Chicago-Kent Law Review

Volume 91
Issue 1 *Congressional Dysfunction and Executive Lawmaking During the Obama Administration*

Article 12

1-29-2016

Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches

Andrew Hemmer
IIT Chicago-Kent College of Law

DUTY OF CANDOR IN THE DIGITAL AGE: THE NEED FOR HEIGHTENED JUDICIAL SUPERVISION OF STINGRAY SEARCHES

ANDREW HEMMER[1]

I. INTRODUCTION

Cell phones and other mobile devices have radically transformed our world.[2] In fact, cell phone technology is the "most quickly adopted consumer technology in the history of the world," and the number of cell phone users worldwide increases every year.[3] Today, ninety-one percent of adults in the United States own a cell phone.[4] Many users constantly check their phones, keep them by their bedsides at night, and use them in connection with virtually every daily activity.[5] This "nearly ubiquitous mobile connectivity" means that almost every American citizen is constantly connected to the global mobile network.[6]

Little do they know, however, that law enforcement officers now use Stingrays[7]—or International Mobile Subscriber Identity ("IMSI") catchers—to mimic a wireless carrier's base station and "trick" cell phones into connecting to it.[8] These devices track the location of suspected criminals and gather evidence against them by sending electronic signals to all cell phones within the device's vicinity in

1. Student, Chicago-Kent College of Law

2. *See generally* Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RESEARCH CTR. (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

3. *Id.*

4. *Id.*

5. *See id.*

6. *See id.*

7. "Stingray" is the brand name for the IMSI-catcher product manufactured by the Harris Corporation. Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and 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, 146 n.35 (2013). This Comment will use the term "Stingray" to refer generally to IMSI-catcher technology.

8. ADRIAN DABROWSKI ET AL., SECURE BUS. AUSTRIA RESEARCH, IMSI-CATCH ME IF YOU CAN: IMSI-CATCHER-CATCHERS (2014), https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

order to trigger an automatic response from each phone.[9] Stingrays are also capable of "hijacking" a targeted mobile device—performing "silent calls," calling or texting on behalf of the targeted cell phone, and changing the content of text messages sent from the cell phone.[10]

With the emergence of this cutting-edge police technology, we should be particularly vigilant about the potential for abuse. The "militarization" of the police as part of the War on Drugs provides a cautionary tale regarding the devastating effect that overzealous policing can have on privacy.[11] In 1990 the 101st Congress enacted the National Defense Authorization Act (NDAA),[12] and section 1208 of the Act allowed the Secretary of Defense to transfer military-grade weapons and ammunition to state and local police departments to combat the War on Drugs.[13] The result of the 1208 program was that the number of paramilitary police raids conducted on the private residences of civilians nationwide increased from approximately 3,000 in 1980 to 45,000 in 2001.[14] There was also a 292 percent increase in the number of police departments deploying SWAT team units against citizens from 1982 to 1997.[15] Also, many police departments nationwide have deployed these quasi-military tactics against citizens who turn out to be innocent of any crime. A study conducted by the American Civil Liberties Union (ACLU) in twenty-six states during 2011 and 2012 found that up to sixty-five percent of SWAT deployments for drug searches turned up no contraband of any kind.[16]

Stingrays present a similar threat to the privacy of individuals that are innocent of any crime. Through the use of Stingray technology, law enforcement agencies are now capable of ascertaining the precise location of millions of cell phone users across the country, intercepting the content of those phones and manipulating their op-

9. *Id.*

10. *Active GSM Interceptor*, ABILITY, http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html (last visited Aug. 15, 2015).

11. *See generally* RADLEY BALKO, RISE OF THE WARRIOR COP: THE MILITARIZATION OF AMERICA'S POLICE FORCES 137–284 (1st ed. 2014).

12. H.R. Res. 2461, 101st Cong. (1990) (enacted).

13. H.R. Res. 2461, *supra* note 12, at § 1208.

14. BALKO, *supra* note 11, at 221.

15. *Id.*

16. KARA DANSKY ET AL., AM. CIVIL LIBERTIES UNION, WAR COMES HOME: THE EXCESSIVE MILITARIZATION OF AMERICAN POLICING 34 (2014).

erations at will.[17] The frightening capabilities of Stingray devices implicate serious Fourth Amendment concerns. The Fourth Amendment protects citizens from unreasonable searches and seizures,[18] and without proper judicial oversight, Stingray use in many cases will be unreasonable within the meaning of the Fourth Amendment.

The first federal district court case to address the constitutional implications of Stingray use, *United States v. Rigmaiden*, is still proceeding in the District Court of Arizona.[19] The judge in that case recently issued a detailed order denying the defendant's motion to suppress evidence seized by the use of a Stingray.[20] However, in that case, the government failed to specify the technology that it intended to use in executing the search warrant, leaving out crucial details related to the device's invasiveness and likely impact on third parties.[21]

This Note proposes a different approach than the one taken in *Rigmaiden* and advocates a new standard of judicial supervision of Fourth Amendment searches in the context of Stingray technology. Given the enormous power that Stingray technology gives the police to spy on American citizens, the judiciary must hold law enforcement to a heightened "duty of candor"[22] in search warrant applications involving this specific technology. In addition, magistrate judges should follow certain guidelines in issuing search warrants involving Stingray use in order to mitigate the impact on the privacy of third parties.

Part II of this Note will detail the operational capabilities of Stingrays and highlight the grave societal concerns that the devices raise. Part III will discuss Fourth Amendment jurisprudence in the digital age and argue that Stingray use constitutes a Fourth Amendment search. It will also analyze *United States v. Rigmaiden*[23] and a particularly relevant case involving a search warrant for electronic data, *United States v. Comprehensive Drug Testing,*

17. ABILITY, *supra* note 10.

18. U.S. CONST. amend. IV.

19. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012).

20. Order Denying Motion to Suppress, United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013).

21. [Proposed] Brief for American Civil Liberties Union & Electronic Frontier Foundation as Amicus Curiae Supporting Defendant, United States v. Rigmaiden, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013) (No.904-3) [hereinafter Rigmaiden Brief].

22. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring).

23. *Rigmaiden*, 844 F. Supp. 2d 982.

Inc.,[24] with an emphasis on Chief Judge Kozinski's concurrence.[25] Part IV will advocate a two-fold proposal for the issuance of search warrants involving Stingray technology. First, the judiciary must require government officials to include in warrant applications a detailed description of the technology and its capabilities. This additional information will allow magistrates to impose appropriate limitations on the scope and execution of the warrant and to mitigate the impact on the privacy of third parties. Second, magistrates should impose the following specific limitations and conditions[26] on Stingray warrants: (1) government officials must waive reliance on the plain view doctrine; (2) segregation and redaction of electronic data must be done by specialized law enforcement personnel not involved in the investigation, and those personnel must not disclose to the investigators any information other than that which is the target of the warrant; (3) the government's search protocol must be narrowly tailored to uncover only the information for which it has probable cause, and agents may examine that information only; and (4) the government must immediately destroy any intercepted third-party data without examining its contents. This two-part proposal will enable magistrates to ensure that Stingray warrants do not become *de facto* "general warrants" effectively nullifying Fourth Amendment protections. Part V will discuss and respond to potential criticisms of this solution.

II. OPERATIONAL CAPABILITIES OF THE STINGRAY

Stingrays are used in mobile cell phone networks to "identify and eavesdrop" on cell phones.[27] Cell phones connect to the global network through a wireless carrier's base station, and a Stingray is designed to mimic a base station and "trick" cell phones into connecting to it.[28] Stingrays emit a stronger frequency signal than wireless carrier base stations, and thus "exploit [a cell phone's] behavior to prefer the strongest cell phone tower in [its] vicinity."[29] Technology companies in the United States, including the Harris Corporation,

24. *Comprehensive Drug Testing*, 621 F.3d 1162.
25. *Id.* at 1178 (Kozinski, C.J., concurring).
26. *See generally id.* at 1178–1180.
27. DABROWSKI ET AL., *supra* note 8.
28. *Id.*
29. *Id.* (alteration in original).

offer Stingrays for purchase by law enforcement agencies.[30] The Harris Corporation's Stingray device is available for a base price of roughly $75,000.[31] The devices were originally designed simply to steal IMSI numbers[32] from phones, which allows authorities to identify the phone number associated with each particular cell phone and track the location of each cell phone within a few meters.[33] However, more recent versions offer call and message interception features, along with features allowing the interception of data and content, including emails.[34] For example, the Harris Corporation offers an "Intercept Software Package" as a supplement to its Stingray product.[35]

The operational capabilities of the Stingray device should be troubling to all citizens, not just those involved in criminal activity. First, the use of Stingrays impacts countless numbers of innocent third parties, not just the target of an investigation.[36] A Stingray sends electronic signals to all of the cell phones within its vicinity and triggers an automatic response from each cell phone.[37] This "dragnet sweep of third-party information"[38] enables law enforcement to track the location and intercept the data of all the individuals within a range of "several kilometers."[39] In other words, by use of a Stingray, law enforcement can invade the privacy of potentially thousands of innocent parties in the pursuit of often a single individual suspected of criminal activity. The devices also drain the battery

30. *Id.*; Letter from Lin Vinson, Major Account Manager, Harris Corp., to Raul Perez, City of Miami PD (Aug. 25, 2008) (on file at http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf).

31. HARRIS GCSD PRICE LIST, HARRIS CORP. WIRELESS PRODS. GRP. (2008) (on file at http://info.publicintelligence.net/Harris-SurveillancePriceList.pdf).

32. An IMSI number is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI number identifies a GSM subscriber. It is stored in the Subscriber Identity Module (SIM) inside the phone and is sent by the phone to the appropriate network. The IMSI number is used to acquire details about the mobile in the Home Location Register (HLR) or the Visitor Location Register (VLR). *See* Cory Janssen, *International Mobile Subscriber Identity (IMSI)*, TECHOPEDIA, http://www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi (last visited Sept. 17, 2005).

33. DABROWSKI ET AL., *supra* note 8.

34. *Id.*

35. HARRIS GCSD PRICE LIST, *supra* note 31.

36. Rigmaiden Brief, *supra* note 21, at 10.

37. DABROWSKI ET AL., *supra* note 8.

38. Rigmaiden Brief, *supra* note 21, at 10.

39. DABROWSKI ET AL., *supra* note 8.

of the affected third-party cell phones and disrupt their network connectivity.[40]

Second, Stingrays connect to third-party cell phones in the same manner as a network carrier's base station, and thus the devices necessarily send signals into private areas including homes, offices, and the like.[41] This means that the government can ascertain a cell phone user's location and activity not just in areas accessible to the public, but in areas that are supposed to provide optimal privacy and personal autonomy.[42] Further, Stingrays can "pinpoint an individual with extraordinary precision, in some cases 'within an accuracy of 2 m[eters].'"[43] Thus, not only can the police know which private residence a cell phone user is occupying, but which *room* of that private residence, and indeed what specific two-meter area of that room.[44] This leads to an unsettling realization: Stingrays give government officials the ability to track your movements and activity twenty-four hours a day wherever you are; there is no longer any realm of personal privacy from the government to which a citizen can retreat.

Precise movement tracking is a concerning feature of the Stingray. All individuals have sensitive personal information that they seek to keep private, even in public spaces. Supreme Court Justice Sonia Sotomayor explained this fact thoroughly in her concurrence in *United States v. Jones*, a case involving GPS monitoring of the defendant's car.[45] Precise movement tracking of a person's cell phone, like the defendant's car in *Jones*, "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."[46] Information disclosed by precise movement tracking of an individual's cell phone will reveal trips of an intimately private nature: "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the

40. Julian Dammann, IMSI-Catcher and Man-in-the-Middle Attacks, Presentation at the Seminar on Mobile Security at the Univ. of Bonn (Feb. 9, 2011) (on file at http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf).

41. *See, e.g.*, *What You Need to Know About Your Network*, AT&T, http://www.att.com/gen/press-room?pid=14003 (last visited Oct. 31, 2015).

42. *See generally id.*

43. Rigmaiden Brief, *supra* note 21, at 11 (citing PKI ELEC. INTELLIGENCE GMBH GER., GSM CELLULAR MONITORING SYSTEMS (2010) (citation omitted).

44. *See id*.

45. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

46. *Id.* (citing People v. Weaver, 882 N.Y.S.2d 357, 909 (App. Div. 2009).

criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar" and so on.[47] The government can then store these records and "efficiently mine them for information years into the future."[48]

While Justice Sotomayor highlights how deeply troubling precise movement tracking is in itself, the chilling fact is that the Stingray's operational capabilities go much further.[49] One technology company describes the functionalities of its Stingray product by stating that "[t]he user can control the level of service to the target mobiles, selectively Jam[50] specific mobiles, perform silent calls, call or SMS on behalf of target mobile, change SMS messages . . . and many additional operational features."[51] Technology companies that offer Stingray products typically sell the "base" model by itself, which is capable of ascertaining a mobile device's IMSI number and cell phone number and tracking the device, and sell the "add-ons" allowing for the more alarming functions separately.[52] Also, data encryption software does not protect a smartphone user from a Stingray's "state-of-the-art" attack: current models "allow for a timely decryption and key recovery."[53] The operational capabilities of the Stingray clearly underscore the extreme intrusiveness involved in law enforcement's use of the device to investigate criminal activity and highlight the need for heightened judicial supervision of Stingray searches.

III. THE FOURTH AMENDMENT IN THE DIGITAL AGE

The Fourth Amendment to the United States Constitution states:[54]

47. *Id.* (quoting *Weaver*, 882 N.Y.S.2d at 909).

48. *Id.* at 955–56 (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting).

49. DABROWSKI ET AL., *supra* note 8.

50. "Jamming" refers to a multi-faceted technique that includes preventing the mobile device from making or receiving calls, text messages, and emails; preventing the mobile from connecting to the Internet via Wi-Fi; and preventing the mobile's GPS unit from receiving correct positioning signals. *See GPS, Wi-Fi, and Cell Phone Jammers*: *Frequently Asked Questions (FAQs)*, FED. COMMC'NS COMM'N ENF'T BUREAU, transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf (last updated Oct. 9, 2015).

51. ABILITY, *supra* note 10 (alteration in original).

52. *See, e.g.*, DABROWSKI ET AL., *supra* note 8; ABILITY, *supra* note 10; Lin Vinson, *supra* note 30; HARRIS GCSD PRICE LIST, *supra* note 31.

53. *See* DABROWSKI ET AL., *supra* note 8.

54. U.S. CONST. amend. IV.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Since the adoption of the Fourth Amendment, the Supreme Court has developed an extensive and complicated set of jurisprudential rules interpreting its text.[55] An understanding of the origins of the Fourth Amendment will help to put the Court's jurisprudence in context.

A. Origins of the Fourth Amendment

The Fourth Amendment was a "cause and a product of the American Revolution," and the Framers enacted it as a safeguard against what they considered to be one of the most profound evils perpetrated by the English Crown against the colonists: unreasonable searches and seizures.[56] Under English rule, colonial representatives of the Crown regularly executed general search warrants, called "Writs of Assistance," which authorized officials to "go into any house, shop, cellar, warehouse or room, or other place, and in case of resistance, to break open doors, chests, trunks and other packages" to search for and seize any "prohibited" items.[57] No factual basis was required to justify these intrusions; British officials were free to rummage through any privately owned property that they wished to search.[58]

The framers responded to this tyrannical practice by enacting the Fourth Amendment, which was designed to prevent similar abuses in the new American nation.[59] The amendment safeguards the civil liberties of American citizens by ensuring that the government may only obtain a search warrant upon a showing of probable cause and every government search must be reasonable whether or not conducted pursuant to a warrant.[60]

55. *See generally* LEWIS R. KATZ ET AL., BALDWIN'S OHIO PRACTICE CRIMINAL LAW § 4 (3d ed. 2006).
56. *Id.*
57. *Id.*
58. *Id.*
59. *See id.*
60. *Id.*

B. Modern Interpretation

The Supreme Court has developed a comprehensive and detailed interpretation of the Fourth Amendment since its enactment.[61] In *Katz v. United States*, the Court established the current test that states that a search occurs where governmental officials intrude on an individual's "reasonable expectation of privacy."[62] In order for an individual's expectation of privacy to be afforded constitutional protection, two prongs must be satisfied: (1) the individual must exhibit an actual, subjective expectation of privacy; and (2) that expectation must be "one that society is prepared to recognize as 'reasonable.'"[63] More recently, in *United States v. Jones*, the Court explained that *Katz* "did not narrow the Fourth Amendment's scope," and instead supplemented the existing property-based Fourth Amendment rule: when the government engages in "physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment."[64] Although the Court has maintained that a search is "presumptively unreasonable" in the absence of a warrant, the true test is whether a search is reasonable. For this reason, the Court has found many types of warrantless searches to be reasonable.[65]

The Court also requires that all searches be supported by adequate "probable cause."[66] The Court has defined probable cause as existing "where 'the facts and circumstances within their (the officers') knowledge and of which they had reasonably trustworthy information (are) sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed."[67] The probable cause requirement "seek[s] to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime"[68] by limiting baseless searches unsupported by adequate facts. Magistrates are vested with a vital constitutional responsibility in the issuance of search warrants to determine that all aspects of the search are supported by probable

61. *See generally id.*
62. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
63. *Id.* at 361.
64. United States v. Jones, 132 S. Ct. 945, 951 (2012) (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)).
65. *See Katz*, 389 U.S. at 360.
66. Brinegar v. United States, 338 U.S. 160, 174 (1949).
67. *Id.* at 175 (quoting Carroll v. United States, 267 U.S. 132, 162 (1925).
68. *Id.* at 176.

cause.[69] Magistrates also have a duty to impose appropriate limitations and conditions on the scope and execution of warrants, and police officers must "execute the warrant as directed by its terms."[70]

Next, the Fourth Amendment requires that a warrant "particularly describe both the place to be searched and the person or things to be seized."[71] The particularity requirement "prevents general, exploratory searches and indiscriminate rummaging through a person's belongings."[72] It also ensures that the issuing magistrate is "fully apprised of the scope of the search."[73]Magistrate judges have a duty to impose limitations on the scope of a search and seizure "in order to prevent an overly intrusive search."[74] In *Dalia v. United States*,[75] the Court held that the Fourth Amendment warrant requirement necessitates only three things: (1) issuance by a detached and neutral magistrate; (2) probable cause; and (3) a particular description of the things to be seized and the place to be searched.[76] However, some courts and commentators have also recognized a "duty of candor" owed by government agents in presenting warrant applications to judicial officers.[77] This duty requires the government to fairly disclose the scope of the intended search, including the likely impact on third parties. A lack of candor in any aspect of the warrant application "must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized [items]."[78] The rationale behind the duty is that a magistrate cannot faithfully perform his vital constitutional function if the government withholds material information relating to the scope of the search.[79] A reviewing court, in deciding whether an executed search exceeded the scope authorized in the warrant, looks to "the circumstances surrounding the issuance of the warrant,

69. Illinois v. Gates, 462 U.S. 213, 263 (1983).
70. *Id.* at 262.
71. United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986).
72. *Id.*
73. *Id.*
74. United States v. Rettig, 589 F.2d 418, 423 (9th Cir. 1978).
75. Dalia v. United States, 441 U.S. 238 (1979).
76. Christina M. Schuck, Note & Comment, *A Search for the Caselaw to Support the Computer Search "Guidance" in* United States v. Comprehensive Drug Testing, 16 LEWIS & CLARK L. REV. 741, 774 (2012) (citing *Dalia*, 441 U.S. at 255)).
77. United States v. CDT, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring).
78. *Id.* (alteration in original).
79. Rigmaiden Brief, *supra* note 21, at 14 (citing *Rettig*, 589 F.2d at 422–23).

and the circumstances of the search."[80] Certainly, when a court analyzes a search based on the "totality of the circumstances"[81] surrounding the search, the impact on third-party privacy should be considered.

Finally, of particular relevance here is the "plain-view" doctrine.[82] The plain view doctrine provides that when the police have a warrant to search a given area for specified items, and "in the course of the search [they] come across some other article of incriminating character," they are authorized to seize that item.[83] The Court has established three conditions that must be satisfied to justify warrantless seizure under the plain view doctrine: (1) the item must be in plain view of the officer; (2) its incriminating character must be "immediately apparent"; and (3) the officer must have a lawful right of access to the object itself.[84] This doctrine elicits dangerous possibilities in the context of Stingray use. Unless magistrates impose proper limitations on the use of this device, the police may sift through thousands of third-party emails, text messages and phone calls in the pursuit of a single suspect.[85] Furthermore, there is nothing to prevent police officers or federal agents from "seizing" and reviewing ostensibly "incriminating" data from third parties not the subject of investigation and using that information against them.

C. Application in the Digital Age

The complex set of rules developed since the enactment of the Fourth Amendment have proved difficult for courts to apply in a consistent manner, and the emergence of advanced digital technology has further clouded the issue. Courts face significant challenges in attempting to apply the text of an amendment designed to prevent governmental intrusion into houses, shops, and cellars[86] to cell phones, computers, and other digital devices. The emergence of these technologies has resulted in situations implicating Fourth Amendment concerns that were beyond the imagination of the Framers of the Constitution.

80. United States v. Hurd, 499 F.3d 963, 966 (9th Cir. 2007) (citation omitted).
81. United States v. Weikert, 504 F.3d 1, 7 (1st Cir. 2007) (citation omitted).
82. Horton v. California, 496 U.S. 128, 133–34 (1990).
83. *See id.* at 136 (alteration in original).
84. *Id.* at 136–37. (citing Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).
85. *See* DABROWSKI ET AL., *supra* note 8.
86. *See* KATZ ET AL., *supra* note 55, at § 4.

1. Stingray Use Constitutes a Fourth Amendment Search

The first question that arises in the context of new technologies like the Stingray is whether the use of the technology at issue constitutes a "search" for the purposes of the Fourth Amendment. The Supreme Court has decided a number of cases that raised this question in the context of other technologies, and Congress has enacted legislation that attempts to address the issue of law enforcement's use of certain advanced technology. In *Smith v. Maryland*, a case decided in 1979, the Court held that the installation and use of a pen register,[87] a device designed to record the numbers dialed from the defendant's phone, was not a "search" that required a warrant.[88] The Court reasoned that because the defendant voluntarily turned over the numbers that he dialed to a third party (the telephone company) he did not have a "reasonable expectation of privacy" in those numbers.[89]

Congress responded to the Court's decision in *Smith* by enacting the Electronic Communications Privacy Act of 1986 (ECPA).[90] The Act established a number of regulations designed to make electronic surveillance laws uniform, and it included the "pen/trap" provisions that addressed law enforcement's use of pen registers.[91] The so-called "Pen Register Statute" made it unlawful for the government to use a pen register to gather evidence in an investigation without first obtaining a court order based upon a showing that the information likely to be obtained through surveillance of the target phone is "relevant to an ongoing criminal investigation."[92] Fifteen years later, Congress enacted the USA PATRIOT Act,[93] and one provision of the Act amended the definition of a "pen register" to make it more

87. A "pen register" is a mechanical device attached to a telephone line and installed at a central telephone facility. It functions by recording on a paper tape all phone numbers dialed from that phone line. It does not identify the telephone numbers from which incoming calls originate, nor does it reveal whether any call, incoming or outgoing, was completed successfully. It does not involve any monitoring of telephone conversations. *See* United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., dissenting in part).

88. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

89. *Id.* at 744.

90. H.R. Res. 4952, 99th Cong. (1986) (enacted).

91. 18 U.S.C. §§ 3121–3127 (1986).

92. *See, e.g.*, *In re* Application of the United States for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 439 (S.D.N.Y. 2005).

93. H.R. Res. 3162, 107th Cong. (2001) (enacted).

encompassing.[94] Due to this amendment to the Pen Register Statute, law enforcement agencies have been able to convince some magistrates to issue court orders under the statute for the use of Stingrays.[95] However, the Pen Register Statute should not even apply to Stingrays. The amended definition of a "pen register" under the statute describes it as "a device . . . [that] records or decodes dialing, routing, addressing, or signaling information . . . ."[96] The Stingray does not fit this definition: the base model including only the most limited functions includes precise location tracking and the ability to ascertain the phone number and IMSI number of a cell phone.[97] Also, the Pen Register Statute requires that the order state "the number and, if known, physical location of the telephone line" that the pen register is to be attached to.[98] However, in the context of Stingrays and other digital analyzers, the telephone number and location of the phone typically will not be known at the time that an order is issued, and thus "it would be impossible to comply literally with the requirements of § 3123(b)(1)(C)."[99] For these reasons, an order issued pursuant to that statute is insufficient to justify the use of a Stingray.[100]

Further, unlike pen registers, Stingray use constitutes a Fourth Amendment search, which requires a showing of probable cause and a warrant. In *Kyllo v. United States*[101] the Court held that police officers' use of thermal imaging technology to detect heat levels from the defendant's home was a search because the technology

94. The amended definition states: "the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;" 18 U.S.C. § 3127(3).

95. *See, e.g.*, *In re* Application of the United States for an Order, 433 F. Supp. 2d 804 (S.D. Texas 2006).

96. 18 U.S.C. § 3127(3) (alteration in original).

97. DABROWSKI ET AL., *supra* note 8.

98. *In re* Application of United States for an Order Authorizing Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 200 (C.D. Cal. 1995) (quoting 18 U.S.C. § 3123(b)(1)(C)).

99. *Id.* at 201.

100. *See In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).

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

allowed the police to obtain information that could not otherwise be obtained without "intrusion into a constitutionally protected area."[102] The Court limited its holding in that case as applicable where "the technology in question is not in general public use."[103]

Like the thermal imaging device in *Kyllo*, a Stingray sends signals that penetrate the walls of a home, which allows the police to obtain information about the suspect that they could not obtain otherwise without intruding into the home itself.[104] Under this analysis, use of a Stingray to monitor phones in public areas ostensibly would not constitute a Fourth Amendment search; however, when a Stingray is deployed it affects all cell phones within an area of "several kilometers,"[105] and it is reasonable to assume that at least some of those affected cell phones will be inside private residences. Also, the Stingray cannot plausibly be characterized as being "in general public use."[106] Stingray manufacturers typically offer the device exclusively to police departments and federal law enforcement agencies through vendor letters sent directly to those agencies, and even a "base" model Stingray costs about $75,000, which is likely too expensive for most members of the general public to purchase.[107] Interestingly, in *Rigmaiden* the government stipulated to the fact that it conducted a Fourth Amendment search when it used a Stingray to ascertain the defendant's location inside his apartment.[108] Thus, the government "acknowledged that the proper analysis [for Stingrays] had to be pursuant to Fourth Amendment search and seizure jurisprudence."[109]

In *Riley v. California*, the Court indicated that examining the contents of a person's cell phone constitutes a Fourth Amendment

102. *Id.* at 34; *see also* United States v. Karo, 468 U.S. 705, 715 (1984) (holding that installation of an electronic monitor on a can of ether taken into the defendant's residence constituted a Fourth Amendment search).

103. *Kyllo*, 533 U.S. at 34.

104. *Id.*; AT&T, *supra* note 41; *see also* United States v. Jones, 132 S. Ct. 945, 950 (2012) (holding that the government's installation and monitoring of a GPS device on suspect's vehicle constituted a search due to "physical intrusion" for the purpose of obtaining information).

105. DABROWSKI ET AL., *supra* note 8.

106. *See Kyllo*, 533 U.S. at 34.

107. *See, e.g.,* DABROWSKI ET AL., *supra* note 8; ABILITY, *supra* note 10; Lin Vinson, *supra* note 30; HARRIS GCSD PRICE LIST, *supra* note 31.

108. United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (citing Government Doc. 723 at 13–14).

109. *In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) (alteration in original).

search.[110] *Riley* held that the police officer's warrantless search of the contents of the defendant's phone was unreasonable, and it could not be justified by the "search incident to arrest" exception.[111] That exception allows the police to make a limited warrantless search of the arrestee's person and the area within the arrestee's immediate control following a lawful, custodial arrest.[112] Because the government did not contest that examining a phone's content is a search, the Court assumed without deciding that in this case examining the contents of the defendant's phone constituted a Fourth Amendment search.[113]

Thus, under *Riley*,[114] use of a Stingray's "add-on" features that allow for software content interception[115] also constitutes a Fourth Amendment search. Like the police officer examining the contents of the defendant's phone in that case, Stingrays allow police officers to examine the contents of cell phones remotely, and thus intrude on cell phone users' reasonable expectations of privacy in a similar manner as the police officer in that case.[116]

Although there have been a number of cases decided regarding what constitutes a "search" in the digital age, there is scant case law addressing the warrant requirements applicable to searches involving electronic data and Stingrays. However, one important case was recently decided in the Ninth Circuit and another case is currently pending in the District Court of Arizona, both of which will be discussed below.

2. The Stingray Examined: *United States v. Rigmaiden*

The first federal district court case to address the constitutional implications of Stingray searches, *United States v. Rigmaiden*, is currently pending in the District Court of Arizona.[117] In *Rigmaiden*, the government indicted the defendant, Daniel Rigmaiden, on seventy-four counts of mail and wire fraud, aggravated identity theft,

110. Riley v. California, 134 S. Ct. 2473, 2485 (2014).
111. *Id.* at 2484–85.
112. *Id.* at 2490–94.
113. *Id.* at 2482.
114. *Id.* at 2485.
115. *See* DABROWSKI ET AL., *supra* note 8.
116. *Riley*, 134 S. Ct. at 2482; DABROWSKI ET AL., *supra* note 8.
117. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012).

and conspiracy.[118] The defendant allegedly perpetrated a scheme to obtain fraudulent tax refunds by filing electronic tax returns in the names of hundreds of deceased persons and third parties.[119] The government located the defendant by tracking the location of an aircard[120] in his possession. The defendant and the ACLU argued that the technology used by the government—Stingray technology—violated his Fourth Amendment rights even though the government obtained a warrant to use the technology.[121]

The defendant filed a motion to suppress evidence obtained through use of the Stingray, and the ACLU and the Electronic Frontier Foundation (EFF) filed an *amici curiae* brief in support of his motion.[122] They argued that the government's Stingray search exceeded the scope of the warrant issued in the investigation of Mr. Rigmaiden.[123] The warrant directed Verizon Wireless to provide the government with information and assistance in tracking the defendant, but "nowhere authorize[d] the *government* to search or seize anything."[124] The warrant application also failed to describe the technology that the government planned to use, and only made fleeting references to a "mobile tracking device."[125] The application also implied that Verizon would operate the device and turn the information it gathered over to government agents.[126] The district court concluded that the Stingray surveillance was not outside the scope of the warrant, although it conceded that the so-called "Tracking Warrant" was "not a model of clarity."[127]

The defendant and the ACLU also argued that because Stingrays are a "new and potentially invasive technology," the government was required to describe the technology in detail in the warrant application.[128] The court conceded that the government failed to

118. Order Denying Motion to Suppress, United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013).

119. *Id*.

120. An aircard is a wireless adapter for cellular data; also called a "cellular modem," "data card," "3G modem," or "4G modem." *Definition of: Air Card*, PCMAG, http://www.pcmag.com/encyclopedia/term/59687/air-card (last visited Sept. 17, 2015).

121. *Rigmaiden*, 2013 WL 1932800, at *1.

122. *Id*. at 14.

123. *Id*.

124. Rigmaiden Brief, *supra* note 21, at 12 (alteration in original).

125. *Id*.

126. *Id*. at 13.

127. Order Denying Motion to Suppress, United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *19 (D. Ariz. May 8, 2013).

128. *Id*.

alert the magistrate to the privacy implications for third parties that use of the Stingray would involve, stating, "the application did not disclose that the mobile tracking device would capture signals from other cell phones and aircards in the area of Defendant's apartment."[129] However, the court quickly disposed of this issue by regarding it as a "detail of execution" which need not be specified.[130] Further, the court contended that the government's omissions implicated only the question of "how the search would be conducted," and were not material to the probable cause determination.[131] In conclusion on this point, the court considered it relevant that the warrant did not explicitly authorize the government to retain and review intercepted third-party data.[132]

The district court in *Rigmaiden* underestimated the potential for abuse of Stingray technology by police, and overestimated the wisdom of allowing government agents to set restrictions on their own search warrants, instead of requiring those decisions to be made by a judicial officer. The court failed to recognize the fundamental aspect of Fourth Amendment jurisprudence that states that decisions regarding the limitations on a search warrant are to be made by neutral, detached magistrates, not by police officers involved in the "often competitive enterprise of ferreting out crime."[133] For example, the court suggests that the lack of a specific provision in Stingray warrants authorizing the government to retain and review intercepted third-party data will result in the government refraining from doing so.[134] While this certainly may be true in some cases, it is not a reassuring safeguard against privacy intrusions to allow the government to make these determinations. A "neutral and detached magistrate"[135] must make the decisions regarding how a Stingray search is to be executed and how third-party data will be handled, not police officers and other government agents. The emergence of Stingray technology necessitates a new standard for search warrants imposing affirmative requirements on law enforcement and putting the decisions regarding limitations and conditions of the warrants in the hands of magistrate judges, not police officers.

129. *Id*. at 20.
130. *Id*.
131. *Id*. at 21 (quoting United States v. Mittelman, 999 F.2d 440, 444 (9th Cir. 1993).
132. *Id*. at 22.
133. Johnson v. United States, 333 U.S. 10, 14 (1948).
134. *See Rigmaiden*, 2013 WL 1932800, at *19.
135. Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972).

3. Guidelines to Follow: *United States v. Comprehensive Drug Testing, Inc.*

In a case decided in 2010,[136] the Ninth Circuit strongly emphasized the need for heightened judicial supervision of searches in the context of evolving technology, "where the danger of overly intrusive searches and seizures is acute."[137] Specifically, the court addressed the "procedures and safeguards that federal courts must observe in issuing and administering search warrants" for electronic data.[138]

The case involved a federal investigation into the Bay Area Lab Cooperative (BALCO), which the government suspected of providing steroids to professional baseball players.[139] Comprehensive Drug Testing, Inc. (CDT) administered a Major League Baseball program that provided for suspicionless drug testing of all players, and maintained a list of players tested and their respective test results.[140] During the investigation, the government learned of ten players who had tested positive for steroid use.[141] Federal authorities subsequently obtained a warrant in California authorizing the search of CDT's facilities in Long Beach, and the warrant was limited to the records of the ten players as to whom the government had probable cause.[142] The magistrate who issued the warrant granted "broad authority for seizure of [electronic] data," including a large volume of computer equipment, data storage devices, manuals, logs, and other materials.[143] However, the warrant also contained "significant restrictions on *how* the seized data were to be handled," designed to ensure that the investigators would not examine data beyond the scope of the warrant.[144] Despite these restrictions, when the agents executed the search warrant they seized and reviewed electronic drug testing records of hundreds of players and many other innocent clients of CDT.[145] CDT and the Players Association moved for the return of the property seized, and the reviewing judge found that the

136. United States v. CDT, 621 F.3d 1162 (9th Cir. 2010).
137. Rigmaiden Brief, *supra* note 21, at 14.
138. *CDT*, 621 F.3d at 1165–66.
139. *Id*. at 1166.
140. *Id*.
141. *Id*.
142. *Id*.
143. *Id*. at 1168.
144. *Id*. (emphasis added).
145. *Id*. at 1166.

government had failed to comply with the procedures specified in the warrant and ordered the property returned.[146]

The Ninth Circuit, sitting *en banc*, agreed with the lower court and affirmed its order, emphasizing the "threat to the privacy of innocent parties" from an investigation involving electronic data like the one in this case.[147] The court was troubled by two constitutional problems that an opposite holding would cause: (1) broad authorization for law enforcement to examine electronic records would create a risk that every warrant for electronic data would become a *de facto* general warrant; and (2) authorizing the government to sift through third-party electronic data in the search for a suspect's data without judicial restraint would allow the government to claim that a third party's data is in "plain view" and, if incriminating, would allow the government to retain it.[148]

Chief Judge Kozinski wrote a concurring opinion in the case,[149] and that opinion is particularly relevant to Stingray searches. The Chief Judge agreed with the court's holding, but wrote a separate opinion in order to provide guidance to magistrates about how to deal with search warrants for electronic data.[150] The guidelines that he set forth are as follows: (1) the government must waive reliance upon the plain view doctrine in digital evidence cases; (2) segregation and redaction of electronic data must be done either by specialized government personnel or an independent third party, and those personnel must not disclose to investigators any data other than that which is the target of the warrant; (3) warrants must fairly disclose the risks of destruction of information; (4) the government's search protocol must be designed to uncover only the information for which it has probable cause; and (5) the government must destroy the non-responsive data collected from third parties.[151]

These recommendations by the Chief Judge are sensible guidelines designed to protect third=party privacy, and they are applicable and adaptable to Stingray searches. First, the electronic data seized in *CDT* included electronic directories and drug testing records cop-

146. *Id.*
147. *See id.* at 1175.
148. *Id.* at 1176.
149. *Id.* at 1178.
150. *Id.*
151. *Id.* at 1180.

ied from CDT's computers,[152] and Stingrays are capable of intercepting electronic content like that seized in *CDT*.[153] Next, "smartphones" function similarly to desktop computers; "the main difference is that one is portable and the other is not."[154] Finally, the main concern surrounding Stingray data interception is similar to that implicated by the electronic data search in *CDT*: Stingrays allow authorities to "sift through" third-party cell phone data the same way that the government sifted through third-party electronic records in *CDT*.[155]

The Chief Judge also discussed the government's "duty of candor" in submitting warrant applications and affidavits, emphasizing the vital importance of this duty in the context of electronic data searches.[156] In *CDT*, the government presented a warrant application that outlined theoretical risks that data might be destroyed if the warrant did not grant broad seizure authority.[157] However, the application failed to mention that CDT had pledged to keep all data intact until the Northern California District Court ruled on its motion to quash the subpoena.[158] The government's omission "created the false impression that, unless the data were seized at once, it would be lost."[159] Chief Judge Kozinski proceeded to state that "omitting such highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant application," and that the government should be held to a stricter duty of candor in the context of electronic data searches.[160] Similarly, the government must be held to a stricter duty of candor in the context of Stingray searches in order to allow magistrates to evaluate all the information material to the search warrant, including the capabilities of the device and the likely impact on third parties, so that the magistrate can impose appropriate limitations on the execution and scope of the warrant.

152. United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1092 (9th Cir. 2008).

153. *See* DABROWSKI ET AL., *supra* note 8.

154. John C. Dvorak, *Should We Consider the Smartphone a Computer?*, PCMAG (Dec. 4, 2012, 3:34 PM), http://www.pcmag.com/article2/0,2817,2412850,00.asp.

155. *See* DABROWSKI ET AL., *supra* note 8; *CDT*, 621 F.3d at 1166, 1176.

156. *CDT*, 621 F.3d at 1162, 1178.

157. *Id.*

158. *Id.*

159. *Id.* (citation omitted).

160. *Id.*

IV. PROPOSAL FOR HEIGHTENED WARRANT REQUIREMENTS IN THE CONTEXT OF STINGRAYS

Because law enforcement's use of Stingrays to conduct Fourth Amendment searches presents an increased risk of abuse and is especially intrusive, there is a need for heightened judicial supervision of Stingray searches. The appropriate solution involves a two-fold proposal for the issuance of search warrants involving Stingray technology. First, magistrate judges must require government officials to include in warrant applications and affidavits a detailed description of the technology and its capabilities in order to allow magistrates to impose appropriate limitations on the scope and execution of the warrant to mitigate the impact on the privacy of third parties. Second, magistrates should impose the following specific limitations and conditions on Stingray warrants: (1) government officials must waive reliance on the plain view doctrine; (2) segregation and redaction of electronic data must be done by specialized government personnel not involved in the investigation, and those personnel must not disclose to the investigators any information other than that which is the target of the warrant; (3) the government's search protocol must be narrowly tailored to uncover only the information for which it has probable cause, and agents may examine that information only; and (4) the government must immediately destroy all intercepted third-party data without examining its contents.[161] These guidelines for the issuance of search warrants involving Stingray use will serve to protect innocent third parties from unreasonable governmental intrusion on their privacy and, most significantly, will prevent law enforcement from abusing this incredibly powerful technology.

A. "Duty of Candor" Requirement

The first part of this two-fold proposal is that judicial officials must require government agents to include in warrant applications and affidavits a detailed description of the technology it plans to use and its capabilities in order to allow magistrates to impose appropriate limitations on the scope and execution of the warrant. Law enforcement's description of the Stingray and its capabilities should be detailed enough to allow the magistrate to get a general idea of how

161. *See generally id.* at 1180 (Kozinski, C.J., concurring).

the technology works, how the government plans to use it, what functions of the device it plans to employ, and the general geographic and temporal parameters that will be implicated by the government's use of the device. This requirement could be satisfied by law enforcement attaching the device's manual as an exhibit and then describing in sufficient detail which functions it plans to employ and where and for how long it will employ them.

It is particularly important for the government to be candid towards magistrates in the context of Stingray warrant applications because Stingray manufacturers typically sell the base model by itself, and sell the "add-ons" allowing much more intrusive functions separately.[162] That means that even if law enforcement states in the warrant application that it intends to use a Stingray in executing the warrant, magistrates cannot be certain what functions the government intends to employ unless that information is included in the application. Whether law enforcement intends to employ only the "base" model of a Stingray, or one or more of the offered "add-ons," can make a radical difference in the scope of the search.[163] For example, if a law enforcement agency intends to use only the base model Stingray, the agency will only be able to utilize the device's more limited functions, including ascertaining the target phone's IMSI number and phone number and precisely tracking the phone.[164] However, if the government plans to use one or more of the typical supplements to the base model, it may be able to "jam" the target phone, perform silent calls or send text messages on behalf of the target phone, or change the content of text messages, phone calls, or emails sent to and from the target phone.[165] Therefore, in order for magistrates to be confident that they are fully apprised of the scope of the intended search, the government must make clear which company's Stingray product it intends to use, how it intends to use it, and which functions it intends to employ.

The government's candor in this regard will allow magistrates to fully examine the scope of the intended search and impose sensible limitations and conditions on its scope and execution. Depending on the facts and circumstances of the particular case, the magistrate

162. *See, e.g.*, DABROWSKI ET AL., *supra* note 8; ABILITY, *supra* note 10; Lin Vinson, *supra* note 30; HARRIS GCSD PRICE LIST, *supra* note 31.

163. *See generally id.*

164. *See* DABROWSKI ET AL., *supra* note 8.

165. *See* ABILITY, *supra* note 10.

will be able to limit the scope of the intended search by conditioning the issuance of the search warrant on the government's pledging to only use certain functions of the Stingray. Also, by the government disclosing the intended geographical scope of the search, the magistrate will be able to estimate the number of third-party devices that will be affected and thereby impose appropriate conditions regarding the government's handling of this wealth of third-party information. The government's candor towards magistrate judges in submitting search warrant applications for Stingray use is vitally important to the magistrate's faithfully executing his or her constitutional role, and will allow magistrates to impose specific limitations and conditions on the scope and execution of the search.

B. Specific Limitations and Conditions on Stingray Search Warrants

The second part of the two-fold proposal is that magistrates should impose specific limitations and conditions on Stingray search warrants. These limitations and conditions include the following: (1) government officials must waive reliance on the plain view doctrine in Stingray cases; (2) segregation and redaction of electronic data must be done by specialized law enforcement personnel not involved in the investigation, and those personnel must not disclose to the investigators any information other than that which is the target of the warrant; (3) the government's search protocol must be narrowly tailored to uncover only the information for which it has probable cause, and agents may examine that information only; and (4) the government must immediately destroy any intercepted third-party data without examining its contents.[166] These limitations and conditions provide sensible methods of ensuring that law enforcement does not abuse the incredible power that Stingrays allow for, and will allow magistrates to retain their vital constitutional role as the supervisors of Fourth Amendment searches. Each of these four limitations and conditions involve different concerns, and thus each will be discussed separately in turn.

166. *See* United States v. CDT, 621 F.3d 1162, 1189 (9th Cir. 2010) (Kozinski, C.J., concurring).

1. Government Must Waive Reliance on the Plain View Doctrine

The first of these four conditions is that magistrates should require the government to waive reliance on the plain view doctrine in Stingray cases. The plain view doctrine is an exception to the warrant requirement that states that when the police have a warrant to search a given area for specified items, and "in the course of the search come across some other article of incriminating character," they are authorized to seize and retain that item.[167] The plain view doctrine is particularly relevant in the context of Stingray searches because when the government deploys a Stingray, it may sift through thousands of third-party emails, text messages, and phone calls unrelated to the investigation.[168] Therefore, if during the course of a Stingray search government agents come across third-party data of "incriminating character," they would apparently be authorized to retain that data and use it against that third party.

It should be made clear, however, that the plain view doctrine "has no application to intermingled private electronic data."[169] The plain view doctrine is commonly applied to justify warrantless seizures in cases where a police officer had a prior justification for the intrusion "in the course of which he came inadvertently across a piece of evidence incriminating *the accused*."[170] However, in Stingray searches and other searches involving large volumes of intermingled private electronic data, often the evidence that police will come across will be evidence incriminating someone other than the accused, i.e., a third party. In this context, allowing the government to rely on the plain view doctrine would essentially allow it to search the data of all cell phones within a large vicinity with no prior justification needed other than the warrant obtained authorizing it to search for a single suspect. Therefore, magistrates should insist that government officials waive reliance on the plain view doctrine in Stingray searches. This will ensure that Stingray searches do not

167. Horton v. California, 496 U.S. 128, 135 (1990).

168. *See* DABROWSKI ET AL., *supra* note 8.

169. United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1117 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part).

170. United States v. McLevain, 310 F.3d 434, 439 (6th Cir. 2002) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)) (emphasis added).

make a "mockery" of the Fourth Amendment "by turning all warrants for digital data into general warrants."[171]

2. Segregation and Redaction of Third-Party Data

The second condition that magistrates should impose on Stingray warrants is to require that specialized law enforcement personnel not involved in the investigation segregate and redact all third-party data, and that those personnel not disclose to the investigators any information other than that which is the target of the warrant.[172] This is another sensible safeguard that will prevent investigating agents from collecting or reviewing third-party data and thus protect innocent third parties from the search. To accomplish this objective, the issuing magistrate should include in the warrant a protocol for preventing agents involved in the investigation from examining or retaining any third-party data.[173] The issuing judicial officer should prohibit the specialized law enforcement officers reviewing the data from communicating to the investigating agents any information other than that covered by the warrant itself.[174] This requirement is necessary due to the extremely large volume of third-party data that will inevitably be collected by a Stingray.[175]

3. The Government's Search Protocol Must Be Narrowly Tailored

Next, magistrates should require the government's search protocol to be narrowly tailored to uncover only the information for which it has probable cause, and require that agents examine that information only.[176] This narrow tailoring includes the segregation and redaction procedures discussed above, and also includes how the government plans to use the Stingray, where it plans to use it, how long it plans to use it, and which (if any) "add-on" features it plans to use. Depending on the facts and circumstances of the particular case, the issuing magistrate should require the government to only utilize the features of the Stingray that are necessary to accomplish the objective of the warrant. For example, if the search warrant

171. *See CDT*, 621 F.3d at 1178 (Kozinski, C.J., concurring).
172. *See id*.
173. *See id*. at 1179.
174. *See id*.
175. *See* DABROWSKI ET AL., *supra* note 8.
176. *See CDT*, 621 F.3d at 1180 (Kozinski, C.J., concurring).

authorizes the government to use the Stingray only to ascertain the location of the suspect, the government should only utilize the "base" model Stingray, which allows for precise movement tracking.[177] If, on the other hand, the warrant authorizes the government to "search" the suspect's phone remotely for emails, text messages, or phone calls, the government may use certain "add-ons" allowing for those capabilities.[178]

4. Destruction of Intercepted Third-Party Data

The final condition that magistrates should impose on Stingray search warrants is that, following segregation and redaction of third-party data, the specialized government personnel must immediately destroy any non-responsive third-party data intercepted during the search without revealing its contents to the investigating agents.[179] This will ensure that the government's search does not reveal any data that is not connected to the subject of the investigation and will preserve the privacy of innocent third parties. To that end, the government should also provide the issuing magistrate with a return "disclosing precisely what it has obtained as a consequence of the search," as well as a "sworn certificate that the government has destroyed . . . all copies of [third-party] data that it's not entitled to keep."[180]

These four conditions and limitations provide sensible methods by which magistrates judges can ensure that the government does not abuse the highly advanced technological capabilities involved with Stingrays. Without these limitations, the government could use a warrant authorizing them to search for a single individual's mobile data to canvass the mobile data of entire cities' populations. Therefore, this proposal ensures that the judiciary will be able to properly supervise Stingray searches and the government will not be allowed to abuse Stingray technology in criminal investigations.

V. RESPONSE TO POTENTIAL CRITICISMS OF THIS PROPOSAL

One potential criticism of this proposal could be that the solution is too complicated and will be difficult to implement. First, the re-

177. *See* DABROWSKI ET AL., *supra* note 8.
178. *See id*.
179. *See CDT*, 621 F.3d at 1180 (Kozinski, C.J., concurring).
180. *Id*. at 1179 (alteration in original).

quirement that law enforcement adhere to a duty of candor in presenting Stingray warrant applications should not be too difficult to follow. Technology companies that sell Stingrays to law enforcement agencies also send vendor letters, product descriptions, price lists, and technology manuals directly to those agencies.[181] The companies that offer Stingrays to law enforcement include descriptions of the product and its capabilities, as well as a description of each of the supplements to the product.[182] In order for the government to satisfy the first requirement of this two-fold proposal, it would be sufficient for it to attach to warrant applications as exhibits the product manual and the product descriptions sent to them by these various technology companies. Therefore, it should be practicable for the government to satisfy this requirement without expending much time or effort. Also, the list of suggestions for magistrates to follow in issuing Stingray search warrants is similarly practicable. Magistrates often impose limitations and conditions on search warrants, and these limitations and conditions are not unreasonable.

Another potential criticism of this solution could be that it is inconsistent with existing laws. In particular, the requirement that the government narrowly tailor its search protocol is most vulnerable to this criticism. As discussed above in Part III(B), in *Dalia v. United States*, the Supreme Court rejected an argument that was based partly on the fact that the magistrate in that case did not explicitly authorize the particular search protocol employed by the government.[183] There, the Court held that under the Fourth Amendment, warrants must meet only three requirements: (1) issuance by a detached and neutral magistrate; (2) probable cause; and (3) a particular description of the things to be seized and the place to be searched.[184] The Court further explained, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant."[185] While this is certainly a valid criticism, Stingray searches involve different concerns than most other searches. Due to the extremely broad scope of Stingray searches, it is necessary to require the government to include a search protocol in its warrant applica-

181. *See e.g.*, DABROWSKI ET AL., *supra* note 8; ABILITY, *supra* note 10; Lin Vinson, *supra* note 30; HARRIS GCSD PRICE LIST, *supra* note31.

182. *See, e.g.*, HARRIS GCSD PRICE LIST, *supra* note 31.

183. Dalia v. United States, 441 U.S. 238, 255 (1979).

184. Shuck, *supra* note 76, at 774 (citing *Dalia*, 441 U.S. at 255).

185. *Dalia*, 441 U.S. at 257.

tions. Also, the proposition that search warrant applications should include a search protocol, especially where electronic data is involved, is not without support.[186] Ultimately, however, this Comment proposes a substantive change to the existing law limited to Stingray search warrants due to the extremely heightened broadness and intrusiveness involved in such searches.

Finally, another potential criticism of the proposed solution is that it will be too expensive to implement effectively. As explained above, technology companies directly send all the information that police would need to present to magistrates regarding the operational features of Stingrays.[187] Therefore, presenting this information to a magistrate would involve negligible cost to law enforcement. Also, the requirement that police departments and federal law enforcement agencies have specialized personnel review the data could be met simply by the agency assigning officers already employed by that agency to review the data, which likely would not involve additional cost. Finally, the cost of a base model Stingray is around $75,000,[188] and thus if the government is prepared to shoulder the cost of a Stingray, it should be prepared to shoulder the negligible additional costs that go along with using it responsibly.

Overall, although there is some merit to each of the potential criticisms of the proposed solution, its benefits outweigh its potential drawbacks. The protection of the Fourth Amendment rights and basic civil liberties of citizens and the reaffirmation of magistrates as the supervisory authority of Fourth Amendment searches is worth the potential costs that the proposed solution could involve.

VI. CONCLUSION

The vast majority of United States citizens own a cell phone, and many people's cell phones contain intimate details concerning their private and personal lives. Stingrays allow the government to track citizens' every movement and examine the contents of their cell phones. This technology has the potential to be a very effective

186. *See In re* Search of: 3817 W. West End, First Floor Chi., Ill. 60621, 321 F. Supp. 2d 953, 959–61 (N.D. Ill. 2004) (refusing to issue a warrant that did not include a computer search protocol); United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930, at *5 (D. Utah 2001) (suppressing documents seized from the defendant's computer because agents did not present a search methodology).

187. *See, e.g.*, DABROWSKI ET AL., *supra* note 8; ABILITY, *supra* note 10; Lin Vinson, *supra* note 30; HARRIS GCSD PRICE LIST, *supra* note 31.

188. HARRIS GCSD PRICE LIST, *supra* note 31.

law enforcement tool, but it also has the potential to infringe our basic civil liberties on a nationwide scale. This Comment does not suggest that Stingrays should not be used by law enforcement at all, but simply that magistrate judges should be vested with the authority to effectively supervise their use. This proposal will likely have an impact on the ability of law enforcement to combat crime—"[p]rivacy comes at a cost."[189] The Supreme Court has long recognized this basic "truism": "[C]onstitutional protections have costs."[190] The price is worth paying to restore and protect the liberties that we fought the Revolutionary War to gain.[191] Therefore, there is a heightened need for judicial supervision of Stingray searches in order to safeguard the liberties that the Fourth Amendment was designed to protect. The judiciary must hold law enforcement to a heightened "duty of candor" in submitting search warrant applications involving Stingrays, and magistrate judges should follow strict guidelines in issuing Stingray warrants. Stingrays involve technology that was beyond the imagination of the Framers of the Constitution. In order to remain faithful to their intent, our system of jurisprudence and law enforcement must evolve to meet the concerns of the present day, including the dangerous technology that Stingrays involve.

189. Riley v. California, 134 S. Ct. 2473, 2493 (2014).
190. Coy v. Iowa, 487 U.S. 1012, 1020 (1988).
191. *See generally* KATZ ET AL., *supra* note 55, at § 4.