# The Outer Limits: IMSI-Catchers, Technology, and the Future of the Fourth Amendment

*Abstract*

*Recent advances in technology are posing new challenges for a legal system based on decades-old precedent. Nowhere is this more apparent than in law enforcement's warrantless use of IMSI-Catchers. These devices mimic a cell phone tower, and when the device is activated, cell phones will naturally connect to them. Law enforcement officers can use those intercepted cell phone signals to track a suspect's movements in real time with startling accuracy. Scholarly commentary on these devices has largely concluded that their use requires a warrant. This Comment engages in a close examination of Fourth Amendment precedent and argues that, as much as we might wish otherwise, the use of these devices is justified under existing case law. The Fourth Amendment generally protects what a person seeks to keep private, but in a technologically connected world, the public has willingly traded privacy for convenience. Thus, if we are to maintain our privacy in an increasingly technological world, we might require either a rethinking of the precedent underpinning the Fourth Amendment or a proactive Legislature to step in and fill the gap that exists between an eighteenth century Amendment and a twenty-first century world.*

TABLE OF CONTENTS

## I. INTRODUCTION

*I've come up with a set of rules that describe our reactions to technologies:*

1. *Anything that is in the world when you're born is normal and ordinary and is just a natural part of the way the world works.*
2. *Anything that's invented between when you're fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it.*
3. *Anything invented after you're thirty-five is against the natural order of things.*[1]

Depending on one's perspective, technology will either be the gateway to humanity's future or the harbinger of its destruction. Regardless of these extremes, technology will continue to forward society's inexorable march into the unknown, while everyone else will have to find ways to catch up. As society moves further into the twenty-first century, the law is struggling to adapt to rapidly changing technologies that the public barely has time to understand before the technologies become obsolete.[2]

This Comment examines Fourth Amendment precedent's limited application to new technology through the lens of law enforcement's use of IMSI-Catchers; commonly referred to by the brand name "StingRay"—the most popular and well-known model of IMSI-Catchers.[3] If cell phones are the dream of a technological future, privacy advocates would argue that StingRays are its nightmare.[4] Using an IMSI-Catcher, law enforcement

1. DOUGLAS ADAMS, THE SALMON OF DOUBT: HITCHHIKING THE GALAXY ONE LAST TIME 95 (2002).

2. *See* Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

3. Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and a Lot Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 142 (2013) [hereinafter *A Lot More*].

4. *See id*. at 143 ("Whether installed in a vehicle, mounted on a drone, or carried by hand, this unregulated and technologically unmediated surveillance technology can, for example, send signals through the walls of homes to locate and identify nearby cell phones without the assistance of a wireless carrier and without providing any notice to the targets of the surveillance operation.").

officers are able to track a person's location and movements with startling accuracy by intercepting the person's cell phone signals.[5] The use of these devices is unregulated by the Fourth Amendment, and many scholars have called for their use to be controlled, either through the Fourth Amendment[6] or through statutory reform.[7]

This Comment endorses the need for reform in the use of IMSI-Catchers, but unlike previous works, does so by arguing that the use of these devices falls outside the restrictions imposed by existing precedent and is therefore not a search within the meaning of the Fourth Amendment.[8] Part II begins by describing the underlying technology of cell phones and IMSI-Catchers.[9] Part III proceeds to lay out the relevant legal authorities.[10] Part IV then analyzes how the Supreme Court might hold that the use of an IMSI-Catcher does not require a warrant under existing law.[11] Finally, Part V examines the limitations of Fourth Amendment precedent when applied to technology and concludes that the Legislature and not the Court is the ideal means of satisfying the privacy concerns of the people.[12]

## II. OF CELL PHONES AND STINGRAYS

Cellular technology has advanced rapidly over the period of a few short decades,[13] and there is a great deal of confusion concerning tracking devices with "various colorful and ominous names."[14] To help clarify the

5. *See infra* Section II.B.

6. *See* C. Justin Brown & Kasha M. Leese, *StingRay Devices Usher in a New Fourth Amendment Battleground*, 39 CHAMPION 12, 14 (2015).

7. *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 230–31 (2014).

8. *See infra* Part IV.

9. *See infra* Part II.

10. *See infra* Part III.

11. *See infra* Part IV.

12. *See infra* Part V.

13. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("A smart phone . . . was unheard of ten years ago . . . . Even less sophisticated phones . . . have been around for less than 15 years."). In that short time, cell phones have become one of the primary means of communication for Americans. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("[A]s of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.").

14. Owsley, *supra* note 7, at 185. Some of these names include the "TriggerFish, StingRay, AmberJack, KingFish, LoggerHead, Gossamer, Harpoon, Hailstorm, International Mobile Subscriber Identifier ("IMSI") catcher, Electronic Serial Number ("ESN") reader, cell site simulator,

technological landscape, this Part begins with an introduction to cellular technology and proceeds to breakdown the technological features of IMSI-Catchers.[15]

### *A. Cell Phones, Base Stations, and Mobile Communications Technology*

Cellular technology operates as a hierarchy of multiple network levels that interact to ensure that the network functions as a whole.[16] At the smallest level are "mobile stations," which are the cell phones individual subscribers own and use on a daily basis.[17] To connect these phones to the network, service providers divide geographic areas into "honeycomb-shaped segments or 'cells'—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters."[18] Thus, the local "base station" receives the signals from the in-area phones and facilitates their connection to the broader network.[19]

The connection process begins with a removable Subscriber Identification Module (SIM) card contained within each phone.[20] Each SIM card has a unique fifteen-digit International Mobile Subscriber Identity (IMSI) number.[21] The IMSI number is linked to the SIM card and primarily assists in identifying the subscriber connecting to the network.[22] When a cell phone is turned on, it automatically connects to the base station with the strongest signal[23] and then transmits this number as part of a registration and authentication process.[24] By connecting to the strongest signal, the phone is able "to optimize the reception. If there are more than one Base Station of

---

[and] digital analyzer." *Id*.

15. *See infra* Sections II.A–B.

16. *See* DAEHYUN STROBEL, IMSI CATCHER 3 (2007), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

17. *See id*. at 4.

18. S. REP. NO. 99-541, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3563.

19. *See* STROBEL, *supra* note 16, at 4. Base stations are commonly referred to as "cell towers," though they may also be placed atop other objects. *See* Owsley, *supra* note 7, at 188.

20. *See* STROBEL, *supra* note 16, at 4.

21. *Id*. Each IMSI number is comprised of a three digit "mobile country code," a two-to-three digit "mobile network code" and a maximum ten digit "mobile subscriber identification number." *Id*.

22. *Id*. In contrast to an IMSI number, an International Mobile Equipment Identity (IMEI) number is unique to the phone itself and identifies only the hardware. *Id*.

23. *See id*. at 13.

24. *See* Owsley, *supra* note 7, at 188–89.

the subscribed network operator accessible, it will always choose the one, with the strongest signal."[25] To maintain the ongoing connection, the phone re-registers with the base station approximately every seven seconds.[26] Upon the initial registration, the network assigns the phone a Temporary Mobile Subscriber Identity (TMSI) number.[27] Every subsequent re-registration will transmit the TMSI number instead of the IMSI number.[28] This authentication process is one-sided, meaning the phone must prove its authorization to the base station to connect to the network, but the base station does not have to prove anything to the phone.[29]

### *B. StingRays and Cell Phone Tracking*

An important caveat in the discussion of IMSI-Catchers is that the exact technical specifications and procedures of their use remain unclear, in large part because the police departments that use them are required to sign nondisclosure agreements as a purchase condition.[30] Law enforcement officers go to extreme lengths to conceal their use of IMSI-Catchers, often stating that they discovered location information from a "confidential source" in lieu of revealing that they used one of these devices.[31] These

25. STROBEL, *supra* note 16, at 13.

26. *See* Owsley, *supra* note 7, at 188.

27. STROBEL, *supra* note 16, at 6.

28. *Id*.

29. *See id* at 7. Upgraded 3G and 4G networks do feature two-sided authentication, but the traditional cellular frequencies that rely on one-sided authentication are still available and utilized by all cell phones. *See* 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, 12 n.52 (2014) [hereinafter *Secret Stingray*].

30. *See* John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 08, 2013), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsapolice/3902809/ ("Most police aren't talking, either, partly because [the StingRay manufacturer] requires buyers to sign a non-disclosure agreement."). The FCC grants special licenses to the manufacturers of IMSI-Catchers so that they can be sold to state and local agencies. *See* Jason Leopold, *DC Police, the FBI, and Their Secret Agreement to Hide Cell Phone Spying*, VICE NEWS (Sep. 30, 2015, 11:45 AM), https://news.vice.com/article/dc-police-the-fbi-and-their-secret-agreement-to-hide-cell-phone-spying. The FBI is required to approve each sale and made the nondisclosure agreement a requirement in all of them. *Id*.

31. *See* Nicky Woolf, *2,000 Cases May Be Overturned Because Police Used Secret Stingray Surveillance*, GUARDIAN (Sep. 4, 2015, 2:09 PM), http://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance.

agreements even extend as far as prosecutors dismissing court cases to avoid the risk of exposing technical details.[32] As a result, prosecutors across the country have dismissed cases against defendants that would otherwise result in certain convictions.[33] Additionally, federal agencies have been slow to respond to legal requests for information and have heavily redacted released documents related to the procedures and specifications of these devices.[34]

IMSI-Catchers function by taking advantage of two features of mobile network design.[35] The first is the optimization feature that requires the phone to connect to the strongest tower.[36] The second is the one-sided authentication and registration process.[37] Thus, when law enforcement officers activate an IMSI-Catcher, the nearest cell phones will connect to it by design without verifying that it is a genuine base station.[38] While the initial connection process encompasses all the cell phones that "identify the simulator as the most attractive cell tower" in the immediate area, the IMSI-Catcher can narrow its ongoing connection so that "it will obtain the signaling information relating only to that particular phone."[39] The result is that the IMSI-Catcher operates as a "man-in-the-middle attack" where the Catcher tricks the phone into thinking it is a base station while

32. *See* Leopold, *supra* note 30 ("The MPD also agreed that if the department learned that any technical details about the surveillance technology was at risk of being exposed during a judicial proceeding, MPD would contact the FBI so the bureau could ask MPD to 'seek dismissal of the case' in order to continue protecting the overall secrecy of the Stingray.").

33. *See, e.g.*, Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, STL TODAY, (Apr. 19, 2015), http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html ("Just one day before a city police officer was to face questions about a secret device used to locate suspects in a violent robbery spree, prosecutors dropped more than a dozen charges against the three defendants.").

34. *See* Ryan Gallagher, *FBI Accused of Dragging Feet on Release of Info About "Stingray" Surveillance Technology*, SLATE: FUTURE TENSE (Oct. 19, 2012, 4:00 PM), http://www.slate.com/blogs/future_tense/2012/10/19/stingray_imsi_fbi_accused_by_epic_of_dragging_feet_on_releasing_documents.html ("The meager 67 pages were heavily redacted—containing only a glossary of jargon that related to cell networks along with blanked out copies of an internal manual called 'GSM cell phone tracking for dummies.'").

35. *See* STROBEL, *supra* note 16, at 13–14.

36. *See id.* at 13.

37. *See id.* at 7.

38. *Id.* at 13. In this sense, the IMSI-Catcher is simulating a cell tower, meaning that it is within a class of devices called "cell site simulators." *See* Brown & Leese, *supra* note 6, at 13.

39. *See* DEP'T OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 2 (2015), https://www.justice.gov/opa/file/767321/download [hereinafter DOJ POLICY].

simultaneously tricking the real base station into thinking the Catcher is just another phone.[40] Once connected, the IMSI-Catcher submits a "special identity request" to the mobile phone, causing it to continuously transmit its IMSI number instead of its TMSI number.[41] Because the TMSI number helps prevent tracking and identification, this identity request enables the Catcher to overcome this preventative barrier.[42] Thus, the IMSI-Catcher will receive the phone's permanent IMSI number upon every subsequent re-registration.[43]

This signal connection process can have some unintended side effects. Early model IMSI-Catchers substantially interfered with the phone's connection to the network, making it impossible for the tracked subscriber to receive incoming calls.[44] More recently, federal agents stated in a sealed document related to the use of IMSI-Catchers that these devices have the "potential" to disrupt some cellular communications for a small number of users,[45] implying that most users would not experience any disruption of their service.[46] At the same time, IMSI-Catcher manufacturers claim that their devices are undetectable.[47] Because individuals would likely notice service interruptions, modern IMSI-Catchers may be undetectable—not significantly interfering with cell signals. [48]

40. *See* STROBEL, *supra* note 16, at 13–14 fig.4.1. This process can vary somewhat depending on the type of cellular network the IMSI-Catcher is attempting to interface with; however, the result is the same. *See id*. at 15–16 (describing the connection process between an IMSI-Catcher and a Universal Mobile Telecommunications System (UMTS) network).

41. *Id*. at 13.

42. *See id*. at 6.

43. *See id*.

44. *Id*. at 14 ("The subscriber has no direct connection to the network operator. Hence, he is not approachable for incoming calls.").

45. Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015, 4:55 PM), http://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/ (emphasis added) ("'Because of the way, the Mobile Equipment sometimes operates,' Scimeca wrote in his application, 'its use has the *potential* to intermittently disrupt cellular service to a *small fraction* of Sprint's wireless customers within its immediate vicinity.'").

46. *See id*.

47. *Active GSM Monitoring System with IMSI Catcher and Decryption Unit*, PKI ELECTRONIC INTELLIGENCE, http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system-with-imsi-catcher-and-decryption-unit/ (last visited Mar. 2, 2017) ("In spite of its numerous features, the PKI 1560 works in a complete transparent manner and remains absolutely undetectable.").

48. This conclusion is based, in part, on the widespread use of IMSI-Catchers in thousands of investigations. *See infra* note 60 and accompanying text.

Law enforcement officers use IMSI-Catchers to track the location of mobile devices and, presumably, the suspects who carry them.[49] The actual location tracking requires the addition of a directional antenna and a mapping program.[50] Once the IMSI-Catcher establishes a connection with a phone's signal, it "measures its strength and can provide a general location on the map. The officer can then move to another location and again measure the signal strength. By collecting the signaling information from several locations, the system can triangulate the location of the phone more precisely."[51]

Public information about the accuracy of IMSI-Catchers is thin, largely because of the secrecy that surrounds them.[52] A base station utilized by a network provider is generally capable of locating a cell phone to within fifty meters of its actual location.[53] IMSI-Catchers improve upon that accuracy to "within [twenty-five] feet of actual location anywhere in the United States."[54] At least some models currently for sale claim even greater accuracy and are capable of locating a cell phone to within two meters of its

49. *See* DOJ POLICY, *supra* note 39. The first IMSI-Catcher was invented in 1996 for the purpose of identifying subscribers. *See* STROBEL, *supra* note 16, at 13. By 1997, in addition to identifying subscribers, IMSI-Catchers could tap phone calls. *Id*. While IMSI-Catchers may be technically capable of wiretap functions, they are expressly restricted from collecting content. *See* DOJ POLICY, *supra* note 39 ("[T]he simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone.").

50. Jennifer Valentino-Devries, *How 'Stingray' Devices Work*, WALL STREET J. (Sep. 21, 2011, 10:33 PM), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/. Even with these additional components, the final device remains quite small and readily mobile; *see* Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015, 7:51 AM), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ (describing the device as "suitcase-size"); HARRIS CORP., STINGRAY PRODUCT DESCRIPTION 1, http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (describing the device as "designed for vehicular operations") (last visited Mar. 2, 2017).

51. Valentino-Devries, *supra* note 50. There are two main methods for an IMSI-Catcher to make the initial connection. *Id*. The first is by targeting a specific location and analyzing the numbers captured there. *Id*. The second is used where the number is known, but the phone's location is not; thus, police can search a larger area until they locate the specific number they are seeking. *See* Owsley, *supra* note 7, at 193.

52. *See supra* notes 30–32 and accompanying text.

53. *See* Brad Leneis, Note, *Mapping a Way Out: Protecting Cellphone Location Information Without Starting over on the Fourth Amendment*, 50 AM. CRIM. L. REV. 499, 502 (2013).

54. *Secret Stingray*, *supra* note 29, at 11 n.44 (quoting Memorandum from Stephen W. Miko, Resource Manager, Anchorage Police Dep't to Bart Mauldin, Purchasing Officer, Anchorage Police Dep't (June 24, 2009), http://files/cloudprivacy.net/anchorage-pdharris-memo.pdf).

actual location,[55] thus being able to accurately track a phone's movements even over short distances.[56]

Professionally manufactured IMSI-Catchers are a substantial expense for a police department, costing up to $400,000.[57] But the basic components to construct one are readily available to anyone in the general public; individuals can build their own for as low as $1500.[58] The high cost of these devices has not deterred their purchase: over fifty law enforcement agencies have admitted that they utilize IMSI-Catchers in their investigations.[59] These agencies have used these devices for years on thousands of routine crime investigations.[60] While these are the only agencies known to possess them, the actual number is believed to be much higher,[61] in part because new agencies are regularly coming forward to admit that they use these devices.[62] However, one of the most routinely used devices in police investigation

55. *Active GSM Monitoring System with IMSI Catcher and Decryption Unit*, *supra* note 47.

56. *See id*.

57. *Secret Stingray*, *supra* note 29, at 46. Though these devices are expensive, most police departments can afford them because of federal antiterrorism grants. *See* Kelly, *supra* note 30.

58. Owsley, *supra* note 7, at 191 ("[T]hese days, a reasonably bright computer whiz with $1,500 can buy the raw components to make one.").

59. *See Stingray Tracking Devices: Who's Got Them?*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Mar. 2, 2017).

60. *See* Heath, *supra* note 50 ("In April, Det. Emmanuel Cabreja testified that [Baltimore police] officers had used cell-site simulators more than 4,300 times since 2007 . . . ."); Nathan Freed Wessler, *Police Citing "Terrorism" to Buy Stingrays Used Only for Ordinary Crimes*, AM. CIV. LIBERTIES UNION: FREE FUTURE (Oct. 23, 2015, 9:00 AM), https://www.aclu.org/blog/free-future/police-citing-terrorism-buy-stingrays-used-only-ordinary-crimes ("[T]he records show that the [Michigan state police] used its cell site simulators in 128 run-of-the-mill investigations last year . . . ."); Kate Martin, *Tacoma Police Admit to Cellphone Surveillance, Say They Don't Keep Data*, NEWS TRIB. (Aug. 27, 2014, 2:40 PM), http://www.thenewstribune.com/news/local/politics-government/article25878406.html ("Records show [Tacoma PD] has used the device 179 times since 2009—mostly for drug cases.").

61. *The StingRay's Tale*, ECONOMIST, Jan. 30, 2016, at 24, 26.

62. *See* Kim Zetter, *California Police Used Stingrays in Planes to Spy on Phones*, WIRED (Jan. 27, 2016, 6:28 PM), http://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/ ("The Anaheim Police Department has acknowledged in new documents that it uses surveillance devices known as Dirtboxes—plane-mounted stingrays—on aircraft flying above the Southern California city that is home to Disneyland, one of the most popular tourist destinations in the world."); Brad Heath, *U.S. Marshals Secretly Tracked 6,000 Cellphones*, USA TODAY (Feb. 23, 2016, 10:13 PM), http://www.usatoday.com/story/news/2016/02/23/us-marshals-service-cellphone-stingray/80785616/ ("The Marshals Service's surveillance log lists 5,975 cases in which the Marshals Service used stingrays. The agency declined to say what time period the log covered, or where the suspects were arrested. It also declined to identify the suspects, to protect their privacy.").

remains largely in the shadows.[63]

## III. THE LAY OF THE LAND

This Part will outline the current legal rules that govern the use of IMSI-Catchers.[64] It begins with a description of the traditional standard still utilized by many states before addressing the recent changes in state and federal law.[65] Lastly, because this Comment concerns the application of the Fourth Amendment, it concludes with a summation of relevant case law the Supreme Court might apply were it to review the use of IMSI-Catchers.[66]

### *A. The State of the Law*

The state of the law governing IMSI-Catchers can be most accurately summarized as "a chaotic, 'inconsistent legal landscape' that provides no clarity for law enforcement, courts, criminal defense attorneys or those citizens and advocacy organizations interested [in] the protection of privacy."[67]

#### 1. Traditional Statutory Authority

Sometime around 2005, in the absence of clear statutory guidance, the Department of Justice (DOJ) created a court order referred to as a "hybrid order" to establish its legal authority to gather real-time location data.[68] The hybrid order combined elements of a Pen or Trap court order[69] and a Stored Communications Act "D" order.[70] The relevant part of the Pen or Trap order

63. *See* Heath, *supra* note 50.

64. *See infra* Sections III.A–B.

65. *See infra* Section III.A.

66. *See infra* Section III.B.

67. *A Lot More*, *supra* note 3, at 151.

68. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Towards Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 134–35 (2012) [hereinafter *Can You See*].

69. *See* 18 U.S.C. § 3123 (2012). A pen register is a device that collects and records metadata from electronic communications, such as "dialing, routing, addressing, or signaling information . . . provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(3) (2012). Similarly, a trap and trace device records metadata used to identify the origin of electronic communications. § 3127(4).

70. *See* 18 U.S.C. § 2703(d) (2012).

states:

> Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.[71]

The relevant part of the "D" order states:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[72]

The DOJ was forced to take this action for two reasons: First, no existing federal statute explicitly governed the government's use of real-time cell phone tracking devices such as IMSI-Catchers.[73] Second, 47 U.S.C. § 1002 states that, "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber."[74] With the only legislative guidance stating that the Pen or Trap order alone could not authorize real-time location tracking, the DOJ believed that by combining a Pen or Trap order with a § 2703(d) order, it established the authority to legally use these devices.[75] The advantage of the hybrid order for the government is that judicial review is limited to such a degree that it is "ministerial in nature,"[76]

71. § 3123(a)(1).
72. § 2703(d).
73. *See A Lot More*, *supra* note 3, at 149–52.
74. 47 U.S.C. § 1002(a)(2)(B) (2012).
75. *See Can You See*, *supra* note 68, at 136.
76. *A Lot More*, *supra* note 3, at 156 n.86 (quoting United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995)).

because the controlling language of § 3123 states that "the court *shall enter* an ex parte order" if the prerequisites have been met.[77] Thus, the magistrate judge does not conduct an extensive review of the relevant facts surrounding the government's requested use.[78]

2. Developments in Federal and State Law

The hybrid order was the primary authority for the use of IMSI-Catchers until the DOJ announced a recent policy change.[79] In September 2015, effective immediately, all requests for the use of cell-site simulators would require a warrant.[80] This change "applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies."[81] While this change is significant, it has two fundamental limitations.[82] The first is that subsequent administrations can readily alter Justice Department policies, as they have no precedential authority.[83] The second is that the policy is only binding on federal agencies, leaving state governments to largely fall back on the old framework.[84] Though the new policy represents an important change, it is by no means a permanent regulation.

While the hybrid order may be the traditional framework, not every state relies upon it.[85] Several states have taken the lead by enacting laws requiring law enforcement officials to seek warrants before using cell-site simulators, including California,[86] Minnesota,[87] Utah,[88] Virginia,[89] and

77. 18 U.S.C. § 3123(a)(1)–(2) (2012) (emphasis added). The valid prerequisites for the order's issuance being the "specific and articulable facts" required by the D order. *See* § 2703(d).

78. *A Lot More*, *supra* note 3, at 156. *Contra Can You See*, *supra* note 68, at 137–39 (noting that several magistrate judges across the country have rejected the government's reliance on hybrid orders and demanded the government satisfy a higher standard). Thus, "a patchwork of non-binding magistrate and district court decisions has emerged." *A Lot More*, *supra* note 3, at 151.

79. *See infra* notes 80–81 and accompanying text.

80. Press Release, Dep't of Justice Office of Pub. Affairs, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators (Sept. 3, 2015), http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

81. *See* DOJ POLICY, *supra* note 39.

82. *Can You See*, *supra* note 68, at 139–40.

83. *See id*.

84. *Id*. at 140 n.85 ("A DOJ policy decision . . . has no binding authority on state or local law enforcement practices, and state investigators do not always follow DOJ policies.").

85. *See infra* notes 86–90.

86. Electronic Communications Privacy Act, 2015 Cal. Stat. 651 (codified at CAL. PENAL CODE

Washington.[90] At the same time, congressional representatives have begun to express interest in working to update regulations[91] and have proposed legislation that would require a warrant before law enforcement uses an IMSI-Catcher.[92] As this trend is a recent development in the law, it is too early to predict what other legislative changes may occur in the coming months.[93]

### *B. The Fourth Amendment and Reasonable Expectations of Privacy*

The Fourth Amendment states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[94] The seminal case that defines Fourth Amendment application to government surveillance is *Katz v. United States*.[95] In *Katz*, police officers attached a microphone to the outside of a phone booth and were able to record one-half of an incriminating phone call.[96] The Court rejected the parties' arguments surrounding "constitutionally protected area[s]" and instead declared, "the Fourth Amendment protects people, not places."[97] The Court established the dividing line on the principle that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an

§ 1546).

87. Act of May 16, 2014, 2014 Minn. Laws 278 (codified at MINN. STAT. § 626A.28).

88. Act of March 31, 2014, 2014 Utah Laws 223 (codified at UTAH CODE ANN. § 77-23c-103).

89. Act of March 10, 2015, 2015 Va. Acts 43 (codified at VA. CODE. ANN. § 19.2-70.3).

90. Act of May 11, 2015, 2015 Wash. Sess. Laws 222 (codified at WASH. REV. CODE § 9.73.260).

91. *See* Joe Mullin, *Bill Introduced to Criminalize Warrantless Cell Phone Surveillance*, ARS TECHNICA (Nov. 2, 2015, 10:49 AM), http://arstechnica.com/tech-policy/2015/11/utah-congressman-introduces-bill-to-limit-use-of-phone-watching-stingrays/.

92. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015).

93. *See supra* notes 91–92 and accompanying text.

94. U.S. CONST. amend. IV.

95. 389 U.S. 347 (1967).

96. *Id*. at 348.

97. *Id*. at 351. *But see* Minnesota v. Carter, 525 U.S. 83, 88 (1998) (citations omitted) ("[T]he extent to which the Fourth Amendment protects people may depend upon where those people are. We have held that 'capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.'").

area accessible to the public, may be constitutionally protected."[98] To aid in this understanding, Justice Harlan developed a two-part test to determine when a search occurs, stating that first, a person must have "an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[99] Later cases have formally adopted this test as the primary Fourth Amendment privacy standard.[100]

In contrast to *Katz*, the Court later narrowed Fourth Amendment protections by holding that police could install a pen register without a warrant to track the phone numbers a person dials.[101] In *Smith v. Maryland*, police had the phone company use a pen register to record the numbers Smith dialed from his home and discovered he was making threatening phone calls to a robbery victim.[102] The Court upheld the use of the device on two key principles.[103] The first was that the pen register only captured the "means of establishing communication" but not the content of any phone calls.[104] The second principle was that individuals could not claim to have an expectation of privacy when they knowingly send information out into the world and convey it to third parties.[105] The Court did not accept Smith's contention that he subjectively believed his actions were private, but instead applied its own reasoning.[106] The Court reasoned, "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial.

98. *Katz*, 389 U.S. at 351 (citations omitted); *see also* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that an expectation of privacy in trash bags left on a street was unreasonable because they were accessible to the public); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that an expectation of privacy in marijuana plants being grown in a suspect's backyard was unreasonable because they were exposed to an overhead police surveillance flight).

99. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

100. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012) (citations omitted) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'").

101. 442 U.S. 735, 745–46 (1979).

102. *Id*. at 737.

103. *Id*. at 741–42.

104. *Id*. at 741; *cf*. United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (holding that individuals have a reasonable expectation of privacy in the contents of their e-mails, despite the fact that they are conveyed to third parties).

105. *Smith*, 442 U.S. at 742; *see also* United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that an individual has no reasonable expectation of privacy in bank records because they are business documents knowingly exposed to the bank).

106. *Smith*, 442 U.S. at 742.

All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[107] The Court was unconcerned that most people may be "oblivious" to the "esoteric functions" of pen registers, but rather was satisfied that "they presumably have some awareness" of their use.[108] Thus, because the mere idea that phone calls inherently convey numbers had presumably permeated the public consciousness, the Court was satisfied that no search occurred.[109]

The use of technological devices for surveillance activities has continued to plague the Court over the years.[110] The matching cases of *United States v. Knotts*[111] and *United States v. Karo*[112] concerned the use of an electronic beeper to track chemicals used in drug production.[113] These cases' similar facts belie a key distinction: In *Knotts*, police used the beeper to track a suspect on public roads up until he entered a cabin,[114] whereas in *Karo*, police used the beeper to determine that the suspects had moved the chemicals into a home.[115] Thus, the Court upheld the tracking in *Knotts*, stating that individuals have no reasonable expectation of privacy in their public movements, because they are inherently conveying their location to the public.[116] However, the Court recognized in *Karo* that monitoring the beeper "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[117] Thus, when using a beeper to

107. *Id*.

108. *Id*. The Court relied on the fact that phone books notified individuals that phone companies could assist in identifying unwanted phone calls, even though this assurance contained no specific reference to pen registers. *Id*. at 742–43.

109. *Id*. at 743, 745–46.

110. *See infra* notes 111–18 and accompanying text.

111. 460 U.S. 276 (1983).

112. 468 U.S. 705 (1984).

113. *See Knotts*, 460 U.S. at 278 ("With the consent of the Hawkins Chemical Co., officers installed a beeper inside a five-gallon container of chloroform, one of the so-called 'precursor' chemicals used to manufacture illicit drugs."); *Karo*, 468 U.S. at 708 ("The Government obtained a court order authorizing the installation and monitoring of a beeper in one of the cans of ether.").

114. *Knotts*, 460 U.S. at 278–79 ("The record before us does not reveal that the beeper was used after the location in the area of the cabin had been initially determined.").

115. *Karo*, 468 U.S. at 709–10 ("When the vehicles left the Taos residence, agents determined, using the beeper monitor that the beeper can was still inside the house.").

116. *Knotts*, 460 U.S. at 281–82.

117. *Karo*, 468 U.S. at 715.

track movements, a warrant is required to reveal the intimate details of the home.[118]

In *Kyllo v. United States*, the Court again raised the issue of "intimate details" when it required a warrant for the use of a thermal imaging camera on a home.[119] Police observed a home from a street corner and used a thermal imager to determine that the house was emanating unusually high levels of heat.[120] Relying, in part, on this information to secure a warrant, the police discovered Kyllo was growing marijuana in his home.[121] In rejecting the government's use of the camera, the Court declared, "In the home . . . *all* details are intimate details, because the entire area is held safe from prying government eyes."[122] In lieu of a strict application of the *Katz* standard, the Court held "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."[123] While it is clear that the Court was attempting to create a bright line rule that would be a consistent standard for future cases,[124] the dissent raised the argument that "general public use" was, in fact, an ephemeral standard without clear guidance.[125] Although the significance of "general public use" is debatable, the guiding rule from *Kyllo* appears to be that the use of technology to reveal any details about the interior of the home is presumably a search that requires a warrant.[126]

118. *Id*. at 718.

119. 533 U.S. 27, 35–37 (2001).

120. *Id*. at 29–30.

121. *Id*. at 30.

122. *Id*. at 37.

123. *Id*. at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

124. *Id*. at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)) ("We have said that the Fourth Amendment draws 'a firm line at the entrance to the house.' That line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant.").

125. *Id*. at 47 (Stevens, J., dissenting). The majority dodged this argument by blaming precedent as having fixed the standard at "routine" technology. *Id*. at 39 n.6 (majority opinion) (quoting California v. Ciraolo, 476 U.S. 207, 215 (1986)). In *Ciraolo*, the Court upheld the use of a plane to fly over a suspect's backyard so that police could observe his illegal marijuana plants. 476 U.S. at 215. Despite the fact that police targeted the flight towards his home, Ciraolo had no reasonable expectation of privacy because he failed to protect his privacy against aircraft, which society routinely uses. *Id*.

126. *Kyllo*, 533 U.S. at 40.

Although decided on different grounds, *United States v. Jones* provides some insight into how the Court may decide location-tracking cases.[127] In *Jones*, officers violated the terms of their warrant and attached a GPS tracking device to the outside of a suspect's car.[128] The device then provided continuous tracking of the car's movements for a period of twenty-eight days.[129] The Court revived the trespass theory of the Fourth Amendment, holding that because police "physically occupied private property" by attaching the device to the car, they had violated the Fourth Amendment.[130]

While the Court's opinion is a new development in Fourth Amendment jurisprudence, the concurrences of Justice Alito[131] and Justice Sotomayor[132] are important to highlight. Justice Alito chose to apply the *Katz* test and held that individuals have a reasonable expectation of privacy against long-term location tracking because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[133] However, he affirmed the precedent that short-term location tracking does not violate the Fourth Amendment.[134] In contrast, Justice Sotomayor indicated in her concurrence that she would be willing to depart from past precedent and hold that all location tracking would likely violate the Fourth Amendment.[135]

Additionally, *Riley v. California* is important because it indicates the Court's awareness of the technological issues of the time.[136] *Riley* was a consolidation of two cases where police officers searched the contents of individuals' cell phones incident to their lawful arrests.[137] The Court distinguished the case from past precedent and noted that the justifications underpinning the search-incident-to-arrest exception did not justify the

127. 132 S. Ct. 945 (2012).
128. *Id*. at 948.
129. *Id*.
130. *Id*. at 949.
131. *Id*. at 957–64 (Alito, J., concurring in the judgment).
132. *Id*. at 954–57 (Sotomayor, J., concurring).
133. *Id*. at 964 (Alito, J., concurring in the judgment).
134. *Id*.
135. *Id*. at 954–57 (Sotomayor, J., concurring).
136. 134 S. Ct. 2473 (2014).
137. *Id*. at 2480 ("An officer searched Riley incident to the arrest and . . . accessed information on the phone . . . ."); *id*. at 2481 ("[A] police officer . . . . arrested Wurie and took him to the police station. At the station, the officers seized two cell phones from Wurie's person.").

search of the phones.[138] In doing so, the Court noted how widespread cell phone use had become in modern society and the extent to which they had become repositories of the intimate details of peoples' lives.[139] Thus, the Court held that an officer could not search the contents of a phone without a warrant.[140]

Although the Supreme Court has yet to take up the issue of cell-site location data, the circuit courts are beginning to address the issue. In *United States v. Skinner*, the Sixth Circuit had the opportunity to address real-time cell-site location data.[141] There, DEA agents used a court order to obtain real-time location information from Skinner's phone company.[142] Agents "pinged" the phone over the course of several days to determine Skinner's location before arresting him for numerous drug charges.[143] The appellate court upheld the tracking by reasoning that if a "voluntarily procured" device, such as a cell phone, "gives off a signal that can be tracked for location, certainly the police can track the signal."[144] Thus, because Skinner voluntarily carried an inherently trackable device, he had no reasonable expectation of privacy.[145]

*Skinner* dealt with a court order to obtain information from a third party,

138. *Id*. at 2485.

139. *Id*. at 2489–90.

140. *Id*. at 2495.

141. 690 F.3d 772 (6th Cir. 2012). In contrast to real-time cell-site tracking, multiple circuit courts have addressed historical cell-site tracking; they have established a pattern of the en banc court reversing a panel's decision that the tracking violated the Fourth Amendment. *See* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (holding that the third party doctrine forecloses on any expectation of privacy), *rev'g* 796 F.3d 332 (4th Cir. 2015); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (holding that the third party doctrine forecloses any expectation of privacy), *rev'g* 754 F.3d 1205 (11th Cir. 2014), *cert. denied*, 136 S. Ct. 479 (2015). While the policy concerns of historical tracking and real-time tracking overlap in part, historical cell-site data inherently deals with tracking over a longer period of time, thus increasing the possibility of piecing together the intimate details of a person's life. *See, e.g*., *Graham*, 796 F.3d at 341 (noting that the government obtained comprehensive location records for a 221-day time period). For a greater discussion on the "mosaic" theory of privacy in regards to location tracking, see *United States v. Jones*, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring). While a court may adopt a broad view of location tracking, these policy differences provide ready areas to distinguish historical cell-site tracking, real-time cell-site tracking, and IMSI-Catcher tracking. *See A Lot More*, *supra* note 3, at 151.

142. *Skinner*, 690 F.3d at 776.

143. *Id*.

144. *Id*. at 777.

145. *Id*. at 781.

but it remains the only federal appellate court to issue a decision on real-time cell phone tracking,[146] although the Seventh Circuit recently confronted the use of an IMSI-Catcher in *United States v. Patrick*.[147] Patrick had a warrant out for his arrest, and police obtained a second warrant to locate Patrick using cell phone data.[148] After the case was briefed on appeal, the government revealed that police had used an IMSI-Catcher to locate Patrick and arrest him.[149] The court recognized the complex Fourth Amendment issues inherent in an IMSI-Catcher's use, but declined to resolve them for two reasons.[150] First, the government "conceded for the purposes of this litigation that the use of a cell-site simulator is a search."[151] Second, there was a valid warrant, and Patrick was arrested in a public place.[152] Thus, the court believed it was "best to withhold full analysis [of the StingRay's use] until these issues control the outcome of a concrete case."[153]

In the absence of any on-point precedent, these cases provide the best guidance on how to address the privacy issues raised by IMSI-Catchers. Therefore, they can be instructive as to how other appellate courts, or even the Supreme Court, might apply Fourth Amendment principles to IMSI-Catchers and other cell-site simulators.

## IV. IMSI-CATCHERS AND THE FOURTH AMENDMENT

How might the Supreme Court review the use of IMSI-Catchers under the Fourth Amendment? Scholars who have worked to shed light on the government's use of IMSI-Catchers are in universal agreement that the device's use without a warrant violates the Fourth Amendment.[154] The fears

146. *A Lot More*, *supra* note 3, at 151.
147. 842 F.3d 540 (7th Cir. 2016).
148. *Id*. at 542.
149. *Id*.
150. *Id*. at 543–44.
151. *Id*. at 544.
152. *Id*. at 545.
153. *Id*.
154. *See* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1098 (2013) ("[W]e contend a warrant should always be obtained prior to the use of an IMSI catcher given the possibility that its use will lead to an intrusion into a protected space, most especially a home, but also an office, a hotel room, and the myriad of other spaces the Court has acknowledged give rise to a reasonable expectation of privacy."); Brown & Leese, *supra* note 6, at 14 ("Although no court has specifically reached this question, it is likely that the use of a cell site simulator

associated with these devices can best be summarized in this worst-case imagining of a group of people meeting in a home:

> By using a StingRay, the government could tell who is at the meeting (by reading the phones' IMSI signals), what is being discussed (by reading the content of messages), and even who left to use the restroom (by tracking a phone's movement). The potential for intrusion of this type is unbounded—and all the more reason it is a Fourth Amendment search for which a warrant should be required.[155]

Of course, existing policy and precedent can likely assuage the concern that the government is reading the contents of messages.[156] But the other concerns do remain.[157] In this scenario, imagine that police used an IMSI-Catcher targeted towards a specific suspect and tracked his movements for a few days, including in the previously mentioned meeting in the home.[158] Although this scenario does implicate privacy concerns that might lead the public to believe an unconstitutional invasion of privacy has occurred,

---

constitutes a Fourth Amendment search."); Owsley, *supra* note 7, at 186–87 ("[T]he use of cell site simulators constitutes a Fourth Amendment search, which requires probable cause. Consequently, the proper approach is for the government to establish probable cause in order to obtain a search warrant consistent with the Fourth Amendment.").

155. Brown & Leese, *supra* note 6, at 15–16.

156. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (holding that a cell phone could not be searched incident to a lawful arrest, in part because of the vast private content contained therein); DOJ POLICY, *supra* note 39, at 2 (stating that IMSI-Catchers must be configured as pen registers to avoid capturing the contents of messages).

157. *See infra* notes 158–61 and accompanying text.

158. The specific terms of this hypothetical avoid two thorny issues of precedent that would complicate the analysis. First, limiting the device's use to a known suspect avoids the Court's noted concerns about indiscriminate mass surveillance. *See* United States v. Knotts, 460 U.S. 276, 284 (1983) ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."). Second, restricting the surveillance period helps distinguish this scenario from the concerns about long-term surveillance raised by the concurrences in *Jones*. *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."); *id*. at 964 (Alito, J., concurring in judgment) (citation omitted) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

precedent does not always align with the public's expectations.[159] A person challenging the use of an IMSI-Catcher would have to assert that the government violated some sort of reasonable expectation of privacy.[160] Whether individuals assert a privacy interest in the transmission of their IMSI numbers or in their locations, as the following sections explain, the IMSI-Catcher's use likely does not violate the Fourth Amendment.[161]

### *A. The Inherent Openness of Cell Signals*

The nature of cell phone technology precludes a person from asserting a privacy interest in either an IMSI number or the cell phone signal itself.[162] Supreme Court precedent concerning the third-party doctrine supports this position.[163] The fundamental basis of cell phone technology is the transmission of signals out into the world, and phones make these connections on a second-by-second basis.[164] Thus, it would be problematic for a person to claim a privacy interest in a signal that is broadcasting out to the world by design.[165] Although *Smith* is informative, it is necessary to concede the key difference between the government's use of an IMSI-Catcher and the third-party doctrine: Police are not obtaining the IMSI

159. *See* Owsley, *supra* note 7, at 223 n.298 (citing Georgia v. Randolph, 547 U.S. 103, 131 (2006) (Roberts, C.J., dissenting); Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 293 (2011); Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 332 (2009)) (noting that judges' assumptions of privacy are often inconsistent with "societal expectations"); *id*. at 228 (noting that public opinion surveys show that a large percentage of people have disagreed with the Court's interpretation of what is unreasonable).

160. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) ("[T]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."). Although the Court did revive the trespass doctrine in *Jones*, it is inapplicable to IMSI-Catchers because "[s]ituations involving merely the transmission of electronic signals without trespass . . . remain subject to *Katz* analysis."). *Jones*, 132 S. Ct. at 953. Despite this clear statement, some scholars have attempted to apply the *Jones* trespass doctrine to the use of IMSI-Catchers to find that their use constitutes a Fourth Amendment search. *See* Brown & Leese, *supra* note 6, at 15.

161. *See infra* Sections IV.A–B.

162. *See Smith*, 442 U.S. at 743.

163. *See id*. ("Telephone users, in sum, typically know that they must convey numerical information to the phone company . . . .").

164. Owsley, *supra* note 7, at 188.

165. *See id*.

number from the cell phone provider but are instead intercepting the information in transit.[166] Despite this difference, the transmitting information is unencrypted and accessible to all who can read it.[167] Because the IMSI number is unencrypted and helps complete the connection process,[168] it falls within the distinction noted in *Smith* between addressing information, which is inherently public, and content, which is private.[169] This differentiation also renders inapplicable the argument that *Riley* "supports the notion that the use of a StingRay amounts to a Fourth Amendment search of a phone."[170] IMSI-Catchers simply do not implicate the treasure trove of personal information that officers might uncover in searching the contents of a phone, as these devices are forbidden from being configured in such a manner.[171] In the absence of any attempt to secure or encrypt the cell phone signal, the result is essentially a misplaced confidence that the IMSI number is inaccessible to all but the intended recipient. In this regard, a person using a cell phone "can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[172]

Despite the open nature of cell phone transmissions, privacy advocates characterize law enforcement's use of IMSI-Catchers to track a phone as "send[ing] signals to it and forc[ing] it to respond. This is by nature an intrusive act—the simulator makes the phone do something that it would not otherwise do."[173] This characterization is partially true.[174] The IMSI-Catcher does not force a phone to respond; it merely emits the strongest signal, and the phone responds by design.[175] But the IMSI-Catcher does force the phone to transmit an IMSI number instead of the normally

166. *See supra* notes 35–43 and accompanying text.

167. *See supra* notes 23–29 and accompanying text.

168. *See supra* note 24 and accompanying text.

169. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979). The Court's distinction between content and address information is not new but instead goes back over a century. *See, e.g.*, Ex Parte Jackson, 96 U.S. 727, 733 (1877) (noting that the contents of sealed letters are protected under the Fourth Amendment, but not their "outward form").

170. Brown & Leese, *supra* note 6, at 15.

171. *See* DOJ POLICY, *supra* note 39, at 2.

172. United States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012).

173. Brown & Leese, *supra* note 6, at 15.

174. *See supra* note 36 and accompanying text.

175. *See supra* note 36 and accompanying text.

transmitted TMSI number.[176] Outside of the fact that the IMSI-Catcher accomplishes this by sending the phone a "special identity request," the exact technical process is unclear.[177] Yet, the fact that the IMSI-Catcher sends a "request" the phone responds to is indicative of the same underlying principle.[178] A cell phone signal is inherently open to the public and accessible to any who choose to connect to it.[179] Because the openness of these signals is inherent in cell technology, individuals cannot claim an expectation of privacy in their IMSI numbers.[180]

### *B. Location Tracking and Constitutionally Protected Spaces*

The alternative for defendants challenging the use of IMSI-Catchers is to claim a reasonable expectation of privacy in their locations.[181] The long history of public outrage at perceived government infringement of privacy would certainly suggest that people have an expectation of privacy in their location data.[182] But even widespread public support only suggests a subjective expectation of privacy; the Court must accept that belief as reasonable to meet the *Katz* test.[183] Traditionally, in assessing reasonableness, the Court has applied different standards to location tracking

176. *See* STROBEL, *supra* note 16, at 13.

177. *See id*.

178. *See* Brown & Leese, *supra* note 6, at 15.

179. *See supra* notes 162–72.

180. *See supra* notes 162–72.

181. *See* Leneis, *supra* note 53, at 506.

182. *See* Owsley, *supra* note 7, at 227–29. This includes a study done that suggested 73% of Californians "favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company." *Id*. at 228 (quoting JENNIFER KING & CHRIS JAY HOOFNAGLE, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL LOCATION INFORMATION 206 (2008), www.ftc.gov/os/comments/mobilevoice/534331-00005.pdf.).

183. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Admittedly, this statement implies a contradiction: even if most of the public subjectively believes something is private, the Court can declare that society does not accept the expectation as reasonable. But the idea that the Court imposes its own logic to assess reasonableness under *Katz* is a noted and common criticism of the standard. *See, e.g*., Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (quoting *Katz*, 389 U.S. at 360–61) ("In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those 'actual (subjective) expectation[s] of privacy' 'that society is prepared to recognize as "reasonable,"' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.").

in public and location tracking in private in both *Knotts* and *Karo*.[184] However, because an IMSI-Catcher can readily track location in both the home and in public, scholars have gone so far as to say that *Knotts* "has no bearing on the issue of the use of the stingray, as it was limited to the use of vehicle tracking on public thoroughfares."[185] Despite this, it would be wise to reiterate the existing legal standard. To the extent that an IMSI-Catcher can track an individual's public movements, *Knotts* controls.[186] Indeed, courts routinely rely on *Knotts* to affirm the principle that individuals have no expectation of privacy in their public movements.[187] Mere surveillance is not a Fourth Amendment search, and because an IMSI-Catcher is only a more efficient means to track suspects, its use in public spaces does not require a warrant.[188]

At first blush, it would appear that because an IMSI-Catcher is readily capable of tracking people into their homes, it is obviously unconstitutional under *Karo*.[189] The Supreme Court's guiding principle on surveillance of the home would seem to state as much:

> We think that obtaining by sense-enhancing technology any

184. *Compare* United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("When Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."), *with* United States v. Karo, 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time.").

185. Brittany Hampton, Note, *From Smartphones to Stingrays: Can the Fourth Amendment Keep Up with the Twenty-first Century?*, 51 U. LOUISVILLE L. REV. 159, 175–76 (2012).

186. *See Knotts*, 460 U.S. at 281–82 (holding that a person has no reasonable expectation of privacy when traveling in public).

187. *See* Ian Herbert, Note, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442, 452 (2011) ("In analyzing Fourth Amendment claims related to tracking devices, courts typically describe the device simply as a GPS tracker or an electronic monitoring device—perhaps with a sentence or two discussing some of the device's limitations—and then make a simple reference to the holding in *Knotts*.").

188. *See Knotts*, 460 U.S. at 284 ("We have never equated police efficiency with unconstitutionality, and we decline to do so now.").

189. *See* United States v. Karo, 468 U.S. 705, 714 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.").

> 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. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[190]

Indeed, scholars have cited this precedent, stating, "As devices become more accurate, the possibility that they will be used to reveal details about the home increases dramatically. Therefore, these devices pose the potential Fourth Amendment issues discussed in *Kyllo*."[191] But in doing so, scholars are ignoring a fundamental dividing line in Fourth Amendment jurisprudence: "What a person *knowingly exposes* to the public, *even in his own home* or office, is not a subject of Fourth Amendment protection."[192] The Court has consistently applied this principle in cases that concern surveillance in and around the home.[193]

Applied to IMSI-Catchers, this principle serves to distinguish their use from the Court's holdings in *Karo* and *Kyllo*.[194] Turning first to *Karo*, the government clandestinely planted the beeper in the can to conceal it from the intended recipient,[195] whereas individuals voluntarily carry cell phones on

190. Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

191. Herbert, *supra* note 187, at 498; *see, e.g.*, Brown & Leese, *supra* note 6, at 14 ("Accordingly, if the searches in *Karo* and *Kyllo* were in violation of the Fourth Amendment, so too would be the use of a cell site simulator to track a cellphone inside a person's home."); Hosein & Palow, *supra* note 154, at 1098 (quoting *Kyllo*, 533 U.S. at 40) (citing *Karo*, 468 U.S. at 718) ("The Court has repeatedly held such an electronic invasion, 'to explore details of the home that would previously have been unknowable without physical intrusion,' is a search that requires a warrant.").

192. Katz v. United States, 389 U.S. 347, 351 (1967) (emphasis added).

193. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 215 (1986) (finding that the curtilage of the home was knowingly exposed to a police surveillance flight because Ciraolo did not conceal his backyard from aerial view); Smith v. Maryland, 442 U.S. 735, 743 (1979) (finding it irrelevant that Smith made his call from within his home, as no subscribers could "rationally think" their location would make a difference).

194. *See infra* notes 195–229.

195. *Karo*, 468 U.S. at 707 ("In this case, we are called upon to address . . . whether installation of a beeper in a container of chemicals with the consent of the original owner constitutes a search or seizure within the meaning of the Fourth Amendment when the container is delivered to a buyer having no knowledge of the presence of the beeper . . . .").

their person throughout their daily lives.[196] One might imagine that if a person purchased a beeper that transmitted an unencrypted signal capable of being picked up by anyone with a receiver, placed it in the can, and voluntarily traveled around with it, the Court in *Karo* would have reached a different conclusion.[197]

As the Court recognized in *Smith*, it is difficult to quantify the extent to which people *knowingly* convey information to the public.[198] However, the Court has previously engaged in analysis that considers the totality of the surrounding circumstances to determine, in the Court's opinion, what a person should know.[199] If the Court were to conduct a similar analysis here, just what public information exists that should make a person aware that their phone is inherently locatable? To start, search providers make location records available for people to see exactly where they have been at any given time in which their phone has been on.[200] Network providers inform subscribers that the SIM card enables the connection to the network and that an IMSI number is part of the information tied to the card.[201] Networks notify subscribers of the fact their phones are not locked in to their network by informing them of network roaming capabilities.[202] Lastly, service

196. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

197. *See infra* note 205 and accompanying text.

198. *Smith*, 442 U.S. at 743 ("[S]ubjective expectations cannot be scientifically gauged . . . .").

199. *Id*. at 742. The Court considered numerous factors in *Smith* to determine that individuals lacked even a subjective expectation of privacy. *Id*. at 742–43. The Court looked to individuals' general awareness that they are conveying information to a third party. *Id*. at 742. The Court also considered that phone numbers dialed appeared in subscriber's monthly bills. *Id*. Lastly, the Court considered the fact that some phone books informed the public that phone companies can help identify unwanted calls. *Id*. at 742–43.

200. Greg Kumparak, *Google's Location History Browser Is a Minute-by-Minute Map of Your Life*, TECHCRUNCH (Dec. 18, 2013), http://techcrunch.com/2013/12/18/google-location-history/.

201. *SIM Cards*, T-MOBILE SUPPORT, https://support.t-mobile.com/docs/DOC-2031 (last modified Feb. 23, 2017, 4:38 PM) ("The SIM card is the brain of your digital phone and gives you access to our advanced nationwide 4G network."); *4G SIM Information*, VERIZON WIRELESS, http://www.verizonwireless.com/support/activate-4g-sim-card/ (last visited Mar. 4, 2017) ("The Verizon Wireless 4G SIM Card contains the 4G subscriber profile, which includes . . . International Mobile Subscriber Identity (IMSI).").

202. *Domestic Data Roaming FAQs*, T-MOBILE SUPPORT, https://support.t-mobile.com/docs/DOC-3299 (last modified June 12, 2016, 12:01 AM) ("Domestic data roaming occurs when you travel outside of T-Mobile's network coverage, using wireless data from another carrier."); *Customer Agreement*, VERIZON WIRELESS, http://www.verizonwireless.com/b2c/support/customer-

contracts between subscribers and their networks often contain explicit references to the open nature of cell phone transmissions.[203] These facts paint a picture of a public that is aware of a cellphone's ability to be located, to say nothing of the fact that individuals must have some inherent awareness that their mobile device must constantly be sending transmissions to function.[204] Therefore, if the Court were to engage in the established practice of ferreting out what society would expect to be reasonable, it would likely have to conclude that the public is aware their phones can be tracked—meaning the public voluntarily carries tracking devices with them into their homes, which fundamentally distinguishes this case from *Karo*.[205]

Turning then to *Kyllo*, the question of what constitutes "general public use" is one the Court did not fully explain.[206] Despite the Court's protestations that it was fashioning a "firm but also bright" line,[207] the common interpretation is that "*Kyllo* deliberately adopted a rule that allows the outcome to change along with society."[208] If one adopts the "routine"

agreement (last updated Nov. 18, 2016) ("You're 'roaming' whenever your wireless device uses a transmission site outside your Coverage Area or uses another company's transmission site.").

203. *Wireless Customer Agreement*, § 4.2, AT&T, http://www.att.com/legal/terms.wirelessCustomerAgreement.html (last visited Mar. 4, 2017) ("AT&T DOES NOT GUARANTEE SECURITY. Data encryption is available with some, but not all, Services sold by AT&T."); *T-Mobile Terms & Conditions*, T-MOBILE, http://www.tmobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true (Sept. 1, 2016) ("We do not guarantee that your communications will be private or secure . . . .").

204. *See Smith*, 442 U.S. at 742. The Court has considered this type of "common sense" analysis before in *Smith,* where it stated that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id*. at 742.

205. This argument relies on much of the reasoning from *Smith*, but it does not invoke the third-party doctrine because IMSI-Catchers do not require the assistance of the phone company. *See supra* notes 36–41 and accompanying text. Although the location data is not being obtained from a third party, the *Smith* analysis underlies the principle that individuals are aware that they are not simply conveying their location data directly to the phone companies, but are instead broadcasting it to the public, making the *Knotts* analysis applicable. *See supra* notes 111–18 and accompanying text.

206. *See supra* notes 124–25 and accompanying text.

207. Kyllo v. United States, 533 U.S. 27, 40 (2001).

208. Orin Kerr, *Can the Police Now Use Thermal Imaging Devices Without a Warrant? A Reexamination of* Kyllo *in Light of the Widespread Use of Infrared Temperature Sensors*, VOLOKH CONSPIRACY (Jan. 4, 2010, 12:33 PM), http://volokh.com/2010/01/04/can-the-police-now-use-thermal-imaging-devices-without-a-warrant-a-reexamination-of-kyllo-in-light-of-the-widespread-use-of-infrared-temperature-sensors/. *Contra* Florida v. Jardines, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring) (applying *Kyllo*'s bright-line rule to the use of a drug-sniffing dog despite the widespread use of drug dogs because the case involved a home). Justice Stevens would likely view

standard implied by the Court's decision, there is a plausible argument that an IMSI-Catcher can satisfy *Kyllo*.[209] Were one to interpret the definition of "technology" broadly, then one would have to consider the underlying technology of IMSI-Catchers, namely the cell phone–base station relationship that forms the foundation for cellular communication.[210] Cellular networks have blanketed the nation with coverage and frequently make a point of advertising how much of the country they cover.[211] The technology that underpins modern communications is everywhere, and the Court itself has made the case for the ubiquitous nature of cell phones.[212] Thus, under this expansive definition, IMSI-Catchers are unquestionably routine.

Such a broad interpretation of "technology" is hardly ideal, but even limited to the technological devices of IMSI-Catchers themselves, there is still a strong argument that they are routine.[213] The year 2016 marks the twentieth year since the invention of the first IMSI-Catcher.[214] Their use has spread to dozens of state and federal agencies, as well as local police departments across the country.[215] Even scholars critical of their use have been forced to concede that "[a]rguably, there is no police technology that is more commonly used" than IMSI-Catchers.[216] Therefore, it is likely that the Court would conclude that these devices are in general public use and thus not a Fourth Amendment search under *Kyllo*.[217]

---

this interpretative gulf as merely more evidence that the general-public-use standard has failed to provide the guidance it promised. *See Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).

209. *See* Kerr, *supra* note 208 and accompanying text.

210. *See supra* notes 16–29, 36–40 and accompanying text.

211. *See, e.g.*, *4G LTE Coverage Map*, T-MOBILE, http://www.t-mobile.com/coverage-map.html (last visited Mar. 5, 2017).

212. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (stating that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

213. *See infra* notes 214–16 and accompanying text.

214. *See* STROBEL, *supra* note 16, at 13.

215. *See supra* notes 60–62 and accompanying text.

216. Brown & Leese, *supra* note 6, at 12; *accord* Owsley, *supra* note 7, at 186 ("[T]hese devices have also come to be used for routine criminal investigations . . . ."); Hosein & Palow, *supra* note 154, at 1081 (noting that intercepting cell signals with devices like IMSI-Catchers is "commonly done").

217. *See supra* notes 214–16 and accompanying text.

Returning to the previously introduced hypothetical,[218] the governing analysis comes back to the fundamental *Katz* standard.[219] Accepting the Court's understanding of "intimate details" in *Kyllo*, there is no argument that intimate details of a person's movement in the home would be revealed.[220] But the fact that individuals knowingly and voluntarily carry their devices with them abrogates the "minimal expectation of privacy" that otherwise exists within the home.[221] Thus, as the Sixth Circuit noted in *Skinner*, the inherently trackable cell signal fits within a category of surveillance based upon what individuals expose to the public:

> Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen. The recent nature of cell phone location technology does not change this.[222]

Although the government's use of IMSI-Catchers weave together multiple threads of Fourth Amendment jurisprudence, this result is the likely outcome compelled by precedent.[223] The underlying principle of the Court's precedent has always been to protect individuals from invasive government intrusion.[224] In that sense, Fourth Amendment precedent is a shield.[225] Although there are certain ways the police might use IMSI-Catchers that implicate the Fourth Amendment,[226] the Court generally does not take it

218. *See supra* note 158 and accompanying text.

219. *See supra* note 160 and accompanying text.

220. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

221. *Id*. at 34.

222. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

223. *See infra* notes 224–29.

224. "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" *Kyllo*, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

225. *See supra* notes 94–99 and accompanying text.

226. *See supra* note 158. For example, the Dirtbox, a plane-mounted IMSI-Catcher, has a far greater range, potentially collecting thousands of IMSI numbers at once and thus enabling mass tracking. *See* Kim Zetter, *The Feds Are Now Using 'Stingrays' in Planes to Spy on Our Phone Calls*, WIRED (Nov. 14, 2014, 2:14 PM), http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/. This device directly implicates concerns raised by the Court in prior cases. *See* United States v. Knotts, 460 U.S. 276, 284 (1983) (noting that concerns about "dragnet" mass

upon itself to protect individuals from themselves.[227] Thus, despite whatever subjective expectations of privacy the public might entertain, they are simply unreasonable in the realities of cell phone location tracking.[228] So long as the general public chooses to carry inherently locatable devices, individuals will have willingly forfeited any claim of a reasonable expectation of privacy they might have had.[229]

## V. THE UNDISCOVERED COUNTRY

Advancing technology continues to open new frontiers, and although the Fourth Amendment may not apply to IMSI-Catchers, this Comment's purpose is not to suggest that this is a desirable outcome nor even one that the public should accept. At the same time, it would be a mistake to categorically deny law enforcement the tools they need to combat crime[230]—just as it would be a mistake to leave law enforcement to try and guess its way through applying decades-old statutes to new devices.[231] Instead, by having possibly reached the outer limits of the Court's existing precedent, as it applies to technology, it may be time to look to alternative means to protect the privacy interests of the public.

### *A. The Low Likelihood of Judicial Reconsideration*

There is always the possibility that the Court may choose to reconsider past precedent.[232] Members of the Court have signaled their awareness of the weaknesses of the *Katz* test and existing Fourth Amendment

surveillance might necessitate a different result in later cases).

227. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

228. *See* United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

229. *Id.* (stating that if a cell phone "gives off a signal that can be tracked for location, certainly the police can track the signal. The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools").

230. *See* Owsley, *supra* note 7, at 231 ("[I]t is clear that these devices can be effective tools in law enforcement arsenals. For example, the use of a cell site simulator near a prison facility can assist in locating a cell phone used by inmates in furtherance of criminal activity.").

231. *See supra* notes 68–75 and accompanying text.

232. *See generally* Randy J. Kozel, *Precedent and Reliance*, 62 EMORY L.J. 1459 (2013) (discussing the Court's varying reliance on precedent and whether reliance on precedent should be protected).

precedent.[233] Additionally, many state courts have taken a broader view of a reasonable expectation of privacy than the Supreme Court.[234] Thus, it would be prudent to acknowledge these concerns and explore the likelihood that the Court might reverse course.[235]

Just as the Court examined the available knowledge in *Smith* to determine what is objectively reasonable,[236] the Court also considered the importance of the privacy at stake in *Katz* when deciding to protect phone calls:

> One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[237]

Similarly, the Court in *Riley* considered the importance of cell phones when it held that law enforcement could not search one without a warrant incident to a lawful arrest:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[238]

*Riley* concerned an action that was unquestionably a search.[239] But the

233. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test . . . has often been criticized as circular, and hence subjective and unpredictable.").

234. *See* Owsley, *supra* note 7, at 228 ("[S]everal state courts have rejected the applicability of *Miller* pursuant to state constitutions. Similarly, various state courts have rejected the reasoning and ruling in *Smith v. Maryland*.").

235. *See infra* notes 236–60 and accompanying text.

236. *See supra* note 199 and accompanying text.

237. Katz v. United States, 389 U.S. 347, 352 (1967).

238. *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

239. *See id.* at 2480 ("These two cases raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been

facts of this case did not implicate the question of when a search might occur.[240] Justice Alito concurred separately to join the Court's holding.[241] He noted, "[W]e should not mechanically apply the rule used in the predigital era to the search of a cell phone . . . . This calls for a new balancing of law enforcement and privacy interests."[242] While, in this instance, the Court distinguished the case from past precedent, Justice Alito was especially concerned about the application of the Fourth Amendment to modern technology:

> Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.[243]

This concurrence signaled an awareness on his part that the case law that comprises the Court's Fourth Amendment jurisprudence may lead to undesirable results in the modern era.[244] Indeed, two years earlier, Justice Alito made a similar point in *Jones* by highlighting the fundamental weakness of basing a warrant requirement on society's expectations when he warned, "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[245] Thus, the Court has shown awareness of both the importance of cell phones in modern society and the potentially shrinking realm of privacy.[246]

Despite this awareness, it seems unlikely that the Court is prepared to

---

arrested.").

240. *See id*.

241. *Id*. at 2495 (Alito, J., concurring).

242. *Id*. at 2496–97.

243. *Id*. at 2497.

244. *See id*.

245. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring in the judgment).

246. *See supra* notes 236–45 and accompanying text.

reconsider Fourth Amendment precedent.[247] Justice Alito's same concurrence distinguished between the constitutionally permissible "short-term monitoring of a person's movements" and long-term monitoring that would violate a reasonable expectation of privacy.[248] The majority responded, "[E]ven assuming that the concurrence is correct to say that '[t]raditional surveillance' of Jones for a 4-week period 'would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,' our cases suggest that such visual observation is constitutionally permissible."[249] Of the nine justices on the Court, Justice Sotomayor appeared to be the only one ready to consider departing from precedent:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[250]

It is difficult to read the judicial tea leaves and predict how the justices are going to rule on an undecided case, let alone a hypothetical one.[251] But given the majority opinion's affirmation of *Knotts* and Justice Alito's affirmation of short-term public monitoring, the Court does not appear ready to make substantive changes to precedent.[252] Because of the fidelity to

247. *See infra* notes 248–50 and accompanying text.

248. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

249. *Id*. at 953–54 (majority opinion) (citations omitted).

250. *Id*. at 957 (Sotomayor, J., concurring) (citations omitted).

251. For a recent example of the difficulties in predicting judicial outcomes, see Josh Gerstein, *John Roberts's Big Moment*, POLITICO (June 26, 2012, 4:33 AM), http://www.politico.com/story/2012/06/john-robertss-big-moment-077826?paginate=false ("None of the experts interviewed for this story expect Roberts to join with the liberals on the court to create a 5–4 majority to uphold the health care law.").

252. *See Jones*, 132 S. Ct. at 953–54; *id*. at 964 (Alito, J., concurring in the judgment). The alternative to departing from precedent would be for the Court to distinguish from precedent by endorsing the firm bright-line interpretation of *Kyllo* that Justice Kagan applied in her concurrence to *Florida v. Jardines*, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring). By doing so, the Court could stop the use of IMSI-Catchers at the door of the home, much like the thermal imager in *Kyllo*. *See id*. ("That 'firm' and 'bright' rule governs this case: The police officers here conducted a search because they used a 'device . . . not in general public use' (a trained drug-detection dog) to 'explore details of the home' (the presence of certain substances) that they would not otherwise have discovered without entering the premises."). However, out of the five-justice majority, that

existing precedent displayed in *Jones*, there is at least a substantial chance the Court would be unwilling to rewrite the book on the Fourth Amendment.[253] Additionally, the frequent requirement that law enforcement agencies sign nondisclosure agreements as a condition of using IMSI-Catchers prevented these issues from being fully litigated and likely contributed to the absence of any case reaching the appellate level for years.[254] Thus, these procedural barriers present a further complication to future cases.[255]

In the full context of a criminal proceeding, the likelihood that the Supreme Court could provide a judicial remedy decreases even further.[256] A defendant would have to proceed to trial and first prove that police used an IMSI-Catcher during their surveillance.[257] The prosecutor would then have to choose to proceed with the case and risk violating the nondisclosure agreement.[258] If convicted, the defendant would have to appeal the case up through the legal system until the Supreme Court granted certiorari. Finally, the Court would have to be willing to break dramatically from past precedent or find a different means of distinguishing the case.[259] This procession of obstacles means that privacy advocates would be wise to place their hopes elsewhere if they seek a realistic solution for reining in the government's use of IMSI-Catchers.[260]

---

concurrence only garnered the support of Justices Ginsburg and Sotomayor. *Id*. at 1418. The four-justice dissent applied *Katz*, regardless of the home's presence in the facts. *Id*. at 1421 (Alito, J., dissenting) ("A reasonable person understands that odors emanating from a house may be detected from locations that are open to the public, and a reasonable person will not count on the strength of those odors remaining within the range that, while detectible by a dog, cannot be smelled by a human."). The death of Justice Scalia only further raises the possibility that his replacement might be amenable to the reasoning of the dissent in *Jardines* instead of the concurrence.

253. *See supra* notes 245–50 and accompanying text.
254. *See supra* note 30 and accompanying text.
255. *See supra* note 254 and accompanying text.
256. *See infra* notes 257–59 and accompanying text.
257. *See supra* note 31 and accompanying text.
258. *See supra* note 32 and accompanying text.
259. *See supra* notes 251–52 and accompanying text.
260. *See supra* notes 257–59 and accompanying text.

### *B. Legislative Solutions to the Rescue*

Instead of relying on the Court to apply decades of precedent to changing technology, privacy advocates should seek reform through the Legislative and Executive Branches of government.[261] This course of action would mirror the one taken in the latter half of the Twentieth Century, as government had to respond to the initial wave of technological advancement:

> [C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.[262]

This perspective summarizes the most effective means through which privacy can keep up with advancing technology.[263] First, a court case and a legislative bill can operate on dramatically different time scales.[264] A member of Congress can generally introduce even a landmark piece of legislation, and it will have reached the President within the two years in which that Congress meets.[265] In contrast, the GPS tracking in *Jones* occurred in 2005, and the Supreme Court handed down its decision seven years later.[266] Congress can more readily respond to the concerns of the

261. *See infra* notes 262–81 and accompanying text.

262. United States v. Jones, 132 S. Ct. 945, 962–63 (2012) (Alito, J., concurring in the judgment) (citations omitted).

263. *See id*.

264. *See infra* notes 265–66 and accompanying text.

265. For example, the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act was introduced in the House on December 2, 2009 and was eventually signed by President Obama on July 21, 2010. *See H.R.4173—Dodd-Frank Wall Street Reform and Consumer Protection Act*, CONGRESS.GOV, https://www.congress.gov/bill/111th-congress/house-bill/4173/actions (last visited Mar. 5, 2017).

266. *See Jones*, 132 S. Ct. at 948 ("[I]n 2005 the Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of an electronic tracking device on the Jeep Grand Cherokee registered to Jones's wife.").

people and provide solutions on a faster basis than the courts.[267]

Second, the unregulated legal landscape arose because federal officials were left to their own devices and attempted to regulate themselves within broad categories of existing law.[268] The answer is for Congress to perform its intended legislative function and "address the myriad of technological developments in surveillance since 1986."[269] The world we live in today involves the routine use of technology that just thirty years ago bordered on science fiction.[270] Despite these advancements, the governing statutes are unchanged.[271] Requiring Congress to update technological privacy-protection statutes, just as it did after *Katz*, is the sensible solution to the concerns posed by IMSI-Catchers.[272] In light of the ever-changing nuances of new technology, this would be the preferable outcome to a judicially driven solution:

> [I]t would be very unfortunate if privacy protection in the [twenty-first c]entury were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.[273]

267. *See supra* notes 265–66 and accompanying text.

268. Leneis, *supra* note 53, at 503–05 (discussing the different realms of statutory guidance under the 1986 Electronic Communications Privacy Act).

269. Owsley, *supra* note 7, at 230–31.

270. *See, e.g.*, Sophie Curtis, *From Hoverboards to Self-Tying Shoes: Predictions that Back to the Future II Got Right*, TELEGRAPH (Oct. 20, 2015, 4:35 PM), http://www.telegraph.co.uk/technology/news/11699199/From-hoverboards-to-self-tying-shoes-6-predictions-that-Back-to-the-Future-II-got-right.html. Fortunately, the abolition of lawyers remains firmly in the realm of science fiction. *See* BACK TO THE FUTURE: PART II (Universal Pictures 1989).

271. *See* Owsley, *supra* note 7, at 230–31 (discussing the criticisms and technological gaps in the Electronic Communications Privacy Act); *id.* at 231 n.351 (citing Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1431–32 (2004); Orin Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559 (2004)).

272. *See* United States v. Jones, 132 S. Ct. 945, 962–63 (2012) (Alito, J., concurring in the judgment).

273. Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (Alito, J., concurring in part and concurring in the judgment).

Admittedly, it may be naïve to rely on a legislative body plagued by inactivity,[274] partisan division,[275] and intentional obstructionism.[276] Even though the task of coming together to draft important and responsible laws may be beyond our national representatives, the states might be able to lead the way.[277] California recently updated its privacy laws to require a warrant for IMSI-Catchers to be used, providing a potential model for the rest of the nation.[278] The California law was jointly authored by a Democrat and a Republican who stated that they sought to "help[] bridge the gap between progressives and conservatives to make the privacy of Californians a top priority this year. This bipartisan bill protects Californians' basic civil liberties as the Fourth Amendment and the California Constitution intended."[279] Other state legislatures have since begun to push for increased privacy protections.[280] Whether through the Congress or the states, the legislatures are reacting to these new technologies and are proving to be more responsive to the privacy concerns of the people.[281]

## VI. CONCLUSION

Privacy is something for the people of a free nation to value and defend, particularly when it stands as a bulwark against government intrusion. For that reason, scholars who oppose "the Government's unrestrained power to assemble data that reveal private aspects of identity"[282] should be lauded for

274. Cristina Marcos & Ramsey Cox, *Historically Unproductive Congress Ends*, HILL (Dec. 16, 2014, 11:25 PM), http://thehill.com/blogs/floor-action/senate/227365-historically-unproductive-congress-ends.

275. Maureen Groppe, *New Analysis Shows an Increasingly Partisan Congress*, USA TODAY (May 19, 2015, 1:12 PM), http://www.usatoday.com/story/news/politics/2015/05/19/bipartisanship-index-congress-lugar/27584907/.

276. Editorial, *Senate Filibuster in Need of Reform*, L.A. TIMES (Nov. 25, 2012), http://articles.latimes.com/2012/nov/25/opinion/la-ed-filibuster-reform-20121125.

277. *See supra* notes 86–90 and accompanying text.

278. *See* Electronic Communications Privacy Act, 2015 Cal. Stat. 651 (codified at CAL. PENAL CODE § 1546).

279. Dave Maass, *Victory in California! Gov. Brown Signs CalECPA, Requiring Police to Get a Warrant Before Accessing Your Data*, ELECTRONIC FRONTIER FOUND. (Oct. 8, 2015), https://www.eff.org/deeplinks/2015/10/victory-california-gov-brown-signs-calecpa-requiring-police-get-warrant-accessing (quoting California Senator Joel Anderson).

280. The Illinois legislature has recently considered a similar bill to require a warrant for IMSI-Catchers. Citizen Privacy Protection Act, H.B. 4470, 99th Gen. Assemb. (Ill. 2016).

281. *See supra* notes 261–80 and accompanying text.

282. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

their efforts. But as often as the Fourth Amendment's history is a story of a shield against government abuse,[283] it is also a story of exceptions and dashed expectations.[284] The conclusion: Society's expectations of protection are far removed from what Fourth Amendment precedent actually protects.[285]

IMSI-Catchers are an important new frontier in the conflict between the Fourth Amendment and technology. Technological progress will only continue, and the Court has had only limited success in fashioning new rules for new technologies.[286] Although many scholars have tried to rely on "the blunt instrument of the Fourth Amendment"[287] to preserve privacy protections, so long as the public willingly sacrifices privacy for convenience, it is likely that the Court's precedent is nearing its outer limits.[288] Thus, privacy preservation efforts should be focused elsewhere.[289]

State and federal legislatures provide a better alternative to a judicially crafted remedy.[290] Legislatures are more responsive to the concerns of the people and capable of providing clear guidance to law enforcement agencies.[291] New legislation to reign in the use of IMSI-Catchers has already begun to take hold in the states,[292] and may soon advance through Congress.[293] If the privacy protections enshrined in the Fourth Amendment are to survive into the twenty-first century, the various levels of government must be prepared to engage proactively with new technology instead of waiting for the Court to do so. Today, the widespread use of IMSI-Catchers has successfully exploited the limits of precedent and the apathy of

283. *See supra* notes 95–100, 119–26 and accompanying text.

284. *See supra* notes 101–09 and accompanying text.

285. *See* Georgia v. Randolph, 547 U.S. 103, 131 (2006) (Roberts, C.J., dissenting) (citing Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978)) ("The majority suggests that 'widely shared social expectations' are a 'constant element in assessing Fourth Amendment reasonableness,' but that is not the case . . . . Our common social expectations may well be that the other person will not, in turn, share what we have shared with them with another—including the police—but that is the risk we take in sharing.").

286. *See supra* notes 207–16 and accompanying text.

287. Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring in part and concurring in the judgment).

288. *See supra* Section V.A.

289. *See supra* Section V.B.

290. *See supra* notes 262–79 and accompanying text.

291. *See supra* notes 265–69 and accompanying text.

292. *See supra* notes 86–90, 280 and accompanying text.

293. *See supra* notes 91–92 and accompanying text.

Congress. What tomorrow holds, no one yet knows.

Ryan C. Chapman*

* J.D., 2017, Pepperdine University School of Law; Lead Articles Editor, *Pepperdine Law Review*, Volume XLIV. I would like to thank my family and loved ones for their continued support, without which I would not have made it this far. Additionally, Dr. Lewis Ringel of California State University, Long Beach, for helping so many students take their first steps into the law. Finally, I would like to thank the hardworking staff of *Pepperdine Law Review* for the long hours and the tireless work they do in publishing a successful volume.