IN THE

COURT OF SPECIAL APPEALS OF MARYLAND

SEPTEMBER TERM, 2015

No. 1496

BY COURT OF SPECIAL APPEALS
DEC 2 9 2015
RECEIVED

STATE OF MARYLAND

Appellant,

v.

KERRON ANDREWS,

Appellee.

On Appeal from the Circuit Court for Baltimore City
(The Honorable Kendra Ausby, Presiding)

BRIEF OF PROFESSOR DAVID GRAY AS *AMICUS CURIAE*

Jonathan J. Huber
Miles & Stockbridge P.C.
100 Light Street
Baltimore, Maryland 21202
(410) 385-3450
jhuber@milesstockbridge.com

Counsel for Amicus Curiae
Professor David Gray

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Constitutional Provisions

Cases

Statutes

Law Review Articles

Other Sources

INTERESTS OF *AMICUS CURIAE*[1]

David Gray is Professor of Law at the University of Maryland School of Law. He teaches criminal procedure and writes on the Fourth Amendment and technology. The issues raised in this appeal intersect with his current research, which uses the methods of public meaning originalism to analyze contemporary Fourth Amendment challenges.

[1] In accordance with Rule 8-511, the parties to this appeal have consented to the filing of this brief. No party other than *amicus* made a monetary or other contribution to the preparation or submission of the brief. No counsel to a party in this case authored this brief in whole or in part.

INTRODUCTION

In this appeal, the State seeks a license to intercept private communications between citizens of Maryland and their cellular service providers free from constitutional constraint.[2] To accede to this request would be to sanction precisely the kinds of broad and indiscriminate searches our founders regarded as anathema to our basic right to be free from the threat of pervasive government surveillance. They wrote and ratified the Fourth Amendment to guarantee those protections for themselves and their posterity. As guardians of that sacred trust, this Court should deny the State's request by holding that the deployment and use of cell-site simulators absent a warrant based on probable cause constitutes an unreasonable search.

ARGUMENT

I. The Use of Cell-Site Simulators Is a Search.

A. Cell-Site Simulators Intercept Private Communications and Gather Indiscriminately Information About Cellular Phone Users, their Locations, and their Communications.

According to the State, the cell-site simulator used in this case masqueraded as a cellular base tower, passively intercepting communications between Mr. Andrews and his cellular service provider. App. Br. at 8. According to a recently-released Department of Justice memorandum, cell-site simulators also actively engage user devices, emitting signals to all the cellular phones in their areas of operation, which causes those devices to attempt to communicate with their service providers' networks. U.S. Dept. of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, 1-2 (Sept. 3, 2015), available at http://www.justice.gov/opa/file/767321/download (hereinafter "Dept. of Justice Mem."). Cell-site simulators then intercept those communications. *Id*. In either event, cell-site simulators acquire information from user devices, including unique device identifiers, and location information by intercepting

[2] Professor Gray adopts the Nature of the Case, Material Proceedings Below, Questions Presented and Statement of Facts, as set forth in the Brief of Appellee. *See* Md. Rules 8-504(a) and 8-511.

communications between user devices and service providers. They also intercept basic call information traditionally gathered by pen registers such as the time of calls, duration of calls, and numbers called. *See* Harris Corporation, Stingray Product Description, available at http://files.cloudprivacy.net/Harris_Stingray_product _sheet; Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 11-12 (2014); App. Br. at 8-9; Dept. of Justice Mem. at 1-2. Moreover, cell-site simulators gather this information in a purely indiscriminate manner by engaging all cellular phones within their areas of operation. Dept. of Justice Mem. at 2. As a consequence, cell-site simulators can easily intercept thousands of private communications between hundreds of users and their service providers allowing officers to determine who is in the area, where they are, whether they are communicating over their cellular phones, and with whom.

B. The Use of Cell-Site Simulators to Intercept Private Communications is a Search.

The Supreme Court has long held that we have reasonable expectations of privacy in our private communications. *See Berger v. New York*, 388 U.S. 41, 51 (1967) ("'conversation' [falls] within the Fourth Amendment's protections, and that the use of electronic devices to capture it [is] a 'search' within the meaning of the Amendment") (internal citation omitted). For example, in *Katz v. United States*¸ the Supreme Court held that law enforcement officers violated a suspect's reasonable expectations of privacy in his private communications when they eavesdropped using an electronic listening device installed on the outside of a public phone booth. 389 U.S. 347, 350-53 (1967). The Supreme Court has also maintained inviolate the contents of letters and packages "intended to be kept free from inspection." Ex Parte *Jackson*, 96 U.S. 727, 733 (1878).

The State appears to concede that we have reasonable expectations of privacy in some of our communications. Relying on *Smith v. Maryland*, 442 U.S. 735 (1979), and the "third-party doctrine," the State nevertheless maintains that we have no reasonable expectations of privacy in the device identifier, physical location, and the other call

information we communicate to our cellular service providers simply because that information is shared with our cellular service providers. App. Br. at 9-14. That view finds no support in existing Supreme Court doctrine. Quite to the contrary, the Court's reasoning in *Smith* and its progeny necessarily implies the opposite: that we have reasonable expectations of privacy against government's interception of all private communications with our telephone service providers.

C. The Third-Party Doctrine Does Not Authorize the Government to Intercept Communications with Third Parties Without a Warrant.

Simply put, the State's argument regarding the third-party doctrine fails to account for *how* government agents gain access to information we share with others. Indeed, in every case where the Supreme Court has elaborated and applied the third-party doctrine, the third party has acted as a knowing conduit for information sought by the government.[3] In none of these cases did the Supreme Court sanction the government's direct interception of communications. *Smith v. Maryland* is no exception. In *Smith*, a telephone company, acting at the request of law enforcement, installed a pen register device on its own infrastructure for the purpose of gathering call record information associated with Smith's telephone number. 442 U.S. at 737. The company then passed that information to law enforcement. *Id.* That arrangement, in which the telephone company was the conduit of information, was essential to the Court's holding. That is evident in language quoted by the State, in which the Court reasoned that "[w]hen [Smith] used his phone, [he] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of

[3] *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 442-43 (1976) (law enforcement subpoenaed records from defendant's bank); *Hoffa v. United States*, 385 U.S. 293 (1966) (a government informer conveyed the contents of defendant's communications with that informer to law enforcement); *Lewis v. United States*, 385 U.S. 206 (1966) (an undercover agent conveyed the contents of defendant's communications with that agent to law enforcement); *Lopez v. United States*, 373 U.S. 427 (1963) (a cooperating witness conveyed the contents of defendant's communications with that witness to law enforcement). *See also Upshur v. State*, 208 Md. App. 383 (2012) (law enforcement subpoenaed subscriber information from defendant's service provider).

business. In doing so, [Smith] assumed the risk that the company would reveal to police the numbers he dialed." App. Br. at 10 (quoting *Smith*, 442 U.S. at 744). The Supreme Court neither held nor implied that Smith also assumed the risk that law enforcement would intercept information directly by, say, tapping phone lines.

In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court reaffirmed the distinction between gathering information through a third-party conduit and gathering information directly. There, the government cited *Smith* to argue that it was entitled to access directly the call records stored on a suspect's lawfully seized cellular phone because that information revealed nothing more than would have been revealed by a pen register device. *Id.* at 2492. The Court roundly rejected this proposition, pointing out that the use of "a pen register at telephone company premises to identify numbers dialed by a particular caller" is not a search, but maintaining that accessing that same information directly by searching records stored on a phone is a search. *Id.*

The State's claim that "the Fourth Amendment [is] not implicated when police obtain[] information voluntarily transmitted to third parties," App. Br. at 10, leads to absurdity. By definition, everything one says during a telephone conversation is transmitted voluntarily to a third party. Thus, if the State is right, then law enforcement would be entitled to install a surreptitious listening device on the outside of a telephone booth in order to eavesdrop on everything a caller said during the course of a telephone call. In a similar vein, the State's argument would allow law enforcement to open our mail, tap our phones, and read our electronic mail. After all, in each of these instances we voluntarily transmit information to third parties. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. L. Forum 121, 153-54 (2008).

A more accurate statement of the third-party doctrine is that we have no Fourth Amendment complaint if a party to our communications shares that information with government agents. *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."). Under this rule, the State

cannot argue that its use of a cell-site simulator fell within the compass of the third-party doctrine. By the State's own account, agents here did not go to Mr. Andrews's service provider with a request that it install a pen register device or otherwise record information regarding Mr. Andrews's calls and location. App. Br. at 3. The agents instead cut out the middleman by intercepting Mr. Andrews's communications with his cellular service provider. In short, they installed the cellular equivalent of a wiretap. There can be no doubt that this was a search.

D. The Nature of Information Intercepted by Cell-Site Simulators Does Not Diminish Citizens' Reasonable Expectations of Privacy.

The State implies that communications with our telephone service providers regarding our device identifiers, locations, and call data is subject to direct interception because it is less intimate than the contents of our telephonic communications. App. Br. at 10. This is unavailing. As the Supreme Court explained in *Kyllo v. United States*, courts are not in the business of parsing degrees of intimacy in conduct and communications when it comes to evaluating Fourth Amendment interests. 533 U.S. 27, 37-39 (2001). If we have a reasonable expectation of privacy against interception of communications with our cellular service providers, then interception of those communications by law enforcement is a search, regardless of how intimate or non-intimate the contents. *See also Riley*, 134 S. Ct. at 2492-93 (refusing to draw Fourth Amendment distinctions between "smartphones" versus older "flip" phones based on the information each contains). Moreover, as Justice Sotomayor pointed out recently in *United States v. Jones*, a person's location and contact information can be extremely revealing of very intimate conduct and associations. *See* 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring). The Court has since cited Justice Sotomayor's views on this point with approval. *See Riley*, 134 S. Ct. at 2490.

Recent legislative and executive actions offer additional evidence that we have reasonable expectations of privacy against the direct interception of call and location information by cell-site simulators. For example, Maryland law requires that police obtain a warrant backed by probable cause before deploying or using cell-site simulators.

Md. Code Ann., Crim. Proc. § 1-203.1 (2015). The Department of Justice also requires that federal agents obtain a warrant before deploying or using cell-site simulators. Dept. of Justice Mem. at 3. Given this evidence, and in light of existing Fourth Amendment doctrine, there should be no doubt that the use of cell-site simulators to intercept private communications between users and their cellular service providers constitutes a search for purposes of the Fourth Amendment.

E. The Public Observation Doctrine Does Not Authorize the Warrantless Use of Cell-Site Simulators.

The State also appeals to the public observation doctrine in defense of its claim that intercepting private communications and acquiring location information using cell-site simulators is not a search for purposes of the Fourth Amendment. App. Br. at 11-13. The public observation doctrine allows government agents to make direct observations from lawful vantage points. Thus, officers may monitor our movements along public streets from their patrol cars. *See United States v. Knotts*, 460 U.S. 276 (1983). That is not what happened here, however. Here, officers used Mr. Andrews's phone as a tracking device in order to determine his location in a private dwelling. App. Br. at 3. As the Supreme Court held in *United States v. Karo*, 468 U.S. 705 (1984), that is a search.

The State attempts to distinguish *Karo* by arguing that its agents gathered emanations from Mr. Andrews's phone that passed through the walls of the dwelling. App. Br. at 11-12. It is hard to see how that would make any difference from a Fourth Amendment point of view, particularly in light of the Supreme Court's decision in *Kyllo v. United States*, 533 U.S. 27 (2001). There, as in *Karo*, the critical distinction was between using technology to gather information about what is inside a home versus what is in public. *See Kyllo*, 533 U.S. at 34 ("We think that obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search, at least where (as here) the technology in question is not in general public use.") (internal citation omitted)); *Karo*, 468 U.S. at 714 (holding that the "monitoring of a beeper in a private residence, a location not opened to visual

surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."). Here, officers used their device to gather information from inside a home. By definition, that was a search because their device both allowed them to gather information not otherwise available without a physical trespass and is not in general public use.

II. The Use of Cell-Site Simulators Absent a Warrant is Unreasonable.

The central question raised on this appeal is not whether law enforcement officers should be allowed use cell-site simulators to investigate and prosecute crime. They certainly should. The question instead is whether they should have unfettered discretion to use these devices whenever they like, free of Fourth Amendment constraint. In this regard, the State finds itself in the same posture as the Solicitor General in *Jones*, where the Department of Justice sought an unlimited license to use GPS tracking technology. During oral argument in *Jones*, Chief Justice Roberts identified the consequence of granting such a license by asking the Solicitor General a pointed question:

> You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory? . . . you could tomorrow decide [to] put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?

Trs. of Oral Argument at 9-10, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), available at http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf. As the Chief Justice recognized, the consequence of granting law enforcement unfettered access to surveillance technology is that it would license broad and indiscriminate surveillance, allowing the government to monitor anyone, anywhere, and anytime, for good reasons, for bad reasons, or for no reasons at all. It is hard to imagine a more direct threat to the right of the people to be secure against unreasonable searches.

In this case, the State demands precisely this sort of unlimited license. It seeks authority free from constitutional encumbrance to use cell-site simulators to intercept private communications between all citizens of Maryland, including the judges of this

Court, and their cellular service providers. It also asks for an unlimited license, free from Fourth Amendment constraint, to locate any citizen of Maryland, including the judges of this Court, anytime and anywhere by using their phones as personal tracking devices. That is an astonishing demand, particularly in light of the technology in question.

Cell-site simulators cast indiscriminate dragnets, intercepting communications from every user device within their areas of operation. Deployed on the streets of Baltimore or Annapolis, cell-site simulators surveil thousands of innocent citizens. Given these capacities, there can be no doubt that granting the State an unlimited license to deploy and use cell-site simulators would threaten the security of the people of Maryland against unreasonable searches. This Court should therefore reject the State's request by enforcing constitutional constraints on law enforcement's authority to deploy and use cell-site simulators.

A. Founding-Era Concerns with General Warrants Reveal the Role of the Fourth Amendment in Guarding Against Threats of Broad, Indiscriminate Surveillance.

"The Fourth Amendment . . . erects a wall between a free society and overzealous police action—a line of defense implemented by the framers to protect individuals from the tyranny of the police state." Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. Rev. 409, 444 (2007). Those who read the Fourth Amendment in 1791 had a particular example of this sort of tyranny in mind: general warrants and writs of assistance.

The Fourth Amendment's principal bêtes noires were general warrants, including writs of assistance. *See Riley*, 134 S. Ct. at 2494. By 1791, the common law had rejected general warrants. *See Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931). Among the primary reasons courts gave for outlawing general warrants was the threat they posed to the security of the people by granting government agents broad authority to conduct indiscriminate searches and seizures. *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 366 (1974) ("[T]he primary abuse thought to characterize the general warrants and the writs of assistance was their

indiscriminate quality, the license that they gave to search Everyman without particularized cause, the fact that they were—as Wilkes proclaimed Lord Halifax's warrant for the authors and publishers of No. 45 of the North Briton—'a ridiculous warrant against the whole English nation.'"). These courts reasoned that nobody could feel secure if forced to live under a regime where executive agents had unfettered discretion to search whomever they pleased, whenever they liked, for good reasons, for bad reasons, or for no reasons at all. Thus, in the General Warrant cases, Lord Camden notes that, if a government can grant "discretionary power . . . to messengers to search wherever their suspicions may chance to fall . . . it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject." *Wilkes v. Wood*, 98 Eng. Rep. 489 (1763). *See also Entick v. Carrington*, 19 Howell's State Trials 1029 (1765) ("we can safely say there is no law in this country to justify [searches pursuant to general warrants]; if there was, it would destroy all the comforts of society").

Although English citizens enjoyed common law protections against general warrants in the late eighteenth century, those rights were abrogated by statute in the colonies, where British authorities had access to writs of assistance. The very idea that executive agents could secure such broad authority to conduct indiscriminate searches caused grave concerns among the founding generation. Take, for example, James Otis's famous Writs of Assistance speech, which John Adams would later identify as "'the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child of Independence was born'" *Riley*, 134 S. Ct. at 2494 (quoting 10 Works of John Adams 248 (C. Adams ed. 1856)). There, Otis, condemned general warrants as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law-book." James Otis, *Against Writs of Assistance*, (Feb. 24, 1761).

These founding-era concerns carry through to the modern era. Thus, Justice Jackson advises in *Johnson v. United States* that "[t]he right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society

which chooses to dwell in reasonable security and freedom from surveillance." 333 U.S. 10, 14 (1948). *See also Berger*, 388 U.S. at 53 ("The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society.") (internal citation and quotation marks omitted).

B. Granting an Unlimited License to Operate Cell-Site Simulators Would Authorize Broad and Indiscriminate Surveillance Akin to a General Warrant.

On this appeal, the State seeks a general, unlimited license to intercept communications and surveil citizens using cell-site simulators. That kind of broad authority free of constitutional encumbrance is, in essence, a general warrant, and therefore should be rejected.

There can be no doubt that leaving to the police the technological means to intercept private communications between cellular phone users and their service providers would constitute an unreasonable search. *See Osborn v. United States*, 385 U.S. 323, 329 n.7 (1966) (The "indiscriminate use [of eavesdropping] devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments, and imposes a heavier responsibility on this Court in its supervision of the fairness of procedures. . . ."). To hold otherwise would put in jeopardy the Supreme Court's holding in *Katz v. United States*¸ 389 U.S. 347 (1967). It would also cut against an important thread of the Supreme Court's contemporary jurisprudence, which seeks to limit law enforcement's access to emerging surveillance technologies.

For example, in *Kyllo*, the Supreme Court held that granting law enforcement access to heat detection devices absent a warrant would be unreasonable. 533 U.S. 27, 40 (2001). More recently, a majority of the Court warned against granting unfettered access to modern location tracking technologies. *See United States v. Jones*, 132 S. Ct. 945, 954 (Sotomayor, J, concurring); *id.* at 957 (Alito, J., concurring). In each of these cases, the Court warned about the dangers of allowing emerging technologies to erode our basic right to be free from the threat of constant government surveillance. *See Jones*, 132 S. Ct. at 954, (Sotomayor, J., concurring) (expressing fears that allowing government agents

unfettered access to technologically-enhanced surveillance "chills association and expressive freedoms . . . alter[ing] the relationship between citizen and government in a way that is inimical to democratic society") (internal citation omitted); *Kyllo*, 533 U.S. at 34 (warning that courts must not "permit police technology to erode the privacy guaranteed by the Fourth Amendment."). Those concerns are immediately relevant here. Cell-site simulators have the capacity to cast dragnets, capturing in a purely indiscriminate manner private communications and location information from thousands of users. That is precisely the kind of general threat that animated founding-era concerns with general warrants.

The degree and scope of the threat posed by cell-site simulators is evidenced further by the State's suggestion that, if we really want to avoid surveillance by cell-site simulators, we should turn off our phones. App. Br. at 13. It is hard to imagine a world more upside down from a Fourth Amendment point of view. The solution to threats of broad and indiscriminate search is not to ask citizens to "live dark and cloistered lives." *Palimieri v. Lynch*, 392 F.3d 73, 97 (2d Cir. 2005) (Straub, J., dissenting). "This much withdrawal is not required in order to claim the benefit of the amendment because, if it were, the amendment's benefit would be too stingy to preserve the kind of open society to which we are committed and in which the amendment is supposed to function." Amsterdam, 58 Minn. L. Rev. at 402. Moreover, "placing pressure on persons to return to their individual 'private' worlds to seek refuge from government searches and surveillance diminishes the public sphere's security." Thomas M. Crocker, *The Political Fourth Amendment*, 88 Wash. U. L. Rev. 303, 369 (2010). The better course, the course demanded by the Fourth Amendment itself, is to limit law enforcement's access to cell-site simulators.

C. Access to Cell-Site Simulators Should Be Subject to a Warrant Requirement.

The State would prefer that we simply trust its judgment rather than imposing constitutional constraints on its access to cell-site simulators. As Justice Sotomayor recently reminded us, this is both unwise and contrary to our constitutional tradition. *See*

Jones, 132 S. Ct. at 946 (Sotomayor, J., concurring) ("I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'") (internal citation omitted). "The guarantee against unreasonable searches and seizures was written and should be read to assure that any and every form of such interference is at least regulated by fundamental law so that it may be restrained within proper bounds." Amsterdam, 58 Minn. L. Rev. at 400. In this case, history and experience teaches that the best form of legal restraint is the warrant requirement. *See Katz v. United States*, 389 U.S. 347, 356-57 (1967).

In order to preserve and guarantee the security of the people against threats posed by general warrants, the Fourth Amendment bans general warrants and sets limits on the issuance of specific warrants. *See* Silas Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 Am. Crim. L. Rev. 1389, 1393 (1989) (The founders "sought to prohibit the newly formed government from using general warrants, a device they believed jeopardized the liberty of every citizen."). In so doing, it provides critical guarantees for the security of the people by interposing courts between citizens and executive agents and by limiting legislative authority to license searches and seizures. "Any other rule," Justice Jackson tells us, "would undermine 'the right of the people to be secure in their persons, houses, papers and effects,' and would obliterate one of the most fundamental distinctions between our form of government, where officers are under the law, and the police state where they are the law." *Johnson*, 333 U.S. at 17.

In keeping with both that tradition and the historical example provided by the Fourth Amendment itself, this Court should hold that deployment and use of cell-site simulators absent a warrant is unreasonable and therefore unconstitutional. In so doing, the Court would join both the Maryland legislature, which has established a statutory warrant requirement for the use of cell-site simulators, *see* Md. Code Ann., Crim. Proc. § 1-203.1 (2015), and the Department of Justice, which requires that federal agents secure a warrant before deploying or using cell-site simulators, *see* Dept. of Justice Mem. at 3.

D. Maryland's Statutory Regulation of Cell-Site Simulators Does Not Moot the Constitutional Question Presented in this Case.

In 2015, Maryland adopted an amendment to its Criminal Procedure Code requiring that police obtain a warrant backed by probable cause before deploying or using cell site simulators. *See* Md. Code Ann., Crim. Proc. § 1-203.1 (2015). Although this is a wise intervention, it does not moot the constitutional question raised on this appeal. As the founding generation was well aware, statutory and common law protections are subject to the whim of the political moment and are particularly vulnerable to claims of executive necessity. *See, e.g.*, A Maryland Farmer, no. 1 (1788) ("[S]uppose for instance, that an officer of the United States should force the house, the asylum of a citizen, by virtue of a general warrant, I would ask, are general warrants illegal by the constitution of the United States? . . . I fear not, especially in those cases which may strongly interest the passions of government, and in such only have general warrants been used."); The Canadian Freeholder: Dialogue II, 243-44 (1779) (noting that executives are "fond of doctrines of reason of state, and state necessity, and the impossibility of providing for great emergencies and extraordinary cases, without a discretionary power in the crown to proceed sometimes by uncommon methods not agreeable to the known forms of law"). These concerns are as salient today as they were in the eighteenth century and the need for constitutional protections just as great. *See Florida v. Royer*, 460 U.S. 491, 513 (1983) (Brennan, J., concurring) ("In times of unrest, whether caused by crime or racial conflict or fear of internal subversion, this basic law and the values that it represents may appear unrealistic or 'extravagant' to some. But the values were those of the authors of our fundamental constitutional concepts."); *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) ("We must not allow our zeal for effective law enforcement to blind us to the peril to our free society that lies in this Court's disregard of the protections afforded by the Fourth Amendment.").

The Fourth Amendment exists to guard against political temptations of the moment, guaranteeing rights despite the political process. Although the legislature has done well to regulate access to cell site simulators, the framework it prescribes does not

provide the same security as constitutional guarantees simply by virtue of its legislative status. This court should therefore hold that the Fourth Amendment requires a warrant for the deployment and use of cell site simulators.

CONCLUSION

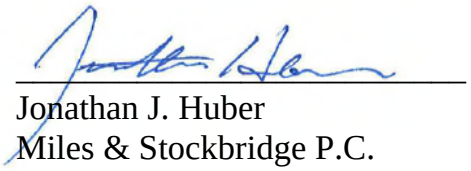
Left to the unfettered discretion of government agents, licenses to use cell-site simulators represent a contemporary threat to the security of the people against unreasonable searches directly akin to general warrants and writs of assistance. Just as did general warrants and writs of assistance, cell-site simulators facilitate broad searches, allowing police to gather information about hundreds or thousands of citizens within their areas of operation. Just as did general warrants and writs of assistance, cell-site simulators facilitate indiscriminate searches, providing information about citizens no matter who they are, be they suspects or unlucky passersby, and no matter where they are, be they in their homes or on public streets. Despite these capacities, the State contends that law enforcement officers should have unfettered discretion to deploy and use cell-site simulators free from Fourth Amendment constraint. As a resident of Baltimore and firm believer in the role of the Fourth Amendment in our constitutional democracy, Professor Gray, as amicus curiae, submits that this contention must be rejected.

STATEMENT OF FONT SIZE AND TYPE

The Brief of Professor David Gray as *Amicus Curiae* is printed in Times New Roman 13 point.

Dated: December 29, 2015

Respectfully submitted,



Jonathan J. Huber
Miles & Stockbridge P.C.
100 Light Street
Baltimore, Maryland 21202
(410) 385-3450
jhuber@milesstockbridge.com

Counsel for Amicus Curiae *Professor David Gray*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 29th day of December, 2015, two copies of the Brief of Professor David Gray as *Amicus Curiae* were mailed via first-class mail, postage prepaid, to each of the following:

Robert Taylor, Jr.
Assistant Attorney General
Office of the Attorney General
Criminal Appeals Division
200 Saint Paul Place
Baltimore, Maryland 21202

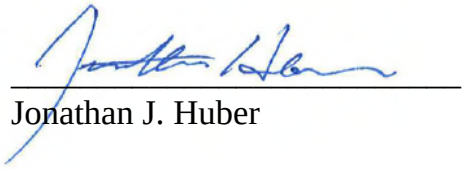
Counsel for Appellant

Daniel Kobrin
Office of the Public Defender
Appellate Division
6 St. Paul Street, Suite 1302
Baltimore, Maryland 21202

Counsel for Appellee

David Rocah
ACLU of Maryland Foundation
3600 Clipper Mill Road, Suite 350
Baltimore, Maryland 21211

Counsel for Amici Curiae *American Civil Liberties Union, American Civil Liberties Union of Maryland, and Electronic Frontier Foundation*



Jonathan J. Huber