SPIES IN THE SKIES: DIRTBOXES AND AIRPLANE ELECTRONIC SURVEILLANCE

Brian L. Owsley[*]

INTRODUCTION

Electronic surveillance in the digital age is essentially a cat-and-mouse game between governmental agencies that are developing new techniques and technologies for surveillance, juxtaposed against privacy rights advocates who voice concerns about such technologies. In November 2014, there was a discovery of a new twist on a relatively old theme.

Recently, the *Wall Street Journal* reported that the U.S. Marshals Service was running a surveillance program employing devices—dirtboxes—that gather all cell phone numbers in the surrounding area.[1] Other federal agencies, including the Drug Enforcement Agency, Immigration and Custom Enforcement, and the Department of Homeland Security, are also documented to have used dirtboxes.[2] These dirtboxes are manufactured by

---

* Assistant Professor of Law, Indiana Tech Law School; B.A., University of Notre Dame, J.D., Columbia University School of Law, M.I.A., Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. The author recognizes both Charles MacLean and Adam Lamparello for their insightful comments and suggestions.

1. Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014, 8:22 PM), http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 [http://perma.cc/C95M-A4B5]; *see also* Sam Frizell, *Is the Government's Aerial Smartphone Surveillance Program Legal?*, TIME (Nov. 15, 2014), http://time.com/3586511/government-aerial-surveillance/ [http://perma.cc/WX9W-JEM4]; Gail Sullivan, *Report: Secret Government Program Uses Aircraft for Mass Cellphone Surveillance*, WASH. POST, (Nov. 14, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/11/14/report-secret-government-program-uses-aircraft-for-mass-cellphone-surveillance/ [http://perma.cc/578F-RSFS]; Trevor Timm, *First Snowden. Then Tracking You on Wheels. Now Spies on a Plane. Yes, Surveillance is Everywhere*, GUARDIAN (Nov. 15, 2014, 8:30 AM), http://www.theguardian.com/commentisfree/2014/nov/15/spies-plane-surveillance-us-marshals [http://perma.cc/89HM-VAJE]; 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/ [http://perma.cc/5NDU-WEXR].

2. Timm, *supra* note 1; Patrick Gallagher, *CIA and DOJ May Face Litigation over "Dirtbox" Cell Spying Technology*, JOLT DIGEST (Mar. 17, 2015),

Digital Receiver Technology (DRT), a subsidiary of Boeing. Dirtboxes get their name based on the acronym of the three letters.[3] The U.S. Marshals Service uses these dirtboxes to gather information on the locations or the cell phone numbers of criminal suspects and fugitives.

To understand how dirtboxes are used, imagine you are attending some kind of protest. While you are involved in that event, you notice a small airplane overhead. You think nothing of the airplane and soon turn your attention back to the event. That seemingly innocuous aircraft happens to be a government airplane with a dirtbox aboard. Using this device, law enforcement have been gathering cell phone data from all of those who attended the protest. Perhaps they are looking for a specific individual or two, but now they have your cell phone information along with all the other protestors.

I. DIRTBOX TECHNOLOGY AND OPERATION

A dirtbox is a two-foot-square box that operates like a cell site simulator (also known as a StingRay) by mimicking a cell phone tower.[4] The device is attached to a small plane such as a Cessna that flies over a target area believed to contain the individual subject of the investigation.[5] Specifically, "the devices force *every* cell phone in a region to connect to them."[6] In order to do so, the device briefly jams the signals of nearby cell towers and then requires all cell phones in a given radius to register with the dirtbox, thus obtaining data from not only the subject of the criminal investigation, but also from all nontargeted cell phone users in the immediate vicinity.[7]

Little information exists about StingRays. There is growing anecdotal evidence in media outlets about the public's concern regarding the use of StingRays,[8] but the information available in the public record no doubt

---

http://jolt.law.harvard.edu/digest/privacy/flash-digest-news-in-brief-180 [http://perma.cc/BVZ7-BX32]; Julian Hattem, *Dem Senators Warn Cellphone Tracking Could Violate Constitution*, THE HILL (Dec. 14, 2014, 5:58 PM), http://thehill.com/policy/technology/226711-dem-senators-fear-cell-trackers-could-violate-constitution [http://perma.cc/ULP9-CK8X].

3. Barrett, *supra* note 1.

4. Zetter, *supra* note 1; *see also* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 191–94 (2014) (discussing how StingRay devices work); Timm, *supra* note 1 ("The plane surveillance operation's on-the-ground-forebearer[,] commonly known as a [StingRay], . . . is like a dirtbox on wheels . . . .").

5. Barrett, *supra* note 1.

6. Zetter, *supra* note 1.

7. Barrett, *supra* note 1; *see also* Owsley, *supra* note 4, at 191–94.

8. *See, e.g.*, Michael Bott & Thom Jensen, *Cellphone Spying Technology Being Used Throughout Northern California*, NEWS10 (Mar. 6, 2014, 11:25 PM),

accounts for just a fraction of the use of such technology. Only a few published decisions have addressed StingRays,[9] and some courts have dealt with applications for authorization to use StingRays in electronic surveillance.[10] However, it is unknown how often the U.S. Marshals Service or other federal agencies use this technology.

There are no court decisions addressing the use of dirtboxes. Moreover, it is unclear whether law enforcement officials even seek judicial authorization prior to using dirtboxes. It is unclear how often these flights occur, but they apparently take place on a regular basis.[11] With this dearth of information regarding the use of dirtboxes, including the authority for such usage, it is important to consider the constitutional implications of dirtboxes.

II. APPLYING FOURTH AMENDMENT PRINCIPLES TO DIRTBOXES

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[12] It further mandates that "no Warrants shall issue, but upon probable cause."[13] As discussed below, the use of a dirtbox constitutes a Fourth Amendment search.[14]

---

http://www.news10.net/story/news/investigations/watchdog/2014/03/06/cellphone-spying-technology-used-throughout-northern-california/6144949/ [http://perma.cc/35UV-M8PR]; Hanni Fakhoury, *Stingrays Go Mainstream: 2014 in Review*, ELECTRONIC FRONTIER FOUND. (Jan. 2, 2015), https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream [https://perma.cc/7XXU-NAUY] (discussing discoveries of law enforcement's use of StingRays in Florida, Maryland, and Washington); Jace Larson, *Houston police chief answers questions about cellphone surveillance program*, KPRC HOUSTON (Nov. 19, 2014, 7:09 p.m.), http://www.click2houston.com/news/investigates/houston-police-have-cell-phone-surveillance-program/29807376 [http://perma.cc/VB7M-MTU4].

9. *See In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012); U.S. v. Rigmaiden, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) (FBI used a cell site simulator to track defendant's Verizon aircard); *see also In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) ("[A] 'TriggerFish' . . . enables law enforcement to gather cell site data directly, without the assistance of the service provider."); *In re* the Application of the U.S. for an Order Authorizing Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 198–99 (1995) ("[A] . . . 'digital analyzer' is a portable device that can detect signals emitted by a cellular telephone.").

10. Owsley, *supra* note 4, at 200–11 (discussing StingRay applications in various courts).

11. Barrett, *supra* note 1.

12. U.S. CONST. amend. IV.

13. *Id.*; *see also* FED. R. CRIM. P. 41 (addressing the issuance of warrants, including for the seizure of electronically stored information).

14. *See infra* notes 16–46 and accompanying text; *see also Riley v. California*, 134 S. Ct. 2473, 2485 (2014) (holding that the Fourth Amendment requires police officers to obtain a warrant before searching the data on a cell phone).

Since the 1967 decision in *Katz v. United States*,[15] the Supreme Court has used a "reasonable expectation of privacy" standard to determine whether governmental action constitutes a search pursuant to the Fourth Amendment.[16] In *Terry v. Ohio*,[17] the Supreme Court reiterated and reaffirmed this standard.[18] Furthermore, in *United States v. Jacobsen*,[19] the Court explained that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[20] Thus, a primary question regarding whether dirtboxes constitute a search is if they violate a reasonable expectation of privacy.

The Supreme Court has previously addressed surveillance by airplanes. In *California v. Ciraolo*,[21] police officers learned that Ciraolo was growing marijuana in the backyard and hiding it from terrestrial view by fences.[22] Officers trained in the identification of marijuana flew 1,000 feet above the fenced area and were able to secure photographic evidence of marijuana plants.[23] Based on evidence gathered from this airplane surveillance, police officers obtained a search warrant for the residence, seized seventy-three marijuana plants, and charged Ciraolo with the offense.[24] He subsequently filed a motion to suppress the evidence obtained from the warrantless search of his backyard, but the trial court denied his motion, and Ciraolo ultimately pled guilty.[25]

---

15. 389 U.S. 347 (1967).

16. *Katz*, 389 U.S. 347 at 360 (Harlan, J., concurring) ("I join the opinion of the Court, which I read to hold only . . . that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy . . . ." (citations omitted)).

17. 392 U.S. 1 (1968).

18. *Terry*, 392 U.S. at 9 ("We have recently held that 'the Fourth Amendment protects people, not places,' and wherever an individual may harbor a reasonable 'expectation of privacy.'" (citations omitted) (quoting *Katz*, 389 U.S. at 351; *Katz*, 389 U.S. at 361 (Harlan, J., concurring)))

19. 466 U.S. 109 (1984).

20. *Jacobsen*, 466 U.S. at 113 (citations omitted); *see also Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("[Legitimate] expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

21. 476 U.S. 207 (1986).

22. *Ciraolo*, 476 U.S. at 209.

23. *Id.*

24. *Id.* at 209–10.

25. *Id.* at 210.

In analyzing the issue, the *Ciraolo* Court relied on *Katz* to consider whether Ciraolo had a reasonable expectation of privacy.[26] The Court found that Ciraolo had a subjective expectation of privacy in his backyard, but that society would not recognize this expectation as reasonable.[27] Relying on *United States v. Knotts*,[28] the *Ciraolo* Court held that the curtilage of the home does not by itself guarantee protection from law enforcement observation, as police officers are not required to shield their eyes from viewing such areas if they are lawfully entitled to be in the place from which the observation occurs.[29] Because the officers were on an airplane in public airspace viewing Ciraolo's property with their naked eyes, the Court concluded that the airplane surveillance did not violate his Fourth Amendment rights.[30]

Similarly, in *Florida v. Riley*,[31] the Court again grappled with whether the use of a helicopter to discover marijuana plants violated the Fourth Amendment. The county sheriff received an anonymous tip that Riley was growing marijuana in the greenhouse located on the five acres behind his mobile home.[32] Although the greenhouse was obscured on two sides by walls, the other two sides were open but obscured from the ground-level view by trees and the mobile home.[33] Based on the tip, a sheriff's deputy flew 400 feet over the greenhouse and identified marijuana growing with his naked eye.[34] As a result, the sheriff's department obtained a search warrant for the greenhouse and located the marijuana, leading to charges against Riley for possession of marijuana.[35] The trial court granted Riley's motion to suppress, but the Florida appellate court reversed before certifying the question to the state supreme court, which quashed the reversal and reinstated the trial court's order granting Riley's motion to suppress.[36]

The *Riley* Court analyzed the question pursuant to *Katz* by addressing whether there was a reasonable expectation of privacy from the surveillance by helicopter.[37] Relying on *Ciraolo*, the Court concluded that there was no

26. *Id.* at 211 (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).
27. *Id.* at 211–12.
28. 460 U.S. 276 (1983).
29. *Ciraolo*, 476 U.S. at 213 (citing *Knotts*, 460 U.S. at 282).
30. *Id.* at 213–15.
31. 488 U.S. 445 (1989).
32. *Riley*, 488 U.S. at 448.
33. *Id.*
34. *Id.*
35. *Id.* at 448–49.
36. *Id.* at 449.
37. *Id.*

Fourth Amendment violation because the helicopter was lawfully in the airspace above the property.[38]

In addition to *Katz*, the Court's third party doctrine jurisprudence informs the question of the constitutionality of dirtboxes. In *Smith v. Maryland*, the Court undermined personal privacy rights by holding that the third party doctrine applied to the numbers that one dials on a telephone. In that case, the Court addressed whether the use of a pen register to obtain the suspect's dialed telephone numbers without a search warrant violated the Fourth Amendment.[39] Ultimately, the Court concluded that the installation of the pen register was not a Fourth Amendment search because the suspect had no reasonable expectation of privacy in his outgoing call log.[40] Moreover, as *Knotts* established a few years later, law enforcement officers have a right to view activity that is clearly visible to the public.[41]

Arguably, the combination of *Knotts* and *Smith* would contravene the conclusion that the use of dirtboxes is problematic, but the Court has recently issued a few decisions that call into question the rigidity of the third party doctrine. In *United States v. Jones*,[42] the Court considered whether law enforcement officers could use GPS to track a criminal suspect without a warrant.[43] In writing for the majority, Justice Scalia distinguished *Knotts* from *Jones* because *Knotts* was based on the *Katz* reasonable expectation of privacy test as opposed to common law trespass.[44]

Additionally, in *Riley v. California*, the Court considered whether a police officer's warrantless search of a suspect's cell phone violated the Fourth Amendment.[45] Because cell phones, which the Court described as minicomputers, have a large storage capacity, they hold very large amounts of private personal records.[46] Indeed, based on this large storage capacity, the Court concluded that a cell phone could hold thousands of personal records such that it was not analogous to circumstances in earlier third party

38. *Id.* at 449–52.

39. Smith v. Maryland, 442 U.S. 735, 741 (1979).

40. *Id.* at 745–46.

41. United States v. Knotts, 460 U.S. 276, 282 (1983).

42. 132 S. Ct. 945 (2012).

43. *Jones*, 132 S. Ct. at 948.

44. *Id.* at 952 (discussing *Knotts*, 460 U.S. at 278).

45. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

46. Id. at 2489–91; see also Charles E. MacLean, But Your Honor, a Cell Phone is not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest, 6 FED. CTS. L. REV. 41, 62 (2012) ("Cell phones are more like extensive computers than wallets."); Owsley, supra note 4, at 226–27 (noting that the Court viewed cell phones as "essentially small computers that stored immense amounts of data and information").

doctrine cases.[47] Thus, in holding that the warrantless search of cell phones violated the Fourth Amendment, the Court undercut the third party doctrine.

There are no exceptions to the warrant requirement that apply to searches using dirtboxes. Although cell phone users authorize their cell phones to register with their nearest telecommunications provider's cell towers, that authorization is not the same as consenting to the release of the cell phone user's data to law enforcement using a fake cell tower and dirtbox device. Indeed, the data obtained by the devices, like GPS tracking and cell phone searches, exceeds any basis to justify a search or seizure from the fact that the cell phone registers with cell towers.

III. SAFEGUARDING INDIVIDUALS' REASONABLE EXPECTATIONS OF PRIVACY

Warrantless searches of cell phones using a dirtbox are no different than warrantless searches using a StingRay. At least one court has rejected the use of StingRays without a warrant.[48] In light of *Riley* and *Jones*, the government should, absent exigent circumstances, obtain a warrant for the use of a StingRay. Similarly, the government should also obtain a search warrant in order to use a dirtbox.

It is unclear what judicial authority, if any, the federal government is seeking when using a dirtbox. In seeking authorization to use a StingRay, the federal government typically bases it application on the pen register statute. However, in order to obtain a pen register "the attorney for the Government" must simply certify "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[49] This is an extremely low standard that results in almost all pen register applications being granted, but is much too low for authorization of a StingRay or a dirtbox because they are capable of obtaining a greater amount of data, some of which is arguably private, from a greater number of citizens.[50]

Instead, judicial authorization of a StingRay or a dirtbox should be based on a probable cause standard and any search warrants issued should state

---

47. *Riley*, 134 S. Ct. at 2493; *see also* MacLean, *supra*, note 46, at 61 (dismissing any analogy because "[a] cell phone can hold millions of pages of data, while a wallet may hold a few").

48. *In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trace & Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).

49. 18 U.S.C. § 3123(a)(1); *see also* 18 U.S.C. § 3122(b)(2); Owsley, *supra* note 4, at 199.

50. Owsley, *supra* note 4, at 199–200; Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1431 (2004) ("[T]he statute does not appear to require the judge to independently assess the factual predicate for the government's certification.").

with particularity the areas that may be searched.[51] Similarly, because the use of a dirtbox and the gathering of cell phone data constitute a Fourth Amendment search and seizure, the Fourth Amendment applies to any use of it by the government, whether done in an application or not.

In addition to the search warrant, courts issuing orders authorizing dirtboxes should also be mindful of the capture by law enforcement officials of personal information and data regarding nontargeted individuals. In other words, as the Cessna with the dirtbox swoops near you at the protest, all of your cell phone's data are captured and potentially stored on government computers in perpetuity. To protect against this concern, strict guidelines should be adopted regulating the use and admissibility of information obtained with a dirtbox.

Of course, there may be times in which law enforcement legitimately needs to use an electronic surveillance device like a dirtbox and can satisfy a court's probable cause standard. There still needs to be some protection for gathering data from nontargeted individuals. Consequently, courts should implement a protocol safeguarding these third parties and their data whenever they issue orders authorizing the use of a dirtbox.[52] For example, a court could order law enforcement officials to "return any and all original records and copies, whether hardcopy or in electronic format or storage, to the Provider, which are determined to be not relevant to the Investigative Agency's investigation."[53] Former U.S. Magistrate Judge Facciola explained that a protocol was necessary because "some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right."[54]

---

51. Owsley, *supra* note 4, at 230–31; *In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trace & Trace Device, 890 F. Supp. 2d at 752 (rejecting a StingRay application based on the pen register statute in favor of a search warrant based on the Fourth Amendment).

52. *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013) ("Although the use of a court-sanctioned cell tower dump invariably leads to such information being provided to the Government, in order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information."); *In re* U.S. ex rel. for an Order Pursuant to 18 U.S.C. § 2703(d), 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012); *see also* Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 46 (2013) (recommending a protocol be designed for courts authorizing cell tower dumps).

53. *Cf. In re* Search of Cellular Telephone Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (giving the same instructions in an order authorizing the government to access historical cell site records at cell towers near a crime scene).

54. *In re* Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis, 21 F. Supp. 3d 1, 9 (D.D.C. 2013).

CONCLUSION

Dirtboxes are here. Just like Pandora's Box, once they have been opened, they cannot be closed. The goal going forward is not only to ensure that law enforcement officials seek judicial authorization before using them, but also that they comply with the Fourth Amendment. In addition to requiring a demonstration of probable cause along with a particularized search warrant, the issuing court should establish a strict protocol to protect nontargeted individuals from law enforcement officials mining their data. Any protocol should provide guidelines for what to do with this captured data to ensure that it does not end up in government databases.