. Caballes*, 543 U.S. 405 (2005), was commissioned by Congress to "identify the needs of the forensic science community." *See* The Science, State, Justice, Commerce, and Related Agencies Appropriations Act of 2006. P.L. No. 109-108, 119 Stat. 2290 (2005). The expert panel reviewed current forensic methods and made recommendations to help establish guidelines and best practices. National Academy Report at 2. The panel focused on the importance of minimizing the forensic community's "current fragmentation and inconsistent practices," including a lack of "uniformity in certification of forensic practitioners." *Id.* at 6. This Court has previously recognized the significance of the National Academy Report in identifying problems with the reliability of forensic methods. *See Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009).[3] The Court

---

[3] In full, the Court stated:

> Nor is it evident that what respondent calls "neutral scientific testing" is as neutral or as reliable as respondent suggests. Forensic evidence is not uniquely immune from the risk of manipulation. According to a recent study conducted under the auspices of the National Academy of Sciences, "[t]he majority of [laboratories producing forensic evidence] are administered by law enforcement agencies, such as police departments, where the laboratory administrator reports to the head of the agency." National Research Council of the National Academies, Strengthening Forensic Science in the United States: A Path Forward 183 (2009) (hereinafter National Academy Report). And "[b]ecause forensic scientists often are driven in their

should look to that report again when considering the required reliability of the detection dog methods at issue in this case, and in other probable cause cases going forward.

The Florida Supreme Court below reached the conclusion that "the State must introduce evidence concerning the dog's reliability" in a case where the State intends for the "dog's alert [to provide] probable cause for a search . . . ." *Harris v. State*, 71 So.3d 756, 759 (Fla. 2011). The National Academy Report focused on the same problem where "the interpretation of forensic evidence is not always based on scientific studies to determine its validity." National Academy Report at 8. This problem is compounded by the use of "subjective assessments" where there exists "the potential for bias and error in human observers." *Id.*

This Court has recognized that, in the context of the Federal Rules of Evidence, a "trial judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable." *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 589 (1993). The focus of a trial judge should be solely on "principles and methodology . . . ." *Id.* at

---

> work by a need to answer a particular question related to the issues of a particular case, they sometimes face pressure to sacrifice appropriate methodology for the sake of expediency." *Id.*, at 23–24. A forensic analyst responding to a request from a law enforcement official may feel pressure--or have an incentive--to alter the evidence in a manner favorable to the prosecution.

Melendez-Diaz, 557 U.S. at 318.

595. This presents a problem where "[f]orensic science facilities exhibit wide variability in capacity, oversight, staffing, certification, and accreditation across federal and state jurisdictions." National Academy Report at 14. The National Academy Report made several recommendations for improving the current, fragmented system. Chief among them was the establishment and funding of "an independent federal entity, the National Institute of Forensic Sciences ('NIFS')." *Id.* at 19. The Report recommended that NIFS have an advisory board comprised of experts in "forensic science disciplines . . . information technology, measurements and standards, testing and evaluation, law, [and] national security . . . ."*Id.* The NIFS would be responsible for implementing standardized reporting, increasing research, developing best practices, and imposing quality control. *Id.* at 19-33.

The problem of the reliability of expert evidence in the courtroom is not new. *See* Learned Hand, *Historical and Practical Considerations Regarding Expert Testimony*, 15 Harv. L. Rev. 40 (1901). The problems with forensic science identified by the National Academy Report are also not new. *See* James W. Osterburg, *A Commentary on Issues of Importance in the Study of Investigation and Criminalistics*, 11 J. Forensic Sci. 261 (1966). After this Court's creation of a new evidentiary test in *Daubert*, 509 U.S. 579 (1993), some forensic associations have even argued in favor of treating "forensic" testimony as non-scientific to avoid exacting standards. *See* Brief for the Int'l Assn. of Arson Investigators, *Mich. Millers Mutual Ins. Co. v. Benfield*, 140 F.3d 915 (11th Cir. 1998). However,

criminal forensic methods should be more reliable, not less, due to the risk of wrongful conviction and unwarranted search and seizure of private property.

The National Academy Report provided additional credence to the arguments of many legal scholars and scientific experts who raised similar questions about forensic methods over the past thirty years.[4] At the time that the Court ruled in *Daubert*, the issue of reliability of scientific evidence admitted in civil trials (and certain criminal contexts) had reached a climax.[5] However, problems with the use of

---

[4] *See*, *e.g.*, Peter W. Huber, *Galileo's Revenge: Junk Science in the Courtroom* (Basic Books 1993). John J. Lentini, *'Progress' in Fire Investigation: Moving from Witchcraft and Folklore to the Misuse of Models and the Abuse of Science*, 4th Int'l Symp. on Fire Investigation Sci. & Tech. (2010); Brandon L. Garret & Peter J. Neufeld, *Invalid Forensic Science Testimony and Wrongful Convictions*, 95 Va. L. Rev. 1 (2009); Jennifer L. Mnookin, *The Courts, the NAS, and the Future of Forensic Science*, 75 Brook. L. Rev., no. 4, at 1 (2009); Joseph L. Peterson & Anna S. Leggett, *The Evolution of Forensic Science: Progress Among the Pitfalls*, 36 Stetson L. Rev. 621 (2007); Paul C. Giannelli, *Forensic Science*, 33 J. L., Medicine, & Ethics 535 (2005); D. Michael Risinger et al., *The Dauberg/Kumho Implications of Observer Effects in Forensic Science: Hidden Problems of Expectation and Suggestion*, 90 Cal. L. Rev. 1 (2002); Paul C. Giannelli, *'Junk Science': The Criminal Cases*, 84 J. Crim. L. & Crimonology 105 (1993); Andre A. Moenssens, *Novel Scientific Evidence in Criminal Cases: Some Words of Caution*, 84 J. Crim. L. & Crimonology 1 (1993); William C. Thompson, *Evaluating the Admissibility of New Forensic Tests: Lessons from the 'DNA War'*, 84 J. Crim. L. & Crimonology 22 (1993).

[5] See examples from the 1993 *Expert Admissibility Symposium* of Northwestern's Journal of Criminal Law and Criminology:

such evidence in criminal trials "remained in the shadows." Paul C. Giannelli, *'Junk Science': The Criminal Cases*, 84 J. Crim. L. & Crimonology 105, 128 (1993). Professor Giannelli warned at the time that "[t]he present adversary system, however, does not contain sufficient safeguards to protect against the misuse of scientific evidence." *Id.*[6]

Recently a group of law professors, academic researchers, and practicing forensic scientists, led by professor Jennifer Mnookin, sought to develop a common framework for modern forensics. *See* Jennifer L. Mnookin et al., *The Need for a Research Culture in the Forensic Sciences*, 58 UCLA L. Rev. 725 (2011). Professor Mnookin's study argues for an increased focus on empiricism, transparency, and the type of ongoing critical perspective inherent in a "research culture." *Id.* at 740-44. These values could be promoted in unified standards set for various forensic techniques, which could then be used by courts to establish reliability.

The National Academy Report stressed that "[s]tandards provide the foundation against which

---

Giannelli, Moenssens, and Thompson as well as Peter Huber's book *Galileo's Revenge*, *supra* note 2.

[6] Professor Giannelli is one of several experts who recently testified before the Senate Judiciary Committee on the need for a new scientific approach to forensics, as outlined in the National Academy Report. See *Strengthening Forensic Science in the United States: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (2009) (testimony of Professor Paul Giannelli, Case Western Reserve University).

performance, reliability, and validity can be assessed." National Academy Report at 201. They also "make it possible to replicate and empirically test procedures and help disentangle method errors from practitioner errors." *Id.* As the Report notes, the FBI initiated a series of Scientific Working Groups ("SWGs") in the early 1990s to "facilitate consensus around forensic science operations among federal, state, and local agencies." *Id.* at 202 (citing Fed. Bureau of Investigation, *Scientific Working Groups*, Forensic Science Comm. (Jul. 2000)). One of these working groups, SWGDOG, was established in January 2005 "in an effort to develop consensus-based guidelines" for the use of detection-dogs. Fed. Bureau of Investigation, *Scientific Working Group on Dogs and Orthogonal Detection Guidelines (SWGDOG)*, Forensic Science Comm. (Oct. 2006). The Report notes that, "[i]deally, standards [from these groups] should be consistently applicable and measureable." National Academy Report at 203.

The SWGDOG has established "consensus-based best practice general guidelines for training, certification, and documentation pertaining to all canine disciplines." Scientific Working Group on Dog and Orthogonal Detector Guidelines, *SWGDOG SC2 – General Guidelines* (1st Rev. 2009).[7] The SWGDOG guidelines outline the best practices for dog training and certification, which include analysis of field tests and performance history, similar to what was required by the Florida Supreme Court. *Id.* at 2-4. *C.f. Harris*, 71 So.3d at 769. Even if the Court does

---

[7] *Available at* http://www.swgdog.org/.

not apply the *Daubert* test strictly in the context of a probable cause determination, a clear standard like the one established by SWGDOG, which was not followed by the officers in the case now before the Court, should weigh heavily in the "totality of the circumstances" under *Gates*. 462 U.S. at 238.

These standards would provide protection for individuals from unreasonable intrusions, and would also encourage the use of reliable investigative techniques. Establishing a requisite level of reliability of narcotic dog detection techniques "serves to deter deliberate, reckless, or grossly negligent conduct, or . . . recurring or systemic negligence" in establishing probable cause. *Herring v. United States*, 555 U.S. 135, 144 (2009).

B. New Forensic Techniques Demonstrate the Ongoing Problem of Inadequate Testing and Evaluation

As with detection dogs, new forensic technique requires extensive training, research, and validation. These tools may help solve crimes, but a substantial amount of work must take place before they are used in the field. When an agent uses an investigative technique to uncover predicate facts used to justify a search, that agent should be able to demonstrate that the technique is tested, reliable, and has been properly used and maintained. Without such proof there can be no probable cause.

As the examples below show, the development of new investigative techniques is an ongoing process. Results obtained in the lab are not necessarily replicated in the field. And the prospect that courts would rely on imperfect drug detection dogs to allow

findings of probable cause for more advanced techniques is troubling. "The dog sniff . . . is just one crude, old-fashioned example of the search technologies available to law enforcement." Julian Sanchez, *The Pinpoint Search*, Reason (Jan. 2007).[8] A "new wave of advanced surveillance tools," far more sophisticated than canine sniffs, will be used to detect "weapons, explosives, and illicit computer files." *Id.*

Law enforcement is now deploying investigative techniques involving chemical detectors, computer hash values, and airport body scanners to attempt to detect contraband. *See* Timothy C. MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. Mem. L. Rev. 299, 345-347 (2010). According to the author, this technology is likely to be used to justify warrantless searches, pursuant to the Court's earlier decisions in *Place* and *Cabelles*. *Id.* at 348.

Many new devices are created to aid law enforcement, but they are not all sufficiently reliable and effective to support invasive searches and the exposure of private information. For example, terahertz scanning technology, whole body imaging, and digital interception all present reliability problems similar to those at issue in this case.

---

[8] *Available at* http://reason.com/archives/2007/01/10/the-pinpoint-search.

1. *Terahertz Scanners Generate False Positives Based on Trace Amounts and Interference Can Cause Unreliable Results*

Law enforcement agencies continually develop new technologies in an attempt to detect contraband substances. One example is Terahertz ("THz") Wave Reflection Spectroscopy. *See* Xi-Cheng Zhang & Jingzhou Xu, *Introduction to THz Wave Photonics* (Springer 2010). This technology has been the subject of extensive research and debate, in part, because it is intended to identify substances from a distance based on a recognized molecular "fingerprint." *See* Markus Walther et al., *Chemical Sensing and Imaging with Pulsed Terahertz Radiation*, 397 Analytical & Bioanalytical Chemistry 1009 (2010). Still, despite ambitious views about the applications of this technology in industrial,[9] security,[10] and even

---

[9] See, e.g., Ronald Ulbricht et al., *Carrier Dynamics in Semiconductors Studied with Time-Resolved Terahertz Spectroscopy*, 83 Rev. Mod. Phys. 543 (2011); Ikufumi Katayama & Masaaki Ashida, *Broadband Terahertz Spectrosocopy and Its Application to the Characterization of Thin Films*, 53 J. Vacuum Soc'y 301 (2010).

[10] *See*, *e.g.*, *BomDetec – Phase I Preliminary Design Review Report*, submitted by Gordon-CenSSiS, Nat'l Sci. Found. Research Ctr., to the Homeland Sec. Advanced Research Projects Agency of the Dep't of Homeland Sec. in response to Prototypes and Technology for Improvised Explosives Device Detection (PTIEDD) Broad Agency Announcement 05-05 (BAA 05-03) [hereinafter *CenSSiS Design Report*]. For more information about this process see http://epic.org/foia/dhs/terahertz-frisking.html.

law enforcement settings,[11] "for many realistic applications in chemical analysis and imaging of biological systems, the technology still lacks the required sensitivity and also suffers from its intrinsically poor spatial resolution." *Id.* at 1010.

The THz scanning technology has shown promise in laboratory conditions, but would face significant challenges if used to identify substances remotely in real world circumstances. Terahertz scanners manipulate electro-magnetic waves between the range of microwaves and infrared waves. *Id.* By analyzing the reflection created by two lasers aimed at a target under controlled conditions, detectors can create material signatures in the terahertz range through spectroscopy. *See* Roger N. Clark, U.S. Geological Survey, *Chapter 1: Spectroscopy of Rocks and Minerals, and Principles of Spectroscopy* (1999). These spectroscopic signatures can create a unique "fingerprint," which a THz scanner may be able to match with the signature of an existing chemical compound. Mark Marchand, *A Revolutionary*

---

[11] Al Baker, *Police Working on Technology to Detect Concealed Guns,* N.Y. Times (Jan. 17, 2012), http://cityroom.blogs.nytimes.com/2012/01/17/police-working-on-technology-to-detect-concealed-guns/; Jess McNally, *Terahertz Detectors Could See Through Your Clothes From a Mile Away*, Wired (July 12, 2010), http://www.wired.com/wiredscience/2010/07/terahertz-detection/; Keith Wagstaff, *Police Developing Tech to Virtually Frisk People from 82 Feet Away*, Time (Jan. 20, 2012), http://techland.time.com/2012/01/20/police-developing-tech-to-virtually-frisk-people-from-82-feet-away/.

Breakthrough in Terahertz Remote Sensing, Rensselaer Polytechnic Institute (July 12, 2010).[12]

In laboratory conditions, a THz scanner may be able to detect signals from up to 67 feet away. *See* Jingle Liu et al., *Broadband Terahertz Wave Remote Sensing Using Coherent Manipulation of Fluorescence from Asymmetrically Ionized Gases*, 4 Nature Photonics 627 (2010). However, this technique is vulnerable to interference from the presence of moisture and metal, *see* CenSSiS Design Report 54, *supra* at Note 10, which would affect the reliability of scans conducted in real world settings. This problem is exacerbated when the device is used outdoors, due to increased water vapor. *Id.* at 64-65. In addition, the THz scanning technique relies on a "comparison between the measured spectrum and a library spectrum," which requires the creation of a verifiable library of material signatures. *Id.* at 56. When this comparison occurs, the operator must determine an acceptable "confidence level" used to determine when a "match" has occurred. *Id.* at 63-64.

Even beyond the underlying technical difficulties with creating and using terahertz signatures to reliably identify target substances, the use of THz scanners would present many of the same problems as detection dogs. The device would ultimately be operated by an agent, and would be subject to human error and manipulation in its configuration, operation, and interpretation. *See*

---

[12]http://news.rpi.edu/update.do?artcenterkey=2748&setappvar=page%281%29.

Melendez-Diaz, 557 U.S. at 318. The device would also be capable of detecting trace particles of a target substance, *see generally* S. Kong & D. Wu, *Terahertz Time-Domain Spectroscopy for Explosive Trace Detection*, CIHSPS – IEEE Int'l Conf. on Computational Intelligence for Homeland Sec. & Personal Safety (2006), and thus an alert would not necessarily indicate that a substantial amount of the target substance was present. Furthermore, the reliability of the spectroscopy technique depends on the reliability of the match between the current reading and the material signature created beforehand. *See* Kodo Kawase et al., *Non-destructive Terahertz Imaging of Illicit Drugs Using Spectral Fingerprints*, 11:20 Optics Express 2550 (2003). Any of these limitations could cause significant error, which could lead to an unreasonable search of an individual and exposure of private information. In order to support a finding of probable cause for a warrantless search, such a technique would have to be shown to produce reliable and verifiable results.

2. Airport "Body Scanners" Are Not Designed to Identify the Contraband the Agency Claims They Detect

In 2005, the TSA began deploying Whole Body Imaging ("WBI") devices in U.S. airports. *See* U.S. Dep't of Homeland Sec*., Budget-in-Brief Fiscal Year 2006* at 81-82 (Feb. 7, 2005).[13] As with narcotics detection dogs, agents attempt to use WBI technology

---

[13] *Available at* http://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2006.pdf.

to establish probable cause to search air travelers and their effects. But in 2007, the Committee on Assessment of Security Technologies for Transportation of the National Academy of Sciences found there had been a "significant overselling of the potential of [WBI technology] to address screening requirements" and that lack of "understanding of the technology and its . . . limitations appear to exaggerate the potential benefits of the technology." *Id.* at 3. The Committee said that WBI technologies were not reliable in detecting explosive materials. Comm'n on Assessment of Sec. Tech. for Transp., National Academy of Sciences, *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons* 4 (2007). The expert panel found that WBI technology can locate certain anomalies or other objects on the body, but cannot necessarily identify the objects. *Id.* at 43. Appropriately identifying the object "may be necessary in order to reduce false positives generated by prosthetics, shoe shanks, and so on." *Id.* Any alert—including false positives—by WBI technology can subject individuals to an invasive search, including an aggressive "frisking" of the traveler's body, by TSA personnel. The study concluded, "there is insufficient technology available to develop a system capable of identifying concealed explosives." *Id.* at 59.

Additional evidence bolsters the study's findings. The TSA's own Procurement Specifications indicate that the WBI machines were not designed to detect powdered explosives, a primary justification for the program. *See* Transp. Sec. Admin., U.S. Dep't of Homeland Sec., *Procurement Specification for*

Whole Body Imager Devices for Checkpoint Operations, Sept. 23, 2008.[14] Subsequent studies by the Government Accountability Office and independent experts confirm the failure to adequacy evaluate the technique prior to deployment. *See U.S. Gov't Accountability Office*, GAO-12-541T, *Transportation Security Administration: Progress and Challenges Faced in Strengthening Three Key Security Programs* (2012); Leon Kauffman & Joeseph W. Carlson, *An Evaluation of Airport X-ray Backscatter Units Based on Image Characteristics*, 4 J. Transp. Sec. 73 (2011).

Members of Congress have also expressed concern about the reliability of this new search technology. In May 2012, Members of the House Transportation and Infrastructure Committee and the Oversight and Government Reform Committee sharply criticized the agency for spending hundreds of millions of dollars on technology that they said had not been properly tested. *TSA Oversight Part IV: Is TSA Effectively Procuring, Deploying, and Storing Aviation Security Equipment and Technology? Joint Hearing Before the H. Comm. on Oversight and Government Reform and the Comm. on Transportation and Infrastructure*, 112th Cong. (2012). A report released by the two committees that day called the machines "ineffective." Staff of H. Comm. on Oversight and Gov't Reform & H. Comm. on Transp. and Infrastructure, 112th Congress, *Airport Insecurity: The TSA's Failure to Effectively*

---

[14] *Available at* http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf.

Procure, Deploy and Warehouse Its Screening Technologies, (Comm. Print 2012).

The approach adopted by the Florida Supreme Court below would avoid this unfortunate outcome by encouraging greater scrutiny of invasive and unreliable threat-identification techniques. By requiring that the Government present some evidence of reliability, this Court would ensure that searches are not devoid of the procedural protections guaranteed by the Fourth Amendment.

3. Digital Intercept Devices Overcollect Communications Data

In the late 1990s, the FBI developed a software program called "Carnivore" to enable interception of Internet communications pursuant to a court order. *See Internet and Data Interception Capabilities Developed by FBI: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation). Carnivore was designed to act like a commercial packet "sniffer" product, which analyzes electronic communications packets as they travel through a network. *See id.* According to the agency, Carnivore could be configured to filter and then store "transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc." *Id.*

The IIT Research Institute conducted an independent assessment of the FBI's program, and determined that the Carnivore software was capable of collecting "everything that passes by on the Ethernet segment to which it is connected." IIT

Research Inst., *Independent Technical Review of the Carnivore System: Final Report* 4-3 (2000) [hereinafter IITRI Final Report]. The Report also found that "Carnivore version 1.3.4 collects more than would be permitted by the strictest possible construction of the pen-trap statute," and the FBI "admitted that a previous version of Carnivore handled pipelined SMTP [packets] incorrectly." *Id.* However, the Report concluded that there were "significant procedural checks to minimize configuration errors." *Id.*

The proper configuration and use of the Carnivore software was thus a critical element of any legal use of the tool. *See Melendez-Diaz,* 557 U.S. at 318. As Professor Orin Kerr also noted, "legitimate concerns exist that the program may malfunction, and as with any tool, human error can cause the program to be configured incorrectly." Orin Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 654 (2003). In response to this concern, Congress added new reporting requirements under the pen register statute, codified at 18 U.S.C. § 3123(a)(3), that require documentation of:

> (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
> (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

> (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
> (iv) any information which has been collected by the device

18 U.S.C. § 3123(a)(3).

Such documentation, as the Florida Supreme Court below recognized regarding the use of drug detection dogs, is necessary to establish the reliability of the investigative techniques. Without detailed information about the configuration or capabilities of a particular investigative tool, a court cannot determine whether a search complies with constitutional and statutory requirements; a judge cannot accept conclusory and general statements about the accuracy and reliability of the methods used.

CONCLUSION

Recognizing the risk that "electronic canine sniffs" have significant implications for the future of the Fourth Amendment, EPIC respectfully asks this Court to uphold the decision of the Florida Supreme Court.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
KHALIAH BARNES
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

August 31, 2012