## CONTENTS

Masthead ................................................................. vii
About the SEVENTH CIRCUIT REVIEW .................. viii

### Constitutional Law

**Yes, It’s the Federal Government’s Duty to Control Foreign Affairs, but What About the President? Humanitarian Concern and Refugee Resettlement in the Wake of Hate**  
Rebecca Horgan 334

**Who’s Pinging Your Phone?: Exploring the Fourth Amendment Ramifications of Stingray Devices**  
Karen Vaysman 365
ABOUT THE SEVENTH CIRCUIT REVIEW

Purpose

The SEVENTH CIRCUIT REVIEW is a semiannual, online journal dedicated to the analysis of recent opinions published by the United States Court of Appeals for the Seventh Circuit. The SEVENTH CIRCUIT REVIEW seeks to keep the legal community abreast of developments and trends within the Seventh Circuit and their impact on contemporary jurisprudence. The articles appearing within the SEVENTH CIRCUIT REVIEW are written and edited by Chicago-Kent College of Law students enrolled in the SEVENTH CIRCUIT REVIEW Honors Seminar.

The SEVENTH CIRCUIT REVIEW Honors Seminar

In this seminar, students author, edit, and publish the SEVENTH CIRCUIT REVIEW. The REVIEW is entirely student written and edited. During each semester, students identify cases recently decided by the Seventh Circuit to be included in the REVIEW, prepare initial drafts of case comments or case notes based on in-depth analysis of the identified cases and background research, edit these drafts, prepare final, publishable articles, integrate the individual articles into the online journal, and “defend” their case analysis at a semester-end roundtable. Each seminar student is an editor of the REVIEW and responsible for extensive editing of other articles. Substantial assistance is provided by the seminar teaching assistant, who acts as the executive editor.
The areas of case law that will be covered in each journal issue will vary, depending on those areas of law represented in the court’s recently published opinions, and may include:

- Americans with Disabilities Act
- antitrust
- bankruptcy
- civil procedure
- civil rights
- constitutional law
- copyright
- corporations
- criminal law and procedure
- environmental
- ERISA
- employment law
- evidence
- immigration
- insurance
- products liability
- public welfare
- securities

This is an honors seminar. To enroll, students must meet one of the following criteria: (1) cumulative GPA in previous legal writing courses of 3.5 and class rank at the time of registration within top 50% of class, (2) recommendation of Legal Writing 1 and 2 professor and/or Legal Writing 4 professor, (3) Law Review membership, (4) Moot Court Honor Society membership, or (5) approval of the course instructor.
YES, IT’S THE FEDERAL GOVERNMENT’S DUTY TO CONTROL FOREIGN AFFAIRS, BUT WHAT ABOUT THE PRESIDENT? HUMANITARIAN CONCERN AND REFUGEE RESETTLEMENT IN THE WAKE OF HATE

REBECCA HORGAN*

Cite as: Rebecca Horgan, Yes, It’s the Federal Government’s Duty to Control Foreign Affairs, but What About the President? Humanitarian Concern and Refugee Resettlement in the Wake of Hate, 12 SEVENTH CIRCUIT REV. 334 (2017), at www.kentlaw.iit.edu/Documents/Academic Programs/7CR/12-l/horgan.pdf.

INTRODUCTION

The principle of federalism is enshrined in the United States governmental framework. Federalism embraces the idea that both the federal government and state governments are sovereigns. When two separate sovereigns exist, it follows that conflict between the laws of each may arise. As such, the Supremacy Clause of Article VI of the United States Constitution gives Congress the authority to preempt state law. The drafters mandated:

---

* J.D. Candidate, Litigation and Alternative Dispute Resolution Candidate, May 2017, Chicago-Kent College of Law, Illinois Institute of Technology.


2 Id.

3 Id.

4 U.S. CONST. art. VI, cl. 2; California v. ARC Am. Corp., 490 U.S. 93, 100 (1989).
This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.  

The practical function underlying the preemption doctrine is that the Supremacy Clause invalidates state laws that interfere with or are contrary to federal laws enacted by Congress, particularly where Congress has expressed its intent to occupy an entire field of law.  

Foreign relations and international affairs, including refugee resettlement, are fields in which the Constitution and Congress have specifically intended the national government to occupy.  

Therefore,  

[W]here the federal government, in the exercise of its superior authority in these field[s], has enacted a complete scheme of regulation and has therein provided a standard for the registration of aliens, states cannot, inconsistently with the purpose of Congress, conflict or interfere with, curtail or complement, the federal law, or enforce additional or auxiliary regulations.  

Part II of this article will address the basic principles of the preemption doctrine that were present, somewhat discussed, but not adequately analyzed, in the Seventh Circuit Court of Appeal’s decision, Exodus Refugee Immigration, Inc. v. Pence. That Part will  

---

5 U.S. CONST. art. VI, cl. 2.  
9 838 F.3d 902 (7th Cir. 2016).
explain conflict and field preemption doctrines and their place in matters involving foreign relations and international affairs.

Part III of this article will discuss the Refugee Act of 1980, a comprehensive regulatory scheme enacted by Congress to establish a detailed framework for refugee resettlement in the United States. That Part will further discuss the ways in which Congress divided power related to refugee resettlement among the Executive Branch, federal agencies and even the states. As follows, Part IV will discuss the implementation of the Act and provide background on the stringent, comprehensive resettlement procedures, facilitated by federal agencies.

Part V of this article will address the Seventh Circuit’s decision in Exodus Refugee Immigration, Inc. v. Pence in which the court correctly upheld the district court’s decision to grant Exodus Refugee Immigration, Inc.’s preliminary injunction against former Governor and current Vice President Mike Pence. But while the Seventh Circuit ultimately reached the correct conclusion, that Part argues that the court’s preemption analysis was inadequate. Part VI will then explain the ways in which Pence’s directive was preempted by federal law. That Part will explain the court’s missed opportunity to directly discuss the important preemption issues underlying the Refugee Act, including the ways in which Congress divided power under the Act. Had the Seventh Circuit more directly addressed the preemption doctrine in its decision, Congress may have been tipped off to the current, and very controversial, actions of President Trump’s administration related to refugee resettlement policy.

This article concludes with Part VII, which suggests that Congress should consider amending the Refugee Act to redistribute its current power balance, as the Refugee Act’s original, humanitarian purpose is being thwarted and replaced by unverified fear and discrimination.

THE PREEMPTION DOCTRINE ARTICULATED BY THE SUPREMACY CLAUSE

The preemption doctrine, flowing from the Supremacy Clause, nullifies state laws that conflict with, or are otherwise contrary to,
established federal law.\textsuperscript{10} There are four traditional ways in which preemption occurs: (1) express preemption, (2) implied preemption, (3) conflict preemption and (4) field preemption.\textsuperscript{11} This article will specifically analyze conflict preemption and field preemption in the context of refugee resettlement policy. Despite the differences between these traditional forms of preemption, the court’s “sole task is to ascertain the intent of Congress” when analyzing any form of preemption.\textsuperscript{12}

\textit{A. A State Law that Interferes with or is Contrary to Federal Law is Conflict Preempted}

A state law is preempted when it conflicts with federal law.\textsuperscript{13} A state law conflicts with federal law where “compliance with both federal and state regulations is a physical impossibility”\textsuperscript{14} . . . [and] where the challenged state law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress[].”\textsuperscript{15} If a state law is either inconsistent with or impairs the operation of federal law, “state law must yield[].”\textsuperscript{16}

In analyzing a claim of conflict preemption, a court may consider the relationship between the state and federal law both as they are written, and as they are applied.\textsuperscript{17} In line with broad concepts of federalism, courts should not assume that the state’s power is

\textsuperscript{10} U.S. CONST. art. VI, cl. 2.
\textsuperscript{14} Arizona, 132 S. Ct. at 2501 (citing Florida Lime & Avocado Growers, Inc., 373 U.S. at 142–43).
\textsuperscript{15} Hines, 312 U.S. at 67.
\textsuperscript{16} U.S. CONST. art. VI, cl. 2; Zschernig v. Miller, 389 U.S. 429, 440 (1968).
\textsuperscript{17} U.S. CONST. art. VI, cl. 2; Weber v. Heaney, 793 F.Supp. 1438, 1443 (D. Minn. 1992).
superseded unless that was the “clear and manifest purpose of Congress.”\textsuperscript{18} But the Supreme Court has also cautioned that “there can be no one crystal clear distinctly marked formula” to determine whether a state law conflicts with a federal law.\textsuperscript{19}

Rather, the court’s primary function is to make a fact-based determination consistent with the specific circumstances of each case.\textsuperscript{20} In considering whether a state law conflicts with federal law, courts look to whether state law is “conflicting; contrary to; occupying the field; repugnant[t]; different[t]; irreconcilab[le]; inconsistent[t]; [in] violation; [in] curtailment; and [in] interference” with established federal law.\textsuperscript{21}

To determine whether an obstacle exists sufficient to nullify a state law, the court uses its judgment, which is informed by “examining the federal statute as a whole and identifying its purpose and intended effects.”\textsuperscript{22} If the state law is contrary to the federal law’s purpose and intended effects, as gleaned from the text, structure and history of the federal law, the state law is invalid and must yield.\textsuperscript{23}

\textit{B. A State Law that Interferes with an Area of Law Exclusively Occupied by the Federal Government is Field Preempted}

Aside from conflict preemption, a state directive, or other law, is preempted where federal law “so thoroughly occupies a legislative field” that one may reasonably infer that Congress left no room for the states to supplement it.\textsuperscript{24} “[T]he States are precluded from regulating conduct in a field that Congress, acting within its proper authority, has determined must be regulated by its exclusive governance.”\textsuperscript{25}

\textsuperscript{18} Arizona, 132 S. Ct. at 2501 (citing Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 240 (1947)).
\textsuperscript{19} Hines, 312 U.S. at 67.
\textsuperscript{20} See id.
\textsuperscript{21} Id.
\textsuperscript{23} See Arizona, 132 S. Ct. at 2496.
\textsuperscript{24} U.S. CONST. art. VI, cl. 2.
\textsuperscript{25} Arizona, 132 S. Ct. at 2501.
A court may infer Congressional intent to preempt state law in a particular legal arena in two relevant ways. First, Congress intended to preempt state law if it enacted a regulatory scheme that is so all encompassing of a certain area. Second, Congress intended to preempt state law if the federal interest in the regulated area is so dominant to state interests that there is simply no room for additional state action.

To determine whether a federal regulatory scheme is so sweeping of an entire area so as to preempt state laws that impermissibly touch on that area, the court’s focus is wholly centered on Congress’s intent underlying the regulatory scheme. Courts analyze the “depth and breadth” of the scheme. Then, they determine whether the state law would frustrate that federal scheme. If the state law would frustrate the federal regulatory scheme, it is invalid as preempted.

Further, a state law is field preempted if the federal interest at stake in the regulated area overrides state interests that may be at play, leaving no room for state action. The importance to the state of its own law is immaterial to field preemption analysis. Thus, if the federal interest is so dominant that no room exists for state action, the state law is void and field preempted.

As the preemption doctrine has existed since the nation’s founding, there is extensive case law on the subject. The United States Supreme Court has addressed conflict and field preemption on numerous occasions, in particular, as the doctrine operates in relation to the fields of foreign relations and international affairs, as discussed in the following section.

27 U.S. CONST. art. VI, cl. 2; S. Union Gas Co., 306 F. Supp. 2d at 133.
28 U.S. CONST. art. VI, cl. 2; S. Union Gas Co., 306 F. Supp. 2d at 133.
32 U.S. CONST. art. VI, cl. 2; S. Union Gas Co., 306 F. Supp. 2d at 133.
34 U.S. CONST. art. VI, cl. 2; S. Union Gas Co., 306 F. Supp. 2d at 133.
C. United States Supreme Court Jurisprudence Supports the Proposition that State Laws Are Conflict or Field Preempted if the Law Impermissibly Interferes with Federal Law in the Areas of Foreign Relations and International Affairs

1. Conflict Preemption

In American Insurance Association v. Garamendi, the Court held that California’s passage of the Holocaust Victim Insurance Relief Act of 1999 (“HVIRA”) interfered with and acted as an obstacle to the federal government’s established policy for resolving Holocaust-era insurance claims; therefore, the Court invalidated the California law as preempted.\(^5\) In that case, California enacted HVIRA, which required all insurance companies doing business within the state to publicly disclose all policies sold to people in Europe between 1920 and 1945, including all policy owner names and the status of each policy.\(^6\) The purpose of HVIRA was to facilitate and resolve Holocaust-era insurance claims by California residents.\(^7\) If that information was not disclosed, HVIRA mandated regulatory sanctions.\(^8\)

Consequently, the plaintiffs, a trade organization and other American and European insurance companies, filed suit against the state, arguing, in part, that HVIRA was conflict preempted.\(^9\) Specifically, the plaintiffs asserted that HVIRA’s mandatory regulatory sanctions for nondisclosure interfered with the policies adopted by the federal government and established by President Clinton in negotiating postwar settlement agreements with Germany, Austria and France.\(^10\) In particular, the agreements negotiated by the President encouraged those governments to volunteer settlement

\(^6\) Id. at 409–10.
\(^7\) Id. at 410–11.
\(^8\) Id. at 423.
\(^9\) Id. at 412.
\(^10\) Id. at 422–23.
funds, rather than proceed to litigation or mandated sanctions.\textsuperscript{41} Therefore, the plaintiffs argued, HVIRA directly interfered with policies established by the President and was preempted.\textsuperscript{42}

The Court agreed.\textsuperscript{43} The Court explained that the President expressly established the federal government’s stance on this issue in the negotiated agreements, amongst other public statements.\textsuperscript{44} But, HVIRA took a much tougher position, which directly conflicted with established federal policy.\textsuperscript{45} Therefore, because California sought “to use an iron fist where the President had consistently chosen kid gloves[,]” the Court held that HVIRA was conflict preempted.\textsuperscript{46}

The Supreme Court most recently addressed the preemption doctrine in its landmark decision, Arizona v. United States. In Arizona, the Court held that sections 5(c) and 6 of Arizona’s Support Our Law Enforcement and Safe Neighborhoods Act, S.B. 1070, were conflict preempted because both sections stood as obstacles to established federal regulations.\textsuperscript{47} There, Arizona essentially enacted its own immigration enforcement policy to ‘discourage and deter the unlawful entry and presence of aliens and economic activity by persons unlawfully present in the United States.’\textsuperscript{48} Specifically, section 5(c) of S.B. 1070 created a new state offense, making it a misdemeanor for an unauthorized alien to seek or engage in work in Arizona.\textsuperscript{49} Section 6 of S.B. 1070 gave state officers authority to arrest, without a warrant, a person “‘the officer had probable cause to believe . . .

\begin{itemize}
\item \textsuperscript{41} \textit{Id.} at 421.
\item \textsuperscript{42} \textit{Id.} at 413.
\item \textsuperscript{43} \textit{Id.} at 427.
\item \textsuperscript{44} \textit{Id.} at 421–23.
\item \textsuperscript{45} \textit{Id.} at 423–24.
\item \textsuperscript{46} \textit{Id.} at 427.
\item \textsuperscript{47} Arizona v. United States, 132 S. Ct. 2492, 2501 (2012).
\item \textsuperscript{48} \textit{Id.} at 2497 (citing Note following \textit{Ariz. Rev. Stat. Ann.} § 11–1051 (2012)).
\item \textsuperscript{49} \textit{Id.} at 2497 (citing \textit{Ariz. Rev. Stat. Ann.} § 13–2928(C) (2010)).
\end{itemize}
ha[d] committed any public offense that ma[de] the person removable from the United States. ”

The federal government asserted that section 5(c) created an obstacle to the federal government’s regulation and control of unauthorized employment of illegal aliens. In enacting the Immigration Reform and Control Act of 1986 (“IRCA”), Congress “made a deliberate choice” not to impose criminal penalties on illegal aliens who were not authorized to work in the country. However, section 5(c) imposed criminal penalties on such persons. Consequently, the Court determined that section 5(c) was contrary to and conflicted with IRCA. Thus, the section was conflict preempted, as it created an obstacle to the federal government’s enforcement of its chosen regulatory scheme.

Moreover, the federal government argued that section 6 of S.B. 1070 was also conflict preempted by the illegal alien removal system enacted by Congress. Congress created federal regulations that denote the situations in which trained federal immigration officers may arrest illegal aliens during the removal process. In addition, Congress articulated circumstances in which state officials are to “cooperate” with the federal government in such arrest and removal.

Nonetheless, section 6 provided state officers with even more authority to arrest illegal aliens on the basis of possible removability than Congress entrusted to its trained officers, in contravention of established federal policies. Therefore, the Court held that section 6 was conflict preempted because it created an obstacle to Congress’s

---

51 Arizona, 132 S. Ct. at 2503.
52 Id. at 2504.
53 Id.
54 Id. at 2505.
55 Id.
56 Id. at 2505.
57 Id. at 2505–06.
58 Id. at 2506.
59 Id.
established protocol for the arrest of aliens based on potential removability.\textsuperscript{60}

2. Field Preemption

In \emph{Hines v. Davidowitz}, the Court held that a Pennsylvania law, regulating immigration, naturalization and deportation, was field preempted, as Congress intended for the federal government to occupy the entire field of immigration regulation.\textsuperscript{61} In 1939, Pennsylvania passed the Alien Registration Act ("the state Act"), which required every alien over 18 years old to register once each year, provide any requested information, pay an annual registration fee and receive an alien identification card.\textsuperscript{62} In addition, the state Act required aliens to carry the identification card at all times, showing the card whenever demanded by law enforcement.\textsuperscript{63} Failure to register resulted in a fine and potential imprisonment.\textsuperscript{64} Failure to carry or show the identification card also resulted in a fine and possible imprisonment.\textsuperscript{65}

But, one year after the state Act’s passage, Congress enacted the federal Alien Registration Act ("the federal Act"), which differed from the state Act.\textsuperscript{66} The federal Act also contained certain registration requirements, but did not require aliens to carry an identification card or show any form of identification to law enforcement officers.\textsuperscript{67} Finally, the federal Act only criminally sanctioned the willful failure to register.\textsuperscript{68}

Subsequently, Bernard Davidowitz, and other Pennsylvania residents, citizens and taxpayers, filed an injunction against enforcement of the state Act, arguing, in part, that the state Act was field preempted by federal law because the power to restrict, limit,
regulate and register aliens is a field that the federal government entirely occupies.\textsuperscript{69} The Court agreed.\textsuperscript{70} The Court explained the importance of advancing “collective interests” and approaching foreign nations as “one people, one nation, one power.”\textsuperscript{71} Harkening back to the Federalist Papers and the Constitution, the Court recognized the longstanding principle of federalism, that the national government has supreme power in the field of foreign affairs, including immigration, naturalization and deportation.\textsuperscript{72} Therefore, in analyzing the federal Act, the Court determined that Congress, with its superior authority, enacted the federal Act with the purpose of providing a complete regulatory system in this area.\textsuperscript{73} Thus, the state Act was field preempted, as it interfered with the federal government’s exclusive occupation of the field of immigration regulation.\textsuperscript{74}

Further, in \textit{Crosby v. National Foreign Trade Council}, the Court held that a Massachusetts statute interfered with the federal government’s occupation over the field of foreign relations, specifically its ability to impose sanctions on Burma.\textsuperscript{75} Therefore, the Court struck down the Massachusetts statute as field preempted.\textsuperscript{76} In that case, Massachusetts passed the Massachusetts Burma Law, which barred state entities from buying goods and services from any person doing business with Burma that was placed on a “restricted purchase list.”\textsuperscript{77} The Law broadly defined “doing business with Burma” and only allowed for three narrow exceptions to its ban.\textsuperscript{78}

Three months after Massachusetts passed its Burma Law, Congress enacted a statute related to United States relations with Burma.\textsuperscript{79} First, the federal statute imposed mandatory and conditional

\textsuperscript{69} Id. at 61.
\textsuperscript{70} Id. at 68–69.
\textsuperscript{71} Id. at 63; Chae Chan Ping v. United States, 130 U.S. 581, 606 (1889).
\textsuperscript{72} \textit{Hines}, 312 U.S. at 62–63.
\textsuperscript{73} Id. at 73–74.
\textsuperscript{74} Id.
\textsuperscript{76} Id.
\textsuperscript{77} Id. at 367.
\textsuperscript{78} Id. at 367–68.
\textsuperscript{79} Id. at 368.
sanctions on Burma. Second, the federal statute delegated power to the
President to develop a comprehensive strategy to improve human
rights practices in Burma. Third, the federal statute required the
President to report to Congress on the development of his strategies.
Fourth, the federal statute gave the President authority to waive
sanctions under circumstances in which the imposition of sanctions
would be contrary to American national security interests.

Subsequently, the National Foreign Trade Council, a nonprofit
corporation whose clients engaged in foreign commerce, sought
declaratory and injunctive relief against Massachusetts state officials,
arguing, in part, that the state statute was field preempted by the
federal government’s foreign affairs power. The Court recognized
that Congress clearly intended to confer great power to the Executive
in passing the federal regulation, which placed power over the
imposition of sanctions on Burma directly in the President’s hands.
The Court explained that it was implausible that Congress would so
clearly define the President’s broad sanction power if it was willing to
hinder his effectiveness by allowing a state statute to lessen the
consequences of the President’s action, which “is just what the
Massachusetts Burma law would do in imposing a different, state
system of economic pressure against the Burmese political regime.”
Therefore, the Court held that the Massachusetts Burma Law was field
preempted.

The case law, discussed infra Part II(C)(1) and (2), reflects a well-
established understanding that when state law interferes with federal
law related to foreign relations and international affairs, federal law
will prevail and preempt the conflicting state law. With these
principles in mind, this article turns to the Refugee Act of 1980 and its

80 Id. at 368–69.
81 Id. at 368.
82 Id. at 369.
83 Id.
84 Id. at 371.
85 Id. at 374–76.
86 Id. at 376.
87 Id. at 373–74.
distribution of power over refugee resettlement between the federal government and state government.

THE REFUGEE ACT OF 1980 AND ITS DISTRIBUTION OF POWER

In 1980, Congress took control of the United States’ unevenly implemented and confusing refugee resettlement policy by enacting the Refugee Act of 1980 (the “Act”), which amended the Immigration and Nationality Act of 1952. Congress specifically enacted the Act to create an organized, permanent process to resettle refugees. The stated purpose for the legislation was to welcome refugees and reflect the United States’ “commitment to human rights and humanitarian concerns.”

In establishing the process, Congress adopted the internationally recognized definition of a “refugee.” The Act defines a refugee as:

[A]ny person who is outside any country of such person’s nationality or, in the case of a person having no nationality, is outside any country in which such person last habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.

---

The Act confers power to oversee the resettlement program as a whole to the Executive Branch. The Act provides that the President shall determine the number of refugees who may be admitted to the United States before the beginning of each fiscal year and after appropriate consultation with Congress based on that which is “justified by humanitarian concerns or is otherwise in the national interest.” The President has total discretion to change that number if unforeseen circumstances arise.

After the President consults with Congress, the President issues a Presidential Determination, which authorizes that number of refugees to resettle in the United States. The President’s annual determination considers the country’s foreign policy goals, family reunification, domestic immigration objectives, pressure from private special interest groups and humanitarian concerns. However, the President’s determination also undeniably hinges on the current political and social happenings around the world.

While the President is the ultimate authority over the refugee resettlement program, federal agencies are responsible for facilitating the actual resettlement process. Congress specifically defined the role of the federal government and its agencies in determining which refugees would be resettled in the United States and how that process would proceed. Even before going through the stringent vetting procedures used to resettle refugees in the country, an applicant for refugee resettlement must establish that: (1) they are a refugee within the definition of the Act; (2) they are coming from a region or country of special humanitarian concern; (3) they have not become firmly

---

93 8 U.S.C. § 1157(a)(2); Lunn, supra note 91, at 842.
95 Id. at § 1157(b); Lunn, supra note 91, at 842.
97 Lunn, supra note 91, at 837–38.
98 Id.
99 Id. at 842.
100 8 U.S.C. § 1522.
101 See infra Part IV.
resettled in any foreign country; and (4) they are admissible as
immigrants under the Act.\textsuperscript{102}

In the same vein, Congress defined the role of the States in the
refugee resettlement process.\textsuperscript{103} Congress identified ways in which a
state may elect to participate in the federal refugee resettlement
program.\textsuperscript{104} To participate, a state must submit a plan to the Director
of the Office of Refugee Resettlement (ORR), detailing the state’s
procedures for facilitating refugees placed within the state by the
federal government.\textsuperscript{105} Once approved, the state receives grants
directly from the federal government to provide various assistance to
refugees within the state.\textsuperscript{106} Further, a participating state receives grant
money from the federal government that is passed on to local
resettlement agencies to reimburse those agencies for monies
expended on refugee assistance and assimilation services.\textsuperscript{107} The State
of Indiana elected to participate in the program when it submitted and
had approved its plan.\textsuperscript{108}

No state is required to participate in the federal refugee
resettlement program.\textsuperscript{109} Rather, where a state does not submit or have
a plan approved by the Director, the Wilson-Fish Program may be
instituted.\textsuperscript{110} The Wilson-Fish Program is “an alternative to traditional
state-administered refugee assistance programs,”\textsuperscript{111} in which the
federal government directly distributes grants to local resettlement

\begin{itemize}
  \item \textsuperscript{102} Lunn, \textit{supra} note 91, at 837–38.
  \item \textsuperscript{103} 8 U.S.C. § 1522(a)(2)(A).
  \item \textsuperscript{104} \textit{Id.} at § 1522(a)(6).
  \item \textsuperscript{105} \textit{Id.}
  \item \textsuperscript{106} \textit{Id.} at § 1522(a)(4)(B).
  \item \textsuperscript{107} \textit{Id.} at § 1522(c).
  \item \textsuperscript{108} Brief of Plaintiff-Appellee at 1, Exodus Refugee Immigration, Inc. v.
Pence, 838 F.3d 902 (7th Cir. 2016) (No. 16-1509); \textit{see infra} Part V.
  \item \textsuperscript{109} 8 U.S.C. § 1522(a)(6).
  \item \textsuperscript{110} \textit{Id.} at § 1522(c)(7); 45 C.F.R. § 400.69.
  \item \textsuperscript{111} 89 NO. 33 Interpreter Releases 1645, 1646 n.39.
\end{itemize}
agencies, rather than distributing the funds through the non-participating state. 112

In defining the ways in which a state may or may not participate in the federal refugee resettlement program, Congress specifically described the state’s role as “consultative.” The Act states: “The Director, together with the Coordinator, shall consult regularly with State and local governments and private nonprofit voluntary agencies concerning the sponsorship process and the intended distribution of refugees among the States and localities.” 113 Thus, as is clearly stated, Congress delegated only a consultative role to states that participate in the program. 114

Congress’s intent in assigning such a role to the States was made even clearer by the 1982 Senate Report addressing the Act and its implementation at that time. 115 Soon after passage of the Act, State and local government officials criticized the federal government’s failure to consult them about refugee placement decisions. 116 While the Report acknowledged the shortcomings of communications at that time, the Report referred to meetings between state and federal government officials merely as a “free exchange of views.” 117 The Report made clear, once again, that the state was to consult, not make decisions about the program and its implementation.

---

112 8 U.S.C. § 1522(e)(7); Brief for American Jewish Committee as Amicus Curiae Supporting Appellees at 7, Exodus Refugee Immigration, Inc. v. Pence, 838 F.3d 902 (7th Cir. 2016) (No. 16-1509).
114 Id.; Brief for American Jewish Committee, supra note 112, at 19.
116 Id.
117 Id.
Refugees seeking entry to the United States undergo a scrutinizing vetting process prior to entry. Federal agencies exclusively facilitate this process. The United States’ process and vetting procedures are divided into seven steps: registration and data collection, initial security checks, Department of Homeland Security (DHS) interview, biometric security check, cultural orientation and medical check, assignment to domestic resettlement locations and travel to the United States.

First, the United Nations High Commissioner for Refugees (UNHCR) collects applications for resettlement and other initial documentation. Then, the UNHCR refers refugees in need of protection to the United States and other countries. Refugee information of those referred to the United States is then transferred to a Resettlement Support Center (RSC), a division of the State Department. The RSC conducts in-depth interviews of each applicant, and the refugee’s information is entered into the State Department’s Worldwide Refugee Admission Processing System (WRAPS), which cross-references and verifies all information received throughout the application process. Thereafter, all applicant information is sent to other federal agencies for background checks.

---

120 THE REFUGEE PROCESSING AND SCREENING SYSTEM, supra note 118, at 1–7.
121 Id. at 1.
122 Id.
123 Id.
124 Id.
125 Id.
Second, the refugee applicant goes through initial security checks by United States national security agencies, including the National Counterterrorism Center, Federal Bureau of Investigation (FBI), DHS, Department of Defense (DOD), State Department and the intelligence community. Those agencies receive background information from an RSC and screen applicants for security threats.

Third, those results are sent to the DHS and State Department. Subsequently, DHS officers trained in refugee vetting review the screening results and conduct in-person interviews of refugees that may be resettled in the United States. DHS officers collect biometric data, confirm prior information collection, enter new information into WRAPS and conduct ongoing security checks based on any additional information collected throughout the process. After the DHS officer completes all interviews and security checks, the DHS decides whether the refugee’s application process will continue.

Fourth, refugee applicants are fingerprinted, and their fingerprints are screened against several federal agency databases, including FBI, DHS, and DOD databases. Fifth, refugee applicants complete a cultural orientation designed to teach refugees American culture and customs. At this stage, refugee applicants must also undergo medical screenings to ensure that they do not transmit any suspect diseases into the country.

Sixth, the RSC sends refugee applicant information to one of nine United States resettlement agencies to review and determine where each refugee is going to be resettled within the United States. Once placement is determined, the refugee applicant is notified and the

126 Id. at 2.
127 Id.
128 Id. at 3.
129 Id.
130 Id. at 3–4.
131 Id. at 3.
132 Id. at 4.
133 Id. at 5.
134 Id.
135 Id. at 6.
International Organization for Migration coordinates refugee travel accommodations. Still, prior to entry to the United States, refugees undergo Customs and Border Protection and Transportation Security Administration screening. Seventh, and lastly, refugees arrive in the United States and are welcomed by representatives of a resettlement agency.

Each of those nine resettlement agencies continue to provide various services to newly arrived refugees, and the agencies partner with local nonprofit refugee resettlement organizations that aid in the assimilation effort. Exodus Refugee Immigration, Inc. ("Exodus") is just one local refugee resettlement agency that participates in refugee resettlement work.

Clearly, Congress has established the most careful screening processes that refugees must undergo prior to resettlement in the United States. And even aside from the federal agencies already mentioned, other federal agencies have “broad responsibilities for separate functions and services” related to refugee resettlement in the United States. For instance, the Department of Health and Human Services handles employment and social services concerns related to refugee resettlement. Moreover, the Immigration and Naturalization Service is responsible for issues related to legal status, conferral of

---

136 Id.
137 Id.
138 Id. at 7; Voluntary Agencies, OFFICE OF REFUGEE RESettlement (July 17, 2012), https://www.acf.hhs.gov/orr/resource/voluntary-agencies (naming as the nine not for profit resettlement agencies: Church World Service, Ethiopian Community Development Council, Episcopal Migration Ministries, Hebrew Immigrant Aid Society, International Rescue Committee, US Committee for Refugees and Immigrants, Lutheran Immigration and Refugee Services, Unites States Conference of Catholic Bishops and World Relief Corporation).
141 Fredriksson, supra note 119, at 758–59.
142 Id.
citizenship and immigration benefits. In addition, the Department of Labor concentrates on labor migration issues related to refugee resettlement. The list goes on and on. But, if one thing is certain, it is that Congress has created a system for refugee resettlement entirely controlled and facilitated by the federal government, as it is a matter of foreign affairs and international relations.

**EXODUS REFUGEE IMMIGRATION, INC. v. PENCE**

**A. Factual Background**

On November 16, 2015, former Governor of Indiana and current Vice President Mike Pence issued a state directive, mandating all state agencies to suspend resettlement of Syrian refugees. Pence stated:

In the wake of the horrific attacks in Paris, effective immediately, I am directing all state agencies to suspend the resettlement of additional Syrian refugees in the state of Indiana pending assurances from the federal government that proper security measures have been achieved. Indiana has a long tradition of opening our arms and homes to refugees from around the world but, as governor, my first responsibility is to ensure the safety and security of all Hoosiers. Unless and until the state of Indiana receives assurances that proper security measures are in place, this policy will remain in full force and effect.

---

143 Id.
144 Id.
145 Id. at 758.
146 Brief for American Jewish Committee, supra note 112, at 13; see also Zschernig v. Miller, 389 U.S. 429, 436 (1968).
Consequently, a family of Syrian refugees scheduled to arrive in Indiana that same day was diverted to settle in Connecticut.\footnote{148}{Id. at 52.} As a result of the Pence’s directive, state agencies refused to assist Syrian refugees resettle within the state.\footnote{149}{Brief for American Jewish Committee, supra note 112, at 13.} One such state agency was the Family and Social Services Administration, which is the Indiana agency that receives and disburses refugee resettlement monies from the federal government to nonprofit agencies under contract with the state.\footnote{150}{Memorandum in Support of Motion for Preliminary Injunction at Introduction, Exodus Refugee Immigration, Inc. v. Pence et al., No. 1:15-cv-1858-TWP-DKL (S.D. Ind. Dec. 2, 2015), 2015 WL 13091773.} As mentioned in Part III, \textit{infra}, Indiana elected to participate in the federal refugee resettlement program by submitting a state plan to the Director of the ORR.\footnote{151}{Brief of Plaintiff-Appellee, supra note 108, at 1.} Indiana’s plan was approved, as it complied with the Act’s requirements.\footnote{152}{Id.; 8 U.S.C. § 1522(a)(6)(A)(B) (providing state plan requirements for approval).} As such, the state received grants from the federal government to spend on refugee assistance in accordance with its plan.\footnote{153}{Id. at 12.} Even further, under its plan, the state received grant money from the federal government to disburse to local resettlement agencies that it contracted with to provide assistance to newly arrived refugees.\footnote{154}{Id.} Exodus is one of three local resettlement agencies under contract with the state.\footnote{155}{Id. at 12.} Consequently, under Pence’s directive, Exodus was not reimbursed by the state for monies spent on its resettlement efforts.\footnote{156}{Id.} However, Exodus continued to receive assignments from the federal government to resettle Syrian refugees within the state.\footnote{157}{Brief for American Jewish Committee, supra note 112, at 13.} Thus, Exodus continued to expend money, time and other resources to resettle the incoming Syrian refugees.\footnote{158}{Id.} Yet, it was
also forced to expend additional money, time and resources to make up for the funds cut off by state following Pence’s directive.\textsuperscript{159}

Consequently, on November 23, 2015, Exodus filed a Complaint for Declaratory and Injunctive Relief against Mike Pence, in his official capacity as Governor of the State of Indiana, and John Wernert, M.D., in his official capacity as the Secretary of the Indiana Family and Social Services Administration.\textsuperscript{160} Exodus’s Complaint alleged that it was entitled to injunctive relief.\textsuperscript{161} In particular, Exodus argued that the denial of constitutional rights was irreparable harm by itself.\textsuperscript{162} In the alternative, it argued that Pence’s actions caused Exodus irreparable harm by impeding its ability to serve the Syrian refugee community.\textsuperscript{163} Further, Exodus’s harm was significant in comparison to the state’s harm in disbursing federal funds it was not entitled to withhold, and therefore, the balance of harms weighed in Exodus’s favor.\textsuperscript{164} Finally, the public interest would be served by defending against violations of the Constitution, federal law and immigration policy.\textsuperscript{165} The district court agreed, and granted Exodus’s motion for preliminary injunction.\textsuperscript{166}

\textsuperscript{159} Id.
\textsuperscript{161} Memorandum in Support of Motion for Preliminary Injunction, \textit{supra} note 150, at Introduction.
\textsuperscript{162} Id. at Part II(A) (referencing Overstreet v. Lexington-Fayette Urban County Gov't, 305 F.3d 566, 578 (6th Cir. 2002)).
\textsuperscript{163} Memorandum in Support of Motion for Preliminary Injunction, \textit{supra} note 150, at Part II(A).
\textsuperscript{164} Id. at Part II(B).
\textsuperscript{165} Id. at Part II(C).
B. The Seventh Circuit’s Decision

Accordingly, Pence appealed the district court’s decision to the Seventh Circuit Court of Appeals.167 The Seventh Circuit affirmed the district court’s decision.168 However, the Seventh Circuit’s analysis only directly concentrated on the Equal Protection Clause and Title VI arguments, despite the overwhelmingly important preemption issues present in the matter. In so limiting its analysis, the court missed important opportunities to delve into timely concepts of federalism, to clarify, or remind, important state and federal actors of their respective roles in this complex regulatory scheme, and to foreshadow for Congress the policies instituted by the Trump administration.

The Seventh Circuit’s opinion begins with an acknowledgment that the “regulation of immigration to the United States, including by refugees . . . is a federal responsibility codified in the Immigration and Nationality Act, 8 U.S.C. §§ 1101 et seq.”169 Further, the opinion alludes to the state’s role as a consultant to the federal government with regard to the federal refugee resettlement program.170 Yet, these are the only instances in which the court somewhat directly recognized the significant preemption issues at play in the case. Instead, the court’s short opinion focused more on the factual circumstances of the matter, the refugee vetting and resettlement process and on an Equal Protection and Title VI analysis.

With regard to the Equal Protection and Title VI claims, Pence contended that the directive did not announce a policy of excluding Syrian refugees from the State of Indiana on the basis of their national origin; rather, Pence asserted the policy was based on the threat Syrian refugees pose to the safety of Indiana residents.171 The Court rightfully mocked this argument and explained that the policy instituted by the

---

167 Brief of Defendant-Appellant at 1, Exodus Refugee Immigration, Inc. v. Pence, 838 F.3d 902 (7th Cir. 2016) (No. 16-1509).
168 Exodus Refugee Immigration, Inc. v. Pence, 838 F.3d 902, 905 (7th Cir. 2016).
169 Id. at 903.
170 Id. at 904.
171 Id.
directive discriminated against Syrian refugees because they are Syrian.\(^{172}\)

Consequently, though, the court applied strict scrutiny, as it found the directive discriminated against Syrian refugees on the basis of national origin, and analyzed whether Pence’s directive was narrowly tailored to achieve a compelling government interest.\(^{173}\) Pence asserted that Indiana had a compelling interest in “protecting its residents from the well-documented threat of terrorists posing as refugees to gain entry into Western Countries.”\(^{174}\) The court rightfully, again, expressed its confusion and disagreement with this argument.\(^{175}\) It explained that neither Pence nor public sources provided evidence of such a threat even existing.\(^{176}\) Thus, the court determined that the asserted state interest was not compelling or narrowly tailored.\(^{177}\) Because Pence’s directive failed on both Equal Protection and Title VI grounds, the court affirmed the lower court’s decision.\(^{178}\)

Notwithstanding the fact that the court’s reasoning and ultimate conclusion were correct, the court’s opinion was simply incomplete. The court cited to the Act’s implementation provision, which bars participating states from aiding refugees on the basis of, among other things, national origin.\(^{179}\) But, the court never directly stated that the directive was conflict preempted on that basis, failing to address head on the critical preemption issues at stake. Specifically, the court missed the vital opportunity to address the ways in which Pence’s directive was both conflict preempted by established federal law and field preempted by the federal government’s exclusive occupation over foreign relations and international affairs. Had the court more directly analyzed the preemption doctrine in conjunction with the Act, Congress might have had notice of its opportunity to reconsider the

\(^{172}\) Id.
\(^{173}\) Id.
\(^{174}\) Id.
\(^{175}\) Id.
\(^{176}\) Id.
\(^{177}\) Id.
\(^{178}\) Id. at 905.
\(^{179}\) 8 U.S.C. § 1522(a)(5).
way in which power is distributed among the states and throughout the federal government under the Act.

**Pence’s Directive was Conflict and Field Preempted by Federal Law**

A. *Pence’s Directive was Conflict Preempted*

Pence’s directive conflicted with federal law and was therefore preempted. First, Pence’s directive discriminated against refugees on the basis of nationality in conflict with the Act and its implementation regulations. The Act specifically states that “[a]ssistance and services funded under this section shall be provided to refugees without regard to race, religion, nationality, sex, or political opinion.” Moreover, the Act mandates that participating states implement approved plans in the same manner – “without regard to race, religion, nationality, sex, or political opinion.”

Pence’s directive directly violated these portions of the Act. Pence’s directive outright withheld federal funds based on nationality. As recognized by the Seventh Circuit’s opinion, refugees entering the United States from Syria are considered Syrian nationals. Therefore, by refusing to disburse federal funding to Exodus for its efforts to resettle Syrian refugees, Pence’s directive conflicted with both provisions of the Act.

Second, Pence’s directive implemented its own screening procedures based on unverified security threats in conflict with the national government’s vetting procedures. Pence’s directive is analogous to the state laws in *Garamendi* and *Arizona*, as the directive implemented its own vetting procedures that interfered with established federal policy. As noted, and derided by the Seventh Circuit, Pence failed to cite any evidence suggesting that Syrian

---

180 Brief for American Jewish Committee *supra* note 112, at 14.
182 45 C.F.R. § 400.5(g).
183 *Exodus Refugee Immigration, Inc.*, 838 F.3d at 903.
184 Brief for American Jewish Committee, *supra* note 112, at 17.
refugees posed a security threat to the residents of Indiana. In fact, available evidence suggested otherwise. The former United States Secretaries of Homeland Security, former Commissioner of the United States Immigration and Naturalization Service and former United States Ambassador to Afghanistan, Pakistan, Iraq, Syria, Kuwait and Lebanon all attested to the country’s stringent vetting processes in light of concerns related to admission of Syrian refugees. As described in detail infra Part IV, the Act established scrutinizing procedures for refugee admission. Because Pence’s directive established a vetting procedure specific to Indiana, the directive conflicted with federal law.

Third, the directive conflicted with Congress’s conferral of power to the Executive Branch to determine the number of refugees, and in particular, Syrian refugees who may enter the country. As noted in Part III, infra, and whether proper or not, Congress conferred power to the Executive to determine the number of refugees that the country admits each fiscal year. The President’s determination is based on various considerations, but the number is meant to focus on humanitarian concerns and the national interest. As such, and in light of those concerns, President Obama determined that during fiscal year 2016, up to 85,000 refugees would be admitted to the United States with at least 10,000 of those admitted being Syrian refugees. Because Pence’s directive attempted to effectively block Syrian refugees from resettling in Indiana, it directly conflicted with the President’s authority under the Act.

Finally, the directive conflicted with the federal government’s placement of refugees within the State of Indiana and its process for determining refugee placement. As described in Part IV, infra, the federal government established procedures for determining where

---

185 Brief of Plaintiff-Appellee, supra note 108, at 8–9.
186 Brief for American Jewish Committee, supra note 112, at 18.
188 Id. at § 1157(a)(2)(B).
189 Brief of Plaintiff-Appellee, supra note 108, at 3.
190 Brief for American Jewish Committee, supra note 112, at 19.
arriving refugees were to be placed within the United States. While each participating state consults with the ORR to determine whether refugees should be placed within the state, no state has authority to make that decision on its own. Rather, the state may merely make recommendations to the ORR in consultative meetings. Therefore, Pence’s directive directly conflicted with the Act’s procedures because it had the effect of blocking Syrian refugees from being placed within the State of Indiana.

Because Pence’s directive conflicted with the Act in each of the aforementioned ways, it was conflict preempted by federal law. Nevertheless, regardless of conflict preemption analysis, Pence’s directive was preempted by the federal government’s exclusive occupation of foreign affairs and international relations, including refugee resettlement, as discussed in the next section.

B. Pence’s Directive was Field Preempted

Pence’s directive was also field preempted because it interfered with the federal government’s primary authority over foreign relations and international affairs. “[T]he supremacy of the national power in the general field of foreign affairs, including power over immigration . . . is made clear by the Constitution[,] was pointed out by authors of The Federalist in 1787, and has since been given continuous recognition by [the Supreme] Court.” Congress holds constitutional authority to regulate dealings with other nations in its war and foreign commerce power and the President has a “degree of independent authority to act” in foreign affairs.

As such, Congress used its authority to create a comprehensive regulatory scheme for refugee resettlement and conferred broad power
to the Executive to handle the federal refugee resettlement program.\textsuperscript{197} Certainly, the Act is a comprehensive regulatory scheme enacted by Congress with the purpose of regulating refugee policy across-the-board.\textsuperscript{198} In creating the Act, Congress demonstrated its intention – refugee resettlement is an area of foreign affairs in which the federal government is to exclusively occupy.\textsuperscript{199}

As noted by the Seventh Circuit, refugee resettlement policy falls squarely within the federal government’s purview over foreign affairs and international relations.\textsuperscript{200} In particular, Pence’s directive interfered with the federal government’s exclusive occupation of refugee resettlement policy because it undercut President Obama’s decision to admit at least 10,000 Syrian refugees during fiscal year 2016, as mention in Part VI(A) infra.\textsuperscript{201} In addition, Pence’s directive impermissibly interfered with the federal government’s creation of uniform laws to approach and develop relationships with foreign nations, in protection of American interests abroad.\textsuperscript{202}

Pence’s directive disrupted the uniformity of refugee resettlement policy.\textsuperscript{203} Power over foreign affairs and international relations, including refugee resettlement, was allocated to the federal government in the interest of creating uniform laws when dealing with foreign nations.\textsuperscript{204} “In our dealings with the outside world the United States speaks with one voice and acts as one, unembarrassed by the complications as to domestic issues which are inherent in the distribution of political power between the national government and the individual states.”\textsuperscript{205}

\textsuperscript{199} Exodus Refugee Immigration, Inc. v. Pence, 838 F.3d 902, 903 (7th Cir. 2016).
\textsuperscript{200} Id.
\textsuperscript{201} Brief of Plaintiff-Appellee, supra note 108, at 3.
\textsuperscript{202} Brief for American Jewish Committee, supra note 112, at 23.
\textsuperscript{203} Id.
\textsuperscript{204} Am. Ins. Ass'n v. Garamendi, 539 U.S. 396, 413 (2003).
\textsuperscript{205} United States v. Pink, 315 U.S. 203, 242 (1942).
Further, the federal government’s interests related to refugee resettlement override any state interest that may be at play; thus, there is no room for state action by Indiana or any other state.\textsuperscript{206} “One of the most important and delicate of all international relationships . . . has to do with the protection of the just rights of a country's own nationals when those nationals are in another country.”\textsuperscript{207} Past occurrences demonstrate that “international controversies of the gravest moment, sometimes even leading to war, may arise from real or imagined wrongs to another's subjects inflicted, or permitted, by a government.”\textsuperscript{208}

In deciding to admit up to 10,000 Syrian refugees in fiscal year 2016, President Obama was encouraging American allies to follow suit and aid the Syrian refugee effort.\textsuperscript{209} Pence’s directive disrupted that effort and impermissibly interfered with the nation’s ability to speak with “one voice”\textsuperscript{210} to foreign nations by instituting its own policy of ousting, rather than admitting, Syrian refugees. Therefore, Pence’s directive interfered with the federal government’s exclusive occupation of refugee resettlement policy and was preempted.

\textbf{CONGRESS SHOULD CONSIDER AMending THE REFUgee ACT IN LIGHT OF CURRENT POLITICAL CIRCUMSTANCES}

As discussed above, the federal government occupies the field of refugee resettlement for vital reasons related to the country’s foreign relations and international affairs. But, in light of that importance, Congress arguably divested too much power in the President alone.\textsuperscript{211} While Congress, numerous federal agencies and even the states are involved in the refugee resettlement program, the President has almost

\begin{flushright}
\textsuperscript{206} \textit{Id.} at 233; Zschernig v. Miller, 389 U.S. 429, 436 (1968).  
\textsuperscript{207} Hines v. Davidowitz, 312 U.S. 52, 64 (1941).  
\textsuperscript{208} \textit{Id.}  
\textsuperscript{209} Brief for American Jewish Committee, \textit{supra} note 112, at 24–26.  
\end{flushright}
unfettered discretion to determine the number of refugees admitted each fiscal year.\textsuperscript{212}

When the Act was initially created, humanitarian concern and national interests were the sole, important factors in determining the number of refugees admitted to the United States each fiscal year.\textsuperscript{213} However, now, unverified security concerns and religious bias are being masked as national interests, and have become the sole factors in determining the number of refugees admitted to the United States.\textsuperscript{214}

On January 27, 2017, just a week after his inauguration, President Trump issued an executive order, limiting the number of refugees to be admitted to the United States in fiscal year 2017 to less than 50,000.\textsuperscript{215} By way of context, during fiscal year 2016, 84,994 refugees were admitted to the United States.\textsuperscript{216} Even more alarming, and similar to Pence’s directive, President Trump issued two executive orders attempting to ban refugees from seven Muslim-majority countries, including Iran, Iraq, Libya, Somalia, Sudan, Syria and Yemen from resettling in the United States.\textsuperscript{217}

While an amendment to the Act would not totally retract the President’s constitutional authority over international affairs, the President’s power specifically over the arena of refugee resettlement would better defined and controlled, just like Congress’s conferral of power to the Executive in \textit{Crosby}. Even further, while an amendment to the Act may not have altered President Trump’s ability to issue the

\textsuperscript{213} Lunn, \textit{supra} note 91, at 838.
aforementioned executive orders, an amendment to the Act redistributing power over refugee resettlement would certainly alter the President’s ability to have the only and final say over refugee resettlement in the United States.\footnote{Washington v. Trump, 847 F.3d 1151, 1161 (9th Cir. 2017) (stating that the courts owe substantial deference to the President’s foreign relations determinations, but that it is the judiciary’s role to interpret the law, resolving any allegations that the President has acted unconstitutionally).} Pence’s directive and President Trump’s executive orders are just the beginning of an ever-growing problem. Therefore, Congress should consider amending the Act to ensure that the Act’s original purposes, humanitarian concern and actual national interests, are upheld. \footnote{Id. (stating that the President does \textit{not} have unreviewable authority to make decisions related to foreign relations) (emphasis added).}
WHO’S PINGING YOUR PHONE? EXPLORING THE
FOURTH AMENDMENT RAMIFICATIONS OF
STINGRAY DEVICES


KAREN VAYSMAN*

INTRODUCTION

In 2001, the Supreme Court in Kyllo v. United States profoundly declared that “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”¹ No less true is this statement today than when it was made, sixteen years ago, at a time when smartphones of the kind that exist today were unheard of to the Court. The modern smartphone device possesses unprecedented capabilities. With its massive storage capacity and ability to collect, all in one place distinct types of information, the phone can reconstruct an individual’s private life, all in the palm of a hand.²

Technological progress has a dual capability to decrease privacy, yet simultaneously augment the expectation of privacy. As cellphones become more sophisticated, so too does police surveillance. With

---


Stingrays and cell-site simulator devices, long gone are the days when law enforcement needed to heavily rely on a phone carrier company’s assistance for surveillance. Stingrays enable law enforcement to obtain directly, in real time (indeed, automatically), unique device identifiers and detailed location information of cellphones—data that it could not otherwise obtain without the assistance of phone companies. These devices can uncover more than just a phone’s location: they can eavesdrop on calls, block cell service, and intercept data transmitted and received by the phone, including, emails, text messages and web pages visited. This is just the tip of the iceberg.

While law enforcement may only seek to identify, or locate the target’s mobile device, “a Stingray will also, as a matter of course, collect data from many other mobile devices in the surrounding area.”

3 “Stingray” is the trade name for a cell-site simulator device manufactured by the Harris Corporation. A cell-site simulator goes by many different names, including, “Stingray,” “Triggerfish” and “Kingfish.” Cell-site simulators are also called International Mobile Subscriber Identity (“IMSI”) catchers, referring to the unique identifier or international subscriber identity of the wireless devices that they track. Howard W. Cox, Stingray Technology and Reasonable Expectations of Privacy in the Internet of Everything, 17 FEDERALIST SOC’Y REV. 29, 29 n.3 (2016); Ryan Gallagher, Meet the Machines That Steal Your Phone Data, ARS TECHNICA (Sept. 23, 2013, 12:00 PM), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/. This Note uses the term “Stingray” to refer generally to cell-site simulator devices.

4 Once the cell phones in the area send their signals to the cell-site simulator, the device captures a vast array of information, including, but not limited to, the cell phones’ IMSI or electronic serial number (“ESN”). *In re Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015); 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, 142–43 (2014).

5 Pell & Soghoian, *supra* note 4, at 142–43.


Regardless of whether law enforcement install the device in a vehicle, mount it on a drone, or carry it by hand on the street, the search is the same: it casts a wide net, receiving information from all cellphones within its range until the target phone is located. 8 These cellphones belong to people not suspected of any wrongdoing, wholly unconnected and unrelated to a search. Unfortunately, the high-volume collection of their information becomes collateral damage.

United States v. Patrick9 is the first time that constitutional questions posed by Stingrays reached a court of appeals, and the Seventh Circuit got the first word. In Patrick, police used a Stingray that pinpointed the defendant’s location for his arrest, and factual deficiencies in the record raised serious questions of whether their location tracking warrant authorized them to do so.10 The defendant then challenged the validity of his arrest and seizure of the gun that police found in his possession during his arrest based on the warrantless Stingray search.11 A divided panel found that the police’s use of the Stingray did not warrant application of the exclusionary rule.12 Judge Easterbrook, writing for the majority, explained the Stingray issues diverted from the meat and potatoes: police arrested the defendant on a public street, with probable cause to arrest and pursuant to an outstanding arrest warrant; this rendered the arrest and seizure of the gun incident to the arrest lawful.13 Chief Judge Wood disagreed, focusing her dissent not on where police found him, but

9 United States v. Patrick, 842 F.3d 540 (7th Cir. 2016).
10 Id. at 541–43.
11 Id. at 541.
12 Id. Judge Easterbrook, joined by Judge Kanne, affirmed the district court’s denial of the defendant’s motion to suppress and affirmed the defendant’s conviction. Id. at 540–45 (majority opinion). Chief Judge Wood dissented. Id. at 545–52 (Wood, C.J., dissenting).
13 Id. at 540–45 (majority opinion).
how.\textsuperscript{14} She argued the many factual holes regarding the Stingray and its use in the case precluded a meaningful resolution of whether the police violated the defendant’s Fourth Amendment rights.\textsuperscript{15} In light of \textit{Patrick} and the inevitable rapid advancements in technology, this Note tackles the inexhaustible question: to what extent will courts allow technology to limit the realm of guaranteed privacy?

This Note unfolds in five parts. Part I explains how Stingrays operate. Part II focuses on the Fourth Amendment jurisprudence and discusses the Supreme Court’s instructive cases governing what constitutes a “search or seizure,” that is “unreasonable,” the warrants requirements, and the exclusionary rule. Part III then examines the Court’s precedential Fourth Amendment case law pertaining to electronic surveillance and its recent decision on the exclusionary rule in \textit{Utah v. Strieff},\textsuperscript{16} all of which that the court in \textit{Patrick} heavily relied upon. Part IV then turns to \textit{Patrick} and reviews the factual background and main points raised by the majority and dissent. Part V argues three ways in which the Seventh Circuit’s decision chipped away at the realm of guaranteed privacy. Given the high stakes of Stingray searches, and in particular, the implications on third parties, this Note concludes with a discussion on the need for greater judicial oversight to strike an effective balance between the objectives of law enforcement and Fourth Amendment privacy rights.

\section*{I. What are Stingray Devices?}

Stingray technology, in some form or another, is more than 20 years old.\textsuperscript{17} Cell-site stimulators were initially developed and used by military and intelligence agencies, and they have since made their way

\textsuperscript{14} Id. at 552 (Wood, C.J., dissenting).

\textsuperscript{15} Id.


to state and local law enforcement agencies.\textsuperscript{18} The American Civil Liberties Union ("ACLU") reports that state and local police began to purchase these devices as early as 2002.\textsuperscript{19} The ACLU estimates that 72 agencies in 24 states and the District of Columbia own a Stingray-type device.\textsuperscript{20}

While a comprehensive analysis of Stingray technology lies beyond the scope of this Note, this Part briefly discusses the basics of Stingray devices and surveillance technology to illustrate the magnitude of the Stingray’s departure from traditional surveillance. Cellphones contain radio signal transmitters and receivers that connect to cellphone towers or “cell sites.”\textsuperscript{21} These cell sites are your typical raised structures with antennae that facilitate the transmission and receipt of electronic communication.\textsuperscript{22} Cellphones and cell sites communicate with one another by sending each other signals, and this back-and-forth communication enables the phone carrier to route calls, text messages and Internet data to and from a cellphone on networks like Sprint, Verizon, AT&T, etc.\textsuperscript{23} Cellphones also have unique digital identifiers, assigned by the device’s manufacturer or cellular network provider, which blast out to cell sites and allow networks to identify a

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{18}Id.
\item \textsuperscript{20}Federal agencies known to use cell site simulators: Federal Bureau of Investigation, Drug enforcement administration, U.S. secret service, Immigration and customs enforcement, U.S. Marshalls service, Bureau of Alcohol, Tobacco, Firearms, and explosives, international revenue service, U.S. army, U.S. Navy, U.S. Marine Corps, U.S. National Guard, U.S. Special Operations Command, and National security agency. Id.
\item \textsuperscript{21}For example, a cellphone displays “bars,” which represent the measurement of signal strength. Shane Dingman, Tracking our Phones: How Stingray devices are being used by police, THE GLOBE AND MAIL (Mar. 21, 2016, 10:37 PM), http://www.theglobeandmail.com/technology/tracking-our-phones-how-stingray-devices-are-being-used-by-police/article29322747/.
\item \textsuperscript{22}See e.g., Dingman, supra note 21; Brinson, supra note 17.
\item \textsuperscript{23}See e.g., Brinson, supra note 17.
\end{enumerate}
\end{footnotesize}
cellphone user and their device.\textsuperscript{24} This process automatically generates identifying information, including location data of varying degrees of precision.\textsuperscript{25}

As a general matter, with a valid order, government agencies can compel a provider to disclose location data, whether that data was generated by the wireless carrier in the normal course of business or specifically created in response to a surveillance request to “ping” a phone.\textsuperscript{26} Pinging is the process that allows service providers to generate location data at any time with a signal that directs the built-in satellite receiver in the particular cellphone to calculate its location and transmit that data back to the service provider.\textsuperscript{27} The cellphone needs only to be turned on; no calls need to be made, received, or completed for the service provider to ping a cellphone and determine its location.\textsuperscript{28} And unlike Global Positioning System ("GPS") technology,\textsuperscript{29} a user cannot disable cell site location information technology and it does not require any specific device capability.\textsuperscript{30}

\begin{itemize}
\item \textsuperscript{24} Id.
\item \textsuperscript{25} Id.
\item \textsuperscript{26} Pell & Soghoian supra note 4, at 145 & n.29.
\item \textsuperscript{27} In re Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 849 F. Supp. 2d 526, 534 (D. Md. 2011).
\item \textsuperscript{28} People v. Moorer, 959 N.Y.S.2d 868, 875 (Monroe Cnty. Ct. 2013); In re Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 849 F. Supp. 2d at 533.
\item \textsuperscript{29} GPS is a satellite based navigation system. It consists of satellites that orbit the Earth and transmit signals that give the current GPS satellite position and time. Once the GPS receiver in a cellphone captures signals from multiple satellites, it uses the transmitted data to calculate, based upon the relative strengths of signals from these multiple satellites and the time it took to receive a transmitted signal, a user’s location. The Global Positioning System, GPS.GOV (last updated Sept. 26, 2016), http://www.gps.gov/systems/gps.
\item \textsuperscript{30} GPS technology can typically calculate high quality accuracy location within ten meters. But limitations expose its fallible nature. A cellphone user can deactivate the GPS function (i.e.—turning off “location services” on an iPhone), and thus disable the ability to locate them. Also, if a GPS receiver’s view of the satellites is obstructed, it can comprise the reliability of GPS data. In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless
\end{itemize}
Stingrays operate in both similar and very different manners. They operate by mimicking cell towers, sending a mimicked “ping” signal. Nearby cellular devices then “identify the simulator as the most attractive cell tower in the area and transmit signals to the simulator that identify the device in the same way that they would with a networked tower.” Stingrays achieve greater precision; while a carrier’s cell-site location data can identify the location of a suspect’s complex, a Stingray can zero in on a phone’s location, down to a specific apartment.

There is one alarming difference: the signal a Stingray sends out compels all cellphones within range to transmit their unique identification information and location data to the Stingray, thereby scooping up data from every cellphone within reach, not just the target. Unlike the target specific search a phone carrier executes when asked to reveal data of the “sought after person,” no such boundary exists with Stingrays. One can dress up a Stingray with the purchase of an “Intercept Software Package,” which allows the user


33 See generally Pell & Soghoian, supra note 4.

34 United States v. Patrick, 842 F.3d 540, 543 (7th Cir. 2016) (“[a] cell-site simulator collects the relative location of everyone whose phone is induced to connect to the simulator . . . .”); Jonathan Bard, Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment, 57 B.C. L. REV. 731, 748 (2016).

35 Patrick, 842 F.3d at 542–44.

36 HARRIS GCSD PRICE LIST, supra note 6, 8.
of a Stingray to intercept calls, text messages, e-mail, and other data as well as block service to all or some devices in the area.\textsuperscript{37}

The severity of a Stingray’s implications vis-à-vis third parties not subjects of an investigation becomes evident when considered in our era of cellphone primacy. Although initially cellphones were primarily used to make calls, modern advancements have transformed the device into a multi-functional tool “more accurately labeled a pocket supercomputer.”\textsuperscript{38} The Pew Research Center reports that as of January 2017, 95 percent of all Americans own a cellphone of some kind.\textsuperscript{39} And of that share, 77 percent own smartphones.\textsuperscript{40} Smartphones have internet access and the ability to download a bountiful number of applications.\textsuperscript{41} Those that provide directions and social networking platforms barely scratch the surface.\textsuperscript{42} And because many third-party applications automatically send and receive data through the cellphone subscriber’s network, it makes this information vulnerable to a Stingray search too.\textsuperscript{43} As smartphones evolve, their storage capacities become the fulcrum; these devices can store for long periods of time

\begin{footnotesize}
\begin{enumerate}
\item The Department of Justice concedes that Stingrays possess such abilities and relies on law enforcement to configure the device to disable these functions. DOJ Policy Guidance, supra note 31, at 2; Pell & Soghoian, supra note 4, at 11–12.
\item The “basic” cellphone model today far exceeds simple call-making capabilities: “Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.” Riley v. California, 134 S. Ct. 2473, 2489 (2014). See also Steven I. Friedland, Riley v. California and the Stickiness Principle, 14 DUKE L. & TECH. REV. 121, 125–27. (2016).
\item Mobile Fact Sheet, PEO RESEARCH CT. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.
\item This is a significant increase from the 35 percent that the Pew Research Center reported in 2011 in a survey of smartphone ownership. Id.
\item Friedland, supra note 38, at 126.
\item Riley, 134 S. Ct. at 2490 (“There are over a million apps available in each of the two major app stores; the phrase “there’s an app for that” is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user’s life.”)
\item United States v. Patrick, 842 F.3d 540, 547 (7th Cir. 2016) (Wood, C.J., dissenting) (citing Pell & Soghoian, supra note 4, at 11–12).
\end{enumerate}
\end{footnotesize}
and disseminate, huge amounts of data, photos, financial and medical records, emails, and messages. Viewed in the aggregate, the data represents “a picture of a person’s private world.” All of this begs the question, how would 95 percent of the population at large react if they knew that police can access the privacies of their world with a simple add-on like the “Intercept Software Package”?

II. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, 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.

During the Colonial era, the crown of England frequently issued general search warrants known as “Writs of Assistance.” At their core, these instruments authorized English officials to enter places, search at their will, and seize customs-prohibited items. The officials needed no factual basis to justify the intrusion; the Writ alone gave them all the power.

_____

44 Friedland, supra note 38, at 126. A prime example of advances that facilitate the interconnectedness of cellphone data is Apple’s recent release of “Continuity,” a software that enables all a user’s devices to work together. Use Continuity to connect your Mac, iPhone, iPad, iPod touch, and Apple Watch, APPLE, https://support.apple.com/en-us/HT204681 (last visited Apr. 7, 2017).
45 U.S. CONST. amend. IV.
47 Id.
48 Id.
To serve as safeguard against such abuses, the Fourth Amendment was enacted with two separate clauses that articulate two distinct requirements. The Reasonableness Clause provides a broad prohibition against all “unreasonable searches and seizures” of “persons, houses, papers, and effects.” The Warrants Clause then requires that a warrant for a search or seizure be supported by “probable cause” and “particularly describe the place to be searched, and the persons or things to be seized.” Read in tandem, the Fourth Amendment requires any search or seizure, subject to certain exceptions, be authorized by a warrant and supported by a showing of probable cause.

Section A of this Part briefly explores the Court’s Fourth Amendment jurisprudence on the Reasonableness Clause. This involves a two-part, and often blurred, analysis that asks whether a “search” or “seizure” occurred within the meaning of the Fourth Amendment. The inquiry turns on whether an individual had a “reasonable expectation of privacy” in the item seized or the place searched. Section B then addresses the warrant requirements triggered when a court finds that a “search” or “seizure” has occurred. Part II concludes with Section C, which introduces the exclusionary rule available for a court to apply to safeguard the Fourth Amendment.

A. The Evolution of the Fourth Amendment & the Reasonableness Clause

Since the Fourth Amendment’s ratification, the Court’s interpretation of a “search” has been in flux. In 1886, the Court in *Boyd v. United States* articulated the first major interpretation of the

---

50 U.S. CONST. amend. IV
51 See id.
term within the meaning of the Fourth Amendment.\textsuperscript{54} In doing so, the Court explained it must interpret the Fourth Amendment broadly, given its protection of “the privacies of life.”\textsuperscript{55} Drawing on pre-Revolutionary events and cases, the Court analogized a forced document production to the physical invasion of one’s home and concluded that the compelled production of private papers at issue in \textit{Boyd} constituted a search under the Fourth Amendment.\textsuperscript{56}

In 1928, however, the Court in \textit{Olmstead v. United States} abandoned \textit{Boyd}’s liberal interpretation.\textsuperscript{57} \textit{Olmstead} involved a case of wiretaps attached to telephone wires on public streets.\textsuperscript{58} Rooting the inquiry in the concept of trespass, which requires a \textit{physical} intrusion, the Court reasoned that because the wiretapping involved neither a physical entry into the defendant’s house nor a confiscation of tangible property, no Fourth Amendment violation had occurred.\textsuperscript{59} Justice Brandeis wrote a noteworthy dissent, finding it “immaterial where the physical connection with the telephone wires was made.”\textsuperscript{60} He argued that while the private conversation transmitted by wire did not fall within the literal words of the Fourth Amendment, the way to meaningfully protect privacy rights is to deem “every unjustifiable intrusion by the government upon the privacy of the individual” as a Fourth Amendment violation.\textsuperscript{61}

Nearly forty years later, the Court decided \textit{Katz v. United States}, proving once again that the Fourth Amendment jurisprudence did not remain static.\textsuperscript{62} At issue in \textit{Katz} was the government’s eavesdropping

\textsuperscript{54} 116 U.S 616 (1886).
\textsuperscript{55} \textit{Id.} at 630; see also Jonathan Bard, \textit{Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment}, 57 B.C. L. REV. 731, 735 (2016).
\textsuperscript{56} \textit{Boyd}, 116 U.S. at 633.
\textsuperscript{57} 277 U.S. 438 (1928).
\textsuperscript{58} \textit{Id.} at 457.
\textsuperscript{59} \textit{Id.} at 466; Sklansky, \textit{supra} note 52, at 152.
\textsuperscript{60} \textit{Olmstead}, 277 U.S. at 479 (Brandeis, J., dissenting).
\textsuperscript{61} \textit{Id.} at 478; \textit{United States v. Jones}, 565 U.S. 400, 421–22 (2012).
\textsuperscript{62} 389 U.S. 347 (1967).
of a public telephone booth from which the defendant placed calls.\textsuperscript{63} Police conducted surveillance through an electronic listening and recording device attached to the outside of the booth.\textsuperscript{64} This form of surveillance fell on par with the wiretapping at issue in \textit{Olmstead}.\textsuperscript{65} Interestingly, under the \textit{Olmstead} framework, no search (physical trespass) or seizure (confiscation of tangibles) occurred in \textit{Katz}.\textsuperscript{66} And like the street wires in \textit{Olmstead}, the booth in \textit{Katz} logically did not fall within the realm of “persons, houses, papers, and effects” that the Court had understood the Fourth Amendment to protect.

Notwithstanding these parallels, Justice Stewart, writing for the majority, notoriously declared: “the Fourth Amendment protects people, not places.”\textsuperscript{67} The \textit{Katz} Court ultimately held that the police’s eavesdropping on the defendant’s calls constituted a search and seizure because it “violated the privacy upon which he justifiably relied when he used the telephone,” despite the booth’s public location.\textsuperscript{68}

The holding in \textit{Katz} extended the Fourth Amendment’s protections from physical intrusions onto physical and tangible property to individual’s privacy interests and intangible property.\textsuperscript{69} \textit{Katz} thus marked a clear shift in the Court’s Fourth Amendment jurisprudence focused on a common-law property-based trespass approach.\textsuperscript{70}

\textit{Katz} also laid the groundwork for the expanded definition of a search to where the government intrudes on an individual’s “expectation of privacy.”\textsuperscript{71} In order for an individual’s expectation of privacy to be afforded constitutional protection, two prongs must be

\begin{itemize}
  \item \textit{Id.} at 348.
  \item \textit{Id.}
  \item \textit{Olmstead}, 277 U.S. at 457.
  \item \textit{Katz}, 389 U.S. at 351–52.
  \item \textit{Id.} at 351.
  \item \textit{Id.} at 353.
  \item \textit{Id.}; see also Sklansky, \textit{supra} note 52, at 150–54.
  \item See United States v. Jones, 565 U.S. 400, 409 (2012) (“Our later cases, of course, have deviated from [the] exclusively property-based approach.”).
  \item \textit{Katz}, 389 U.S. at 360 (Harlan, J., concurring).
\end{itemize}
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.\textsuperscript{72} Since \textit{Katz}, the Court has understood the Fourth Amendment to protect a person’s reasonable expectation of privacy, but has clarified that that \textit{Katz}’s “reasonable expectation of privacy” test has been “\textit{added to, not substituted for}” the “common-law trespass” test.\textsuperscript{73}

\textbf{B. The Warrants Clause}

Absent exceptional circumstances, if a court finds that a search or seizure has occurred under the Fourth Amendment, it triggers the warrants requirements.\textsuperscript{74} The Court has interpreted the Warrants Clause to consist of three requirements: (1) warrants must be issued by a neutral and detached magistrate; (2) those seeking the warrant must demonstrate to the magistrate their probable cause to believe that “the evidence sought will aid in a particular apprehension or conviction” for a particular offense; and (3) warrants must particularly describe the place to be searched and the things to be seized.\textsuperscript{75}

\begin{itemize}
\item \textsuperscript{72} \textit{Id.} at 361. The Court in \textit{Katz}, however, did not refine the understanding of “reasonableness.”
\item \textsuperscript{73} \textit{Jones}, 565 U.S. at 409.
\item \textsuperscript{74} \textit{Katz}, 389 U.S. at 357. The Court eloquently described the purpose and meaning of the Warrants Clause in \textit{Johnson v. United States}:
\begin{quote}
[T]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity . . . When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.
\end{quote}
\textsuperscript{333} U.S. 10, 13–14 (1948).
\item \textsuperscript{75} U.S. CONST. amend. IV; \textit{Dalia v. United States}, 441 U.S. 238, 255 (1979).
\end{itemize}
When the Court decided *Katz*, it typically found searches conducted without warrants to be unlawful “notwithstanding facts unquestionably showing probable cause.”\(^{76}\) In fact, the Court in *Katz* affirmed that the prevailing understanding of an “unreasonable search” under the Fourth Amendment generally meant “without probable cause and a warrant.”\(^{77}\) Consistent with its precedent, the *Katz* Court also reaffirmed that subject only to the specific established and well-delineated exceptions, “searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment.”\(^{78}\)

Six months after *Katz*, the Court in *Terry v. Ohio*\(^{79}\) shed light on its new view on the connection between the Warrants Clause and the unreasonableness of a search. When confronted with the legality of the widespread and controversial stop and frisk procedures that police conducted without a warrant and probable cause, the Court in *Terry* broke with traditional understanding of what constituted “unreasonable” under the Fourth Amendment.\(^{80}\) Rather than reconciling the warrantless stop and frisk procedures under the limited exceptions referred to in *Katz*, the Court instructed that the central inquiry under the Fourth Amendment is “the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security.”\(^{81}\)

Translated to the context of *Terry*, a stop and frisk was not unreasonable simply because it was not authorized by a warrant or because the police lacked the probable cause needed for an arrest.\(^{82}\) The reasonableness of such a search rather turned on whether an

---

\(^{76}\) *Katz*, 389 U.S. at 357 (citing Agnello v. United States, 269 U.S. 20, 33 (1925)).

\(^{77}\) *Id.* (citing Wong Sun v. United States, 371 U.S. 471, 481–482 (1963)). See also Sklansky, *supra* note 52, at 151–52.

\(^{78}\) *Katz*, 389 U.S. at 357.

\(^{79}\) 392 U.S. 1 (1968).

\(^{80}\) *Id.* at 4; Sklansky, *supra* note 52, at 154.

\(^{81}\) *Terry*, 392 U.S. at 19.

\(^{82}\) *Id.* at 26–27; see also Sklansky, *supra* note 52, at 155.
officer had “reasonable suspicion” to first initiate the search, and whether the resulting search was reasonably related to the scope of the circumstances which justified the officer’s search in the first instance.\(^83\) This line of analysis thus allows courts to find that a warrantless search does not violate the Fourth Amendment if the search was “reasonable.”\(^84\) In this respect, \textit{Terry} and \textit{Katz} both clarify that while one may generalize that a warrantless search is “presumptively unreasonable,” it is not \textit{per se} unreasonable.

Despite this wrinkle, the Court has repeatedly held that where law enforcement conducts a search for discovering evidence of criminal wrongdoing, reasonableness generally requires it first obtain a judicial warrant.\(^85\) Magistrates are vested with a vital constitutional responsibility in the issuance of search warrants.\(^86\) To prevent an overly intrusive search, they must determine that all aspects of the search are supported by probable cause and impose appropriate limitations and conditions on the scope by fulfilling the particularity requirements.\(^87\) A sufficiently particular warrant includes an authorization to search places and things in which the particular things described might be concealed.\(^88\) If a court finds that the “scope of the search exceeds that permitted by the terms of a validly issued warrant” then “the subsequent seizure is unconstitutional without more.”\(^89\)

\(^83\) \textit{Terry}, 392 U.S. at 19–20. The framework \textit{Terry} created grants police latitude to conduct a search without a warrant where “the intrusion on the citizen's privacy ‘was so much less severe’ than that involved in a traditional arrest that ‘the opposing interests in crime prevention and detection and in the police officer’s safety could support’ the seizure as reasonable.” \textit{See Bailey v. United States}, 133 S. Ct. 1031, 1037 (2013).


\(^87\) \textit{Groh v. Ramirez}, 540 U.S. 551, 561 (2004). A particular warrant “assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.” \textit{Id.}


Police officers must execute the warrant in a reasonable manner, and the reasonableness of execution is subject to later judicial review. The scope of the warrant does not need to specify the manner of execution because the warrant process and the particularity requirements are concerned more with what may be searched and seized rather than how. The vitality of this distinction becomes unclear in the context of electronic surveillance, because not all information gathering technology is equivalent both in function and degree of intrusiveness.

To illustrate, an officer may obtain a warrant that authorizes the disclosure of an individual’s physical location, and there are numerous ways an officer can then ascertain this information. But, a location tracking warrant that authorizes the disclosure of a phone’s location does not, without more, authorize a search of the contents of the cellphone itself. The latter requires an independent search warrant. A search that forces a cellphone to transmit location data through contents stored within the phone is thus not the same as a phone provider initiating a signal to determine that same information. The two are simply not equivalent, even if the officer’s purpose in both scenarios focuses on identifying the phone’s physical location, which the location warrant may have authorized. It is then possible that an officer’s chosen method includes a device that functions in a manner sufficiently different from the location-gathering methods specified in a warrant that its use should constitute a search outside the warrant’s scope. Part V will discuss these issues in further detail.

Ultimately, because police conduct does not always conform to the Fourth Amendment’s mandates, the Court has recognized that it,

---

91 United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).
92 United States v. Patrick, 842 F.3d 540, 549 (7th Cir. 2016) (Wood, C.J., dissenting).
94 Patrick, 842 F.3d at 549 (Wood, C.J., dissenting).
and other courts, must exclude evidence obtained by unconstitutional police conduct.\textsuperscript{95} Part C now turns to the exclusionary rule.

\textit{C. The Exclusionary Rule}

In practice, the exclusionary rule allows a court to suppress evidence obtained in violation of the Fourth Amendment’s guarantee against unlawful searches and seizures.\textsuperscript{96} As written, the Fourth Amendment does not contain a provision that expressly precludes the use of evidence obtained through unconstitutional conduct.\textsuperscript{97} Whether the application of the exclusionary rule is appropriate in a particular case is “an issue separate from the question of whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct.”\textsuperscript{98} This means a court may recognize that an individual’s Fourth Amendment rights were violated but still decide not to apply the exclusionary rule.

The exclusionary rule is neither intended nor able to “cure the invasion of the defendant’s rights which he has already suffered.”\textsuperscript{99} Rather, it operates as “a judicially created remedy designed to safeguard Fourth Amendment rights generally through its \textit{deterrent effect}, rather than a personal constitutional right of the party aggrieved.”\textsuperscript{100} Because the purpose of the exclusionary rule is to deter police misconduct, a court may only apply the rule and suppress evidence if it determines that the deterrent benefits of exclusion outweigh its costs.\textsuperscript{101} So even when police obtain evidence through an

\textsuperscript{95} Utah v. Strieff, 136 S. Ct. 2056, 2059 (2016).
\textsuperscript{96} \textit{Id.} at 2029.
\textsuperscript{97} United States v. Leon, 468 U.S. 897, 906 (U.S. 1984).
\textsuperscript{98} \textit{Id.} (citing Illinois v. Gates, 462 U.S. 213, 223 (1983)).
\textsuperscript{99} Indeed, the Court has indicated that through its examination of the Fourth Amendment’s origin and purposes, the use of “fruits” of a past unlawful search or seizure “works no new Fourth Amendment wrong.” \textit{Id.}
\textsuperscript{100} \textit{Id.} (citing United States v. Calandra, 414 U.S. 338, 348 (1974) (emphasis added)).
\textsuperscript{101} Strieff, 136 S. Ct. at 2059. sBecause the Court severs the inquiry of whether a Fourth Amendment violation has occurred from the exclusionary rule’s remedy to
unconstitutional search or seizure, suppression of that evidence is not the automatic consequence. 102

Standing doctrine principles also limit a defendant’s ability to invoke the exclusionary rule. 103 The Fourth Amendment right against an unreasonable search and seizure is a personal right, which “may not be vicariously asserted.” 104 Thus, to have the requisite standing to bring a Fourth Amendment claim and invoke the exclusionary rule, a defendant must show that the challenged conduct invaded his own legitimate expectation of privacy rather than that of a third party. 105

Axiomatically, then, a defendant cannot succeed on a motion to suppress evidence by arguing that the challenged police conduct effectively violated others Fourth Amendment rights. 106 Suppression is proper only if the defendant’s own rights have been violated. 107 The Court has made clear that a court cannot suppress otherwise suppress evidence, it can manipulate the results. For an argument on how the Supreme Court has utilized the rule’s deterrent aspect to circumvent the inadmissibility of evidence obtained in violation of the Fourth Amendment, see Gerald G. Ashdown, The Fourth Amendment and the “Legitimate Expectation of Privacy”, 34 VAND. L. REV. 1289, 1292–94 (1981)

102 Leon, 468 U.S. at 906.

103 Standing stems from the “Case-or-Controversy” requirement under the judiciary’s Art. III powers. (“The judicial power shall extend to all Cases . . . [and] Controversies.” U.S. CONST. amend. III, § 2, cl.1. It pertains to who is the proper party to litigate a matter in court


106 Defendants commonly bring Fourth Amendment challenges in pre-trial motions to suppress incriminating evidence. The proponent of a motion to suppress has the burden of establishing that his Fourth Amendment rights were violated by the challenged search or seizure by a preponderance of the evidence. Rakas, 439 U.S. at 130 n.1; United States v. Johnson, 63 F.3d 242, 245 (3d Cir. 1995). Once a proponent establishes a basis for the motion (i.e.—the conduct constituted a search or that a seizure was conducted without a warrant), the burden shifts to the government to show each individual act constituting a search or seizure was reasonable. Johnson, 63 F.3d at 245.

107 In Patrick v. United States, both the majority and the dissent raised this issue. 842 F.3d 540, 545–46. See also infra pp. 55–57 (expanding upon the implications of standing and Stingray searches).
admissible evidence on the ground that it was seized unlawfully from a third party not before the court. “The interest in deterring illegal searches does not justify the exclusion of tainted evidence at the instance of a party who was not the victim of the challenged practices.”

These constrains limit the discussion of unconstitutional conduct that may affect innocent parties, particularly in the context of digital searches. Recall that during a Stingray search, police send out pings that may collaterally search third parties’ phones. But, a defendant does not have an expectation of privacy in the cellphones of third parties, so he cannot attack the search as “too sweeping.” Sadly, this may be unconstitutional conduct as to the parties whose interests were unreasonably invaded, but “a search can be unconstitutional with respect to one person yet lawful as to another.”

III. BACKGROUND PRECEDENTIAL CASE LAW

Although United States v. Patrick is the focus of this Note, the Seventh Circuit’s analysis heavily relied on a collection of Supreme Court case law dealing with electronic surveillance as well as the Court’s recent decision in Utah v. Strieff pertaining to the exclusionary rule. To understand the Patrick decision and why it suggests a departure from Supreme Court precedent, it is imperative to first discuss the facts and analyses of these prior cases.

A. Supreme Court Fourth Amendment Surveillance Case Law

Consistent with Katz, the Supreme Court began to explore whether the use of various novel technologies intruded upon individuals’ reasonable expectations of privacy. In 1979, the Court in Smith v. Maryland held that the installation and use of a “pen register,”

---

108 Payner, 447 U.S. at 735–36.
109 Id.
110 See id.
111 United States v. Gray, 491 F.3d 138, 144–45 (4th Cir. 2007).
a device that attaches to a telephone line and records the phone numbers dialed did not constitute a search and thus did not require a warrant. In Smith, police requested that a telephone company install a pen register to record the numbers dialed by the defendant. The Court held that an individual does not have an expectation of privacy in information conveyed to a third party. Accordingly, the defendant did not have a reasonable expectation of privacy in the numbers he dialed, since he communicated that information to his telephone company.

Then, in United States v. Knotts, questions surfaced regarding the propriety of police monitoring using a “beeper,” a radio transmitter device. In Knotts, police, with the consent of the seller, placed a beeper in a container of chloroform that was subsequently sold to the defendant who they suspected of using the chemicals to manufacture illegal drugs. Police observed the sale and transfer of the container to a car, and they maintained contact, relying both on visual surveillance (following the car that contained the chloroform container as it traveled across the public highways and ultimately to the defendant’s cabin), and a monitor which received the beeper signals. The Court found that the beeper surveillance amounted “to the following of an automobile on public streets and highways.” The police thus obtained information that the defendant voluntarily conveyed through his movements in public, which entitled him to no expectation of privacy. The Court also noted that there was no indication that the beeper was used in any way to reveal information about the movement of the container within the cabin, or information

113 Id. at 737.
114 Id. at 742.
115 Id.
117 Id.
118 Id. at 278.
119 Id.
120 Id. at 281.
that would not have been visible to the naked eye from outside the cabin.\textsuperscript{121} The police then did not need a warrant to use the beeper, since no “search” had occurred.\textsuperscript{122}

One year later, on nearly identical facts, the Court in \textit{United States v. Karo} revisited law enforcement’s warrantless use of a beeper.\textsuperscript{123} Like \textit{Knotts}, the container in \textit{Karo} contained a beeper device previously attached with the consent of the original owner.\textsuperscript{124} But, in \textit{Karo}, the defendant brought the container into various private residences, and the beeper signal identified the homes that the container had visited.\textsuperscript{125} It was this information that police then used to obtain a warrant, which ultimately led to a search of the homes that revealed illegal drug operations.\textsuperscript{126} Recall that in \textit{Knotts}, the record indicated the police limited the use of the beeper to only when they followed the defendant along public streets and not when the container arrived in its final location and transferred to the cabin.\textsuperscript{127} In \textit{Karo}, the police established the location of the beeper inside private residences, information gained from inside the home, and thus information that police would normally need a warrant to obtain.\textsuperscript{128} Logically, since entering a private residence is a search, so too was the use of the tracking device inside the residence.\textsuperscript{129}

\textit{Kyllo v. United States} presented the Court with the use of a then-novel thermal imagining device.\textsuperscript{130} In \textit{Kyllo}, police suspected that the defendant was growing marijuana plants inside his home, which

\textsuperscript{121} \textit{Id.} at 281–82.
\textsuperscript{122} \textit{Id.} at 279–80.
\textsuperscript{123} 468 U.S. 705 (1984).
\textsuperscript{124} \textit{Id.} at 707. Consistently, the Court held the mere transfer of the container to the defendant was not a search nor seizure because it did not convey any information that the defendant wished to keep private and did not reveal information that could not have been obtained through visual surveillance. \textit{Id.} at 712.
\textsuperscript{125} \textit{Id.} at 714.
\textsuperscript{126} \textit{Id.} at 719.
\textsuperscript{127} \textit{Knotts}, 460 U.S. at 281–82.
\textsuperscript{128} \textit{Karo}, 468 U.S. at 715.
\textsuperscript{129} \textit{Id.} at 715–16.
\textsuperscript{130} 533 U.S. 27 (2001).
normally requires a high-intensity heat lamp.\textsuperscript{131} Law enforcement, positioned on a public street nearby, used an advanced thermal imaging device that gathered information about the temperature inside the defendant’s home.\textsuperscript{132} This device allowed police to assess whether the amount of heat that flowed from the home was consistent with the use of marijuana grow lamps.\textsuperscript{133} The reading from the device showed high levels of heat, and police obtained a warrant to search the home based, in part, on this information.\textsuperscript{134} The Court held that when the government “uses a device that is not in general public use” to permeate the walls of the home and find out details it could not know without a physical intrusion, the surveillance constitutes a Fourth Amendment search and requires a warrant.\textsuperscript{135} The government thus may not use technology to observe the inside of the home, even if it does so from a location open to the public.\textsuperscript{136}

Harmonizing these three cases, a strong distinction emerged. Whether a search occurs turns on whether police could have obtained that information through ordinary visual surveillance (i.e.—monitoring movements in public areas, which does not require a warrant),\textsuperscript{137} or if police could not obtain such information through visual surveillance, because the monitoring occurred in a location that it could not access without a warrant (i.e.—the inside of a private residence).\textsuperscript{138}

The Court next turned to GPS tracking. In 2012, all nine Justices unanimously agreed in United States v. Jones that a GPS monitoring device attached to the bottom of the defendant’s car was a search, and its use without a warrant violated the Fourth Amendment.\textsuperscript{139} While all

\textsuperscript{131} Id. at 29.
\textsuperscript{132} Id. at 29–30.
\textsuperscript{133} Id. at 30.
\textsuperscript{134} Id.
\textsuperscript{135} Id. at 34.
\textsuperscript{136} See id. at 34–35.
\textsuperscript{139} United States v. Jones, 565 U.S. 400 (2012). In a notable moment during oral argument, arguing on behalf of the United States, the Deputy Solicitor General
nine agreed that the police’s attachment of the GPS device on the car and subsequent tracking of the car’s movements for 28 days in public constituted a search, they disagreed as to why. Five Justices deviated slightly with the Court’s almost exclusive reliance on the Katz framework for resolving Fourth Amendment cases and couched its holding in the government’s physical trespass on the defendant’s property consistent with the historical common-law trespass test. The four Justices that signed on to the majority opinion explained, the government, by attaching the GPS device, “occupied private property for the purpose of obtaining information.” This narrow basis alone was sufficient to decide the case, because such “a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.” Four Justices concurred in judgment, but disagreed with the majority’s reliance on the trespass theory. Justice Alito wrote on behalf of the four concurring Justices, arguing the Court should have applied Katz and held more broadly that, “reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle

indicated that his theory, which permits attachment of devices to monitor a car’s movement on public roadways, applies equally to the Justices. Oral Argument at 7:02–7:50, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259), https://www.oyez.org/cases/2011/10-1259. Chief Justice Roberts, taken aback, inquired “so you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?” Id. The Deputy Solicitor General responded in the affirmative, an unpopular concession. Id. The Jones colloquies demonstrate that arguments personal for the Justices when they imagine themselves in the shoes of the target. It may be wise for advocates to keep this consideration in mind, as questions regarding the constitutionality of Stingray devices will undoubtedly reach the Supreme Court in due time.

---

140 Jones, 565 U.S. at 404.
141 Id. at 404–05 (majority opinion). Justice Sotomayor provided the fifth vote.
142 Id. at 415 (Sotomayor, J., concurring).
143 Id.
144 Id. at 419 (Alito, J., joined by Ginsburg, Breyer, Kagan, JJ., concurring in judgment).
[the defendant] drove." Justice Sotomayor joined the majority’s trespass holding, but she also agreed with the four concurring Justices, that the long-term surveillance violated the defendant’s reasonable expectation of privacy.\textsuperscript{146} Significantly, then, all five concurring Justices emphasized the heavy weight the expectation of privacy analysis should carry in an era where physical intrusion is no longer necessary to many forms of modern government surveillance.\textsuperscript{147}

Nonetheless, the \textit{Jones} Court reaffirmed that the trespass test is not the exclusive test.\textsuperscript{148} “Situations involving merely the transmission of electronic signals without trespass,” it stated, “would remain subject to \textit{Katz} analysis.”\textsuperscript{149} Under the \textit{Katz} framework, a court can thus find a Fourth Amendment violation has occurred when police track movements through electronic signals if the individual has a reasonable expectation of privacy in the thing or place searched.\textsuperscript{150}

Most recently, in \textit{Riley v. California}, the Court broke with its long-standing categorical rule, that under the search-incident-to-arrest exception to the warrant requirement, police need not obtain a warrant to search “personal property immediately associated with the person of the arrestee.”\textsuperscript{151} The \textit{Riley} Court unanimously held that police must

\textsuperscript{145} \textit{Id.} at 419.

\textsuperscript{146} \textit{Id.} at 415 (Sotomayor, J., concurring) (“I agree . . . that, at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’”).

\textsuperscript{147} The concurring Justices rightfully warned that “the Court’s reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact . . . .” \textit{Id.} at 426 (Alito, J., dissenting); \textit{Id.} at 415–418 (Sotomayor, J., concurring). The majority in \textit{Jones} responded to these concerns, acknowledging, “[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.” \textit{Id.} at 412 (majority opinion).

\textsuperscript{148} \textit{Id.} at 411.

\textsuperscript{149} \textit{Id.} (alternation in the original) (emphasis omitted).

\textsuperscript{150} See \textit{id.}

\textsuperscript{151} 134 S. Ct. 2473, 2490 (2014).
obtain a warrant to search the contents of an arrestee’s cellphone seized incident to arrest.\textsuperscript{152}

Tugging at the seams of \textit{Riley} are countless references to “the pervasive nature of smartphone technology, its “immense storage capacity,” and the bountiful applications that manage “detailed information about all aspects of a person's life.”\textsuperscript{153} Unsurprisingly, the Court rejected California’s proposed test, which would allow officers to search, incident to an arrest, cellphone data if they could have obtained the same type of information from a pre-digital counterpart.\textsuperscript{154} Given the sophisticated functionality of most modern cellphones, the Court indicated that the pre-digital analogue test would lead to a “significant diminution in privacy rights” because it lacked meaningful limits.\textsuperscript{155} The test would permit police to search not only a vast quantity of information but also an unwarranted array of information. Just because a pre-digital era search could have turned up a couple of photographs in an arrestee’s wallet or a bank statement tucked away in a pocket, it did not justify “a search of thousands of photos in a digital gallery” nor “a search of every bank statement from the last five years.”\textsuperscript{156} The test would also allow police to search a range of items contained on a phone, even though an individual is unlikely to carry that information in physical form.\textsuperscript{157} It is highly suspect that individuals would walk around with physical copies of photos and financial records, all jammed in their pockets. Yet because each of these has a pre-digital analogue, they would be fair game.\textsuperscript{158} The Court stated that determining whether a pre-digital counterpart existed would “launch courts on a difficult line-drawing expedition to

\begin{flushleft}
\begin{footnotesize}
\textsuperscript{152} \textit{Id.} at 2490.
\textsuperscript{153} \textit{Id.} at 2484–95.
\textsuperscript{154} \textit{Id.} at 2493.
\textsuperscript{155} \textit{Id.}
\textsuperscript{156} \textit{Id.}
\textsuperscript{157} \textit{Id.}
\textsuperscript{158} \textit{Id.}
\end{footnotesize}
\end{flushleft}
determine which digital files are comparable to physical records” and “keep defendants and judges guessing for years to come.”\textsuperscript{159}

At the heart of \textit{Riley} is the Court’s realization that the rules from the pre-digital era are not so readily transferable to cellphones. Particularly, the possible intrusion on privacy with cellphones is not constrained by physical limitations:

A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.\textsuperscript{160}

Undeniably, \textit{Jones} and \textit{Riley} both illustrate the Court’s genuine and growing concern with privacy rights under the Fourth Amendment considering sophisticated capabilities of surveillance technology continue to evolve with breakneck speed.

Before turning to \textit{United States v. Patrick}, this Part concludes with a discussion on \textit{Utah v. Strieff}. Though not an electronic surveillance case, the Court shed light on the contours of the exclusionary rule in \textit{Strieff}, a decision that the Seventh Circuit extended in \textit{Patrick}.

\textbf{B. Utah v. Strieff}

Though the Court has generally held that officers must articulate proper justification for stops aimed at gathering evidence, it has also recognized exceptions.\textsuperscript{161} One exception, the “attenuation doctrine,”

\textsuperscript{159} \textit{Id.} The Court illustrated the unworkable nature of the test when it questioned, “Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?” \textit{Id.} The test also lacked any meaningful predictability, because “[i]t is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact.” \textit{Id.}

\textsuperscript{160} \textit{Id.} at 2491.

\textsuperscript{161} \textit{Utah v. Strieff}, 136 S. Ct. 2056, 2061 (2016).
permits the use of evidence against individuals even when discovered through misconduct if the connection between the misconduct and discovery of evidence is sufficiently weak.\textsuperscript{162} Consistent with the exclusionary rule’s deterrence objectives,\textsuperscript{163} the attenuation doctrine “mark[s] the point at which the discovery of evidence becomes so attenuated from the police misconduct that the deterrent benefit of exclusion drops below its cost.”\textsuperscript{164}

In \textit{Strieff}, a police officer stopped the defendant after he observed him leave a home that he suspected might contain drug activity.\textsuperscript{165} During the stop, the officer asked the defendant for identification and to explain what he was doing inside that home.\textsuperscript{166} The officer relayed the defendant’s identification information to a police dispatcher, who informed him that the defendant had an outstanding arrest warrant for a traffic violation.\textsuperscript{167} The officer then arrested the defendant pursuant to that warrant.\textsuperscript{168} He also performed a search incident to the arrest and found methamphetamine in the defendant’s pockets.\textsuperscript{169}

The State of Utah conceded that the initial stop was illegal because the officer lacked the requisite suspicion for the stop, but that the subsequent arrest was lawful because it was performed after he discovered the defendant’s outstanding arrest warrant.\textsuperscript{170} It thus argued that the officer’s discovery of the defendant’s valid arrest warrant attenuated the connection between the unconstitutional investigatory stop and the illegal drugs found in the defendant’s possession during the lawful arrest.\textsuperscript{171} The defendant argued that if the attenuation doctrine applied, it would “create a powerful incentive for police

\begin{thebibliography}{1}
\bibitem{162} \textit{Id.}
\bibitem{163} \textit{Id.} at 2063.
\bibitem{164} \textit{Id.} at 2071 (Kagan, J., dissenting).
\bibitem{165} \textit{Id.} at 2059–60 (majority opinion).
\bibitem{166} \textit{Id.} at 2060.
\bibitem{167} \textit{Id.}
\bibitem{168} \textit{Id.}
\bibitem{169} \textit{Id.}
\bibitem{170} \textit{Id.}
\bibitem{171} \textit{Id.}
\end{thebibliography}
officers to walk up to people on the street and simply stop them.”

He maintained that the exclusionary rule should apply to exclude the drug evidence discovered as a result of the illegal stop.

After analyzing the “temporal proximity” and “the presence of intervening circumstances” factors, the Court in Strieff moved to discuss the final factor of the attenuation doctrine test, “the purpose and flagrancy of the official misconduct.” The purpose and flagrancy factor reflects the deterrence rationale of the exclusionary rule by “favoring exclusion only when the police misconduct is most in need of deterrence—that is, when it is purposeful or flagrant.” When police exhibit deliberate, reckless, or a grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion becomes strong enough to outweigh the resulting costs.

Looking to the facts, the Court found that the officer made “good faith” mistakes, and was “at most negligent” in his decision to initiate the unlawful stop of the defendant. The facts did not rise to the level of flagrant misconduct the Court found in Kaupp v. Texas, where police carried out a warrantless search “some of whom, at least, were conscious that they lacked probable cause.” And while the purpose and flagrancy factor considers whether the misconduct was “calculated” to procure the evidence, the Court found that the officer in Strieff did not seek to initiate a fishing expedition when he stopped the defendant. Notably, the Court added “there [was] no

---

173 Strieff, 136 S. Ct. at 2064.
174 Id. at 2061.
175 Id. at 2063.
177 Strieff, 136 S. Ct. at 2063.
179 Strieff, 136 S. Ct. at 2066 (Sotomayor, J., dissenting) (citing Brown v. Illinois, 422 U.S. 590, 603–04 (1975)).
180 Id. at 2064 (majority opinion).
indication that this unlawful stop was part of any systemic or recurrent police misconduct.”\textsuperscript{181} Though it recognized a prevalence of outstanding warrants in various jurisdictions, it was unpersuaded that the mere suspicion of an outstanding warrant would lead police to conduct dragnet searches without cause.\textsuperscript{182} The Court ultimately held that the officer’s discovery of the valid outstanding warrant attenuated the connection between the unconstitutional stop and the evidence found during the later lawful arrest.\textsuperscript{183}

Undeniably, the majority opinion diluted the deterrent effect of exclusionary rule. Pre-\textit{Strieff}, an officer that wanted to stop an individual without any reasonable suspicion may have hesitated to consider the effect of the unlawful investigatory stop on the admissibility of any evidence discovered. But, \textit{Strieff} tells an officer he need not think twice. Post-\textit{Strieff}, an officer is more likely to make a stop even if he or she lacks reasonable suspicion because the stop “may well yield admissible evidence.”\textsuperscript{184}

Both the majority and dissent in \textit{Strieff} agreed that the role of deterrence is the gravamen of the exclusionary rule; they simply parted on whether the circumstances in \textit{Strieff} called for its application. The majority believed that the fear of being held civilly liable should serve as an effective deterrent against the temptation of dragnet searches.\textsuperscript{185} Evidence of such conduct, however, is not always readily available, and \textit{Strieff} opened the door for courts to chisel away at the remedy that the exclusionary was designed to afford.

\textsuperscript{181} \textit{Id.}  
\textsuperscript{182} \textit{Id.}  
\textsuperscript{183} \textit{Id.}  
\textsuperscript{184} The dissents of Justice Kagan and Justice Sotomayor conveyed these grave concerns. \textit{Id.} at 2074 (Kagan, J., dissenting); see also \textit{id.} at 2068–71 (Sotomayor, J., dissenting).  
\textsuperscript{185} \textit{Id.} at 2064 (majority opinion).
IV. UNITED STATES V. PATRICK

A. Background Facts

On October 28, 2013, Milwaukee Police Department ("MPD") officers arrested Damian Patrick while he was in his car on a public street. During the arrest, police found a gun in Patrick’s possession. Patrick was subsequently federally prosecuted as a felon in possession of a firearm under 18 U.S.C. § 922(g)(1).

During the time of his arrest, Patrick had two outstanding warrants. He was on parole, and a warrant was issued for his arrest because he failed to comply with the terms of his probation. To find Patrick, the MPD obtained a location tracking warrant, which authorized them to locate Patrick using cellphone data. But, the MPD did not locate Patrick by receiving coordinates from Patrick’s cellphone provider as the warrant authorized. After Patrick filed his opening brief in his appeal, amicus raised the question of whether the government used a Stingray to locate him. Only then—a year and a half after Patrick’s arrest—did the government admit that the MPD used a Stingray to gather data to pin down his location for the arrest.

---

186 United States v. Patrick, 842 F.3d 540, 541 (7th Cir. 2016);
187 Patrick, 842 F.3d at 541.
188 Id.
189 Id. at 542.
190 Id.
191 Id. This Note refers to the October 27, 2013 state court order, which authorized the disclosure of the location information associated with Patrick’s cellphone and the three approved surveillance methodologies to aid police in effectuating the arrest for the violation of parole warrant collectively as the “location tracking warrant.” See infra Section IV.B.
192 Id.
193 Id. at 546 (Wood, C.J., dissenting); Appellant’s Reply Brief at 11, United States v. Patrick, 2016 WL 2848759 (7th Cir. May 12, 2016) (No. 15-2443).
194 Patrick, 842 F.3d at 542; Appellant’s Reply Brief, supra note 193, at 11 (“In a letter . . . dated March 17th, 2016, the government confirmed that a Stingray was in fact used to track and locate Mr. Patrick.”).
B. The Location Tracking Warrant

So, what exactly did that second warrant authorize police to do? On October 27, 2013, based on an application submitted by the Milwaukee Assistant District Attorney and the supporting affidavit of a Milwaukee Police Officer, Milwaukee County Circuit Court Judge Stark found sufficient probable cause to issue an order that authorized the disclosure of location information for a cellphone that was known to be used by Patrick. Judge Stark’s order found sufficient probable cause to authorize the release of “cellular tower activity, cellular tower location, cellular toll information and cellular telephone global positioning system (GPS) location information, if available, that will permit identification of the physical location of the target cellular phone.” Judge Stark approved (1) the installation and use of a trap and trace device, (2) the installation and use of a pen register device, and (3) the release of cell-site location information related to the target cell phone.

The order also instructed Sprint, Patrick’s carrier, to provide the cell-site location information from July 27, 2013, to the date the order was signed and extending sixty days thereafter. As such, the order indicated the manner in which law enforcement was to collect the cell-site information. Specifically, it ordered Sprint, to provide cell-site location information, instructing “such service provider . . . shall initiate a signal to determine the location of the subject’s mobile

195 United States v. Patrick, No. 13-CR-234, 2015 WL 106158, at *2–*3 (E.D. Wis. Jan. 7, 2015), aff’d, 842 F.3d 540 (7th Cir. 2016) (Order Denying Motion to Suppress). In the order, the district court thoroughly described the contents of the October 27, 2013 state order, including the details of the application submitted by the Milwaukee Assistant District Attorney and the supporting affidavit of a Milwaukee Police Officer. This Note does not detail these documents or the facts each advanced to establish probable cause, as it does not bear on the Seventh Circuit’s analysis.

196 Id. at *2.

197 Id. at *3.

198 Id.

199 Patrick, 842 F.3d at 549 (Wood, C.J., dissenting).
device on the service provider’s network or with such other reference points as may be reasonably available. . . .”

C. Patrick’s Motion to Suppress & Procedural Background

The facts leading to Patrick’s appeal are convoluted, largely because the government disclosed the truth of the Stingray’s use in drawn out phases. At the outset, three officers prepared reports concerning their involvement in Patrick’s arrest. In the reports, they indicated that they either: (1) “obtained information” of Patrick’s location; (2) had “prior knowledge” that Patrick was occupying the vehicle, which officers observed while on patrol; and (3) “obtained information from an unknown source” that Patrick was inside the vehicle at that location.

On January 11, 2014, Patrick filed his first motion to suppress the gun that MPD found in his possession, arguing that the MPD seized him unlawfully without reasonable suspicion. Then, during an evidentiary hearing on February 4, 2014, officers testified that they did not locate Patrick on an anonymous tip, revealing, for the first time, that they located Patrick by tracking his cellphone. Based on this new information, Patrick withdrew his initial motion and filed a new motion on August 1, 2014, arguing that the state order authorizing police to obtain the location of his cellphone did not amount to a warrant under the Fourth Amendment because the order lacked the requisite probable cause to track his phone in real time to determine his location.

---

200 Id.
201 Patrick, 2015 WL 106158, at *2
202 Id. at *2 & n.1.
203 Id. at *1.
204 Id. at *2.
205 Id. at *2; Brief for Appellant at 7, United States v. Patrick, 2016 WL 211768 (7th Cir. Jan. 15, 2016) (No. 15-2443); see also Patrick, 2015 WL 106158, at *3.
On January 7, 2015, the district court adopted the magistrate judge’s recommendation in full and denied Patrick’s motion to suppress the gun evidence. The court found that Judge Stark had a “substantial basis” for concluding that probable cause existed for the order she issued authorizing the disclosure of the location information related to Patrick’s cellphone. What to make of the fact that the order did not mention a Stingray? Not necessary, said the district court. Because the order complied with the three requirements of the warrants clause of the Fourth Amendment, it effectively served as a warrant, so “no further authorization was required for the government to track Patrick’s cellphone.”

Patrick then conditionally pled guilty to the unlawful possession of a firearm charge, but he reserved the opportunity to contest the district court’s denial of his motion to suppress. He received a 57-month sentence on June 29, 2015, and he subsequently filed a notice of appeal on July 8, 2015.

In his opening brief in his appeal to the Seventh Circuit, Patrick argued that the location tracking warrant did not contain the requisite probable cause to authorize the tracking of the cellphone, and accordingly, that the gun that police found as a result of the illegal tracking should be suppressed. Amicus then raised the possibility that the government used a Stingray to locate Patrick, and on March 17, 2016, the government confirmed that police did in fact use a Stingray to track and locate Patrick. Apparently, months before Patrick’s arrest, the MPD signed a non-disclosure agreement (“NDA”)

---

206 Patrick, 2015 WL 106158, at *1. At the time of the district court’s ruling on Patrick’s August 1, 2014 motion to suppress, the government readily acknowledged that law enforcement determined Patrick’s location on October 28, 2013, by tracking his cell phone. Id. at *2 & n.1.
207 Id. at *7.
208 Id. at *7
209 Id.
210 United States v. Patrick, 842 F.3d 540, 541 (7th Cir. 2016).
211 Id.; Brief for Appellant, supra note 205 at 7.
212 Patrick, 842 F.3d at 541; see also Brief for Appellant, supra note 205.
213 Appellant’s Reply Brief, supra note 193, at *11.
with the Federal Bureau of Investigations (“FBI”).214 Per the agreement, the MPD must keep secret information about the Stingray in “pre-trial matters, search warrants and related affidavits, discovery, in response to court ordered disclosure and other affidavits, and on appeal.”215

Patrick then argued in his reply brief that should the Seventh Circuit not order the evidence suppressed, based on the nature of his conditional plea, the court should remand the case to the district court to accept additional briefing on the government’s use of Stingray.216 This new information invoked the question of whether the Stingray’s use constituted a warrantless search outside the scope of the state location tracking warrant, and whether suppression of the gun was proper.

D. The Seventh Circuit’s Decision

A divided panel of the Seventh Circuit held the fact that police used a Stingray to track and locate Patrick for the arrest did not justify application of the exclusionary rule.217 Accordingly, the court affirmed the district court’s denial.218 Judge Easterbrook, writing for the majority, concluded it need not resolve the issues posed by the police’s use of the Stingray.219 The majority saw this case plain and simple: Patrick was arrested in public, based on probable cause, and pursuant to a valid arrest warrant, all of which sufficed to render the arrest and incident search lawful.220 Because police arrested Patrick in a public place, they were entitled to arrest him based on probable cause alone; this made any deficiencies in the location tracking warrant immaterial,

214 Id. at *12
215 Id. As an employee of the MPD, the police officer who prepared the supporting affidavit for the location tracking order was bound to the agreement.
216 Id. at *11–*16.
217 Patrick, 842 F.3d at 545.
218 Id.
219 Id. at 542.
220 Id.
because under the circumstances, police were entitled to arrest Patrick without any kind of warrant.\textsuperscript{221}

The majority also held that \textit{Utah v. Strieff} independently supported its conclusion that suppression was improper.\textsuperscript{222} It interpreted \textit{Strieff} to hold that “a valid arrest warrant precludes the suppression of evidence seized in an arrest, even if the arrest was set in motion by officers who had neither probable cause nor knowledge of the warrant.”\textsuperscript{223} Patrick’s valid outstanding warrant was issued before any of the police’s efforts to learn his location, and so “their efforts could not taint the arrest ‘in the parlance of the exclusionary rule.’”\textsuperscript{224}

The majority acknowledged that no other court of appeals has yet to address questions about whether (1) the use of a cell-site simulator is a search, (2) if the use of a Stingray is a search, whether a warrant must authorize its use. While it stated it would be “best to withhold full analysis until these issues control the outcome of a concrete case,” it nonetheless proceeded to weigh in.\textsuperscript{225}

The government had conceded for purposes of the case only that the use of a Stingray was a search.\textsuperscript{226} Still, the majority recapped Supreme Court precedent and said it could go either way.\textsuperscript{227} The majority raised the possibility that the use of a cell-site simulator could fall under the \textit{Smith v. Maryland} and \textit{United States v. Knotts} framework and thus not a search.\textsuperscript{228} It also then recognized \textit{Jones} provided a contrary line of arguments that analogized cell-site

\begin{itemize}
\item \textsuperscript{221} \textit{Id.} at 542.
\item \textsuperscript{222} \textit{Id.} at 542 (citing \textit{Utah v. Strieff}, 136 S. Ct. 2056 (2016)).
\item \textsuperscript{223} \textit{Id.}
\item \textsuperscript{224} \textit{Id.}
\item \textsuperscript{225} \textit{Id.}
\item \textsuperscript{226} \textit{Id.}
\item \textsuperscript{227} \textit{Id.} at 544.
\item \textsuperscript{228} \textit{Id.} at 543 (majority opinion) (first citing \textit{Smith v. Maryland}, 442 U.S. 735, 1979); then citing \textit{United States v. Knotts}, 460 U.S. 276 (1983)). The majority also cited to recent decisions of the Fourth Circuit in \textit{United States v. Graham} (824 F.3d 421 (4th Cir. 2016) (en banc)) and the Sixth Circuit in \textit{United States v. Carpenter} (819 F.3d 880 (6th Cir. 2016)), which held that “tracking a person via data from phone companies is not a search within the scope of the Fourth Amendment.” \textit{Id.}
\end{itemize}
simulators to GPS locators. It acknowledged that all five concurring Justices suggested that the use of such devices may be searches when used for extended durations, and thus if the concurring approaches are adopted, it would be necessary to know how long the police used the Stingray to track Patrick. Lastly, it alluded that the Stingray’s degree of precision would bear a significance: “is it information that leaves uncertainty about where in several city blocks a suspect may be, such as the beeper in Knotts, or is it closer to the precise location supplied by a GPS tracker [in Jones]?"

With respect to the warrant, Patrick and the United States disagreed on the significance of the fact that police did not reveal to the state judge who issued the location tracking warrant that it planned to use a cell-site simulator. Patrick raised two challenges regarding the warrant and the government’s lack of candor. First, he argued that “leaving the judge in the dark (perhaps misleading the judge by omitting a potentially material fact) made the location-tracking warrant invalid.” Patrick’s position was that the issuing judge was entitled to know that the police intended to use a cell-site simulator and accordingly authorize that method as part of the warrant. This kind of restriction focuses on ex ante limitations, which refer to attempts to regulate the search before it occurs.

The gist of the position on ex ante restrictions is as follows:

Perhaps you will sign the warrant only if the FBI agents agree to use a particular search protocol. Or . . . only if the government agrees to minimize the seizure of the suspect's hardware or if the government agrees to waive any rights to seize any items discovered in plain view outside the warrant. Whatever restriction you choose, the goal is to protect the Fourth
concluded that neither constitutional text nor precedent supports *ex ante* regulations; rather, it forbids such restrictions and confines the judiciary only to the *ex post*, after-the-fact, assessments of whether a search warrant was reasonable.238

Second, and closely related, Patrick argued that even if *ex ante* authorization of the method was unnecessary, the government must be candid when they mention methods of executing a search warrant.239 He sought to remand the case to explore these issues “after the fashion of a Franks hearing at which the court would decide whether the warrant still would have issued if the affidavits had been more forthcoming.”240 The majority rejected further exploration of these issues, because it found the answers to those questions were not dispositive to the case based on the factual circumstances.241 Patrick was arrested in a public place, and the arrest was supported by both probable cause and a valid arrest warrant issued before any effort to learn his location; therefore, the police’s subsequent effort to learn his location could not taint the arrest.242 The majority thus found it would be inappropriate to apply the exclusionary rule, “even if the police should have told the judge that they planned to use a cell-site simulator

Amendment ex ante: you can best protect the Fourth Amendment by imposing conditions when you issue the warrant on how it later will be executed.

Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1243–44 (2010). Stingray searches implicate a great deal of considerations absent in Professor Kerr’ analysis on warrants for computer searches, mainly, because they differ in their collateral consequences vis-à-vis innocent third parties.238

Patrick, 842 F.3d at 544–45 (citing Kerr, supra note 237, at 1260–71).

239 Id. at 545.

240 Id. (citing Franks v. Delaware, 438 U.S. 154 (1978)). Under Franks v. Delaware, the defendant “must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit.” 488 U.S. at 156. See Justin Brown & Kashia M. Leese, Stingray Devices Usher in A New Fourth Amendment Battleground, 39 CHAMPION 12, 17 (June 2005), for a persuasive argument on how defendants can utilize Franks as a lifeline.

241 Patrick, 842 F.3d at 545.

242 Id. at 542, 545.
to execute the location warrant.”\footnote{Id. at 545.} In sum, the majority concluded that because the arrest was lawful, which rendered the gun seized admissible, it need not definitely resolve any issues Patrick raised regarding the police’s use of the Stingray.\footnote{Id. at 542, 546.}

Chief Judge Wood dissented, characterizing the case more about how police found Patrick rather than where they found him.”\footnote{Id. at 545 (Wood, C.J., dissenting) (“This case raises serious issues about the use of cell-site simulators to track down the location of a target person.”).} Chief Justice Wood argued that the record was factually “fatally inadequate” on the use of the Stingray and the intricacies the device.\footnote{Id. at 546–47, 549, 552.} She argued this precluded a meaningful resolution of whether police violated Patrick’s Fourth Amendment rights, because questions posed by the police’s use of the Stingray affected whether Patrick’s initial arrest was valid.\footnote{Id. at 546.} If it was invalid, then the gun that the police spotted in plain view in the car should have been suppressed.\footnote{Id. at 552.} Chief Judge Wood would have thus remanded the case for further fact-finding.\footnote{Id. at 552.}

\section*{IV. The Implications of the Seventh Circuit’s “Blissful Ignorance” / Implications of the Decision & Stingray Technology}

The remainder of this Note focuses its analysis on three key points implicated by the Seventh Circuit’s decision in \textit{Patrick}.\footnote{Chief Judge Wood also discussed Title III, though this Note does not address her argument on that issue in detail.} Section A discusses the holding regarding \textit{Utah v. Strieff}. Section B then examines the court’s discussion on whether the use of a Stingray devices constitutes a search under the Fourth Amendment. Section C looks to the court’s stance on whether the use of the Stingray exceeded
the scope of the location tracking warrant and whether a warrant that specifically authorizes the use a cell-site simulator is necessary to constitute a valid warrant under the Fourth Amendment.

A. The Majority's Uncomfortable Extension of Utah v. Strieff

The majority’s interpretation expanded Strieff to hold that the mere existence of an outstanding warrant attenuates the police officer’s illegal conduct from the items subsequently seized.\(^{251}\) But, Strieff requires more than just an intervening event.\(^{252}\) As Chief Judge Wood pointed out in dissent, Strieff rests on a break in the casual chain that attenuates Fourth Amendment concerns from the officer’s initial illegal actions and the subsequent search.\(^{253}\) The Strieff Court indicated that necessary to its reasoning was not only a valid warrant that predated the officer’s investigation, but that the warrant “was entirely unconnected with the stop,” and that the officer’s decision to arrest the defendant was “a ministerial act that was independently compelled by the pre-existing warrant.”\(^ {254}\) This is factually inapposite to the facts in Patrick. The Stingray was wholly connected—indeed, police intentionally used the device to effectuate Patrick’s arrest.\(^ {255}\)

Subtly, the majority extrapolates from Strieff, “if the police had stopped Patrick’s car for no reason at all and learned only later that he was a wanted man, the gun would have been admissible in evidence.”\(^ {256}\) This conclusion facilitates the very concerns the defendant in Strieff raised. In general, the court’s interpretation as written essentially gives law enforcement carte blanche to conduct searches, so long as they find incriminating evidence after the fact. In

\(^{251}\) Patrick, 842 F.3d at 542 (majority opinion).


\(^{253}\) Patrick, 842 F.3d at 549–50 (Wood, C.J., dissenting) (citing Strieff, 136 S. Ct. at 2060 (2016)).

\(^{254}\) Id. (citing Strieff, 136 S. Ct. at 2062).

\(^{255}\) Id. The MPD’s arrest of Patrick and the search that led to the gun was also not a ministerial act. Id.

\(^{256}\) Id. at 542 (majority opinion) (citing Strieff, 136 S. Ct. 2060).
the factual context of *Patrick*, it insinuates that law enforcement can utilize whatever means it deems fit to locate an individual, regardless of what a warrant authorizes, because the mere existence of the individual’s outstanding arrest warrant will attenuate the connection between illegal Fourth Amendment conduct and evidence seized.\(^{257}\)

The majority also ignored that the Court held in *Strieff* as it did because there was no evidence of purposeful or flagrant police misconduct; rather, the officer in *Strieff* was merely negligent when he conducted the unconstitutional investigatory stop.\(^ {258}\) The record in *Patrick* lacked facts to conclude that the MPD’s conduct was simply mere negligence.\(^ {259}\) The record quite oppositely indicated that “police knew what they were doing.”\(^ {260}\) Facts of possible concealment of intent to use a cell-phone stimulator or knowledge of exceeding the scope of the warrant would rise to the level of flagrance or misconduct that *Strieff* specifically carved out.

As *Strieff* demonstrated, the exclusionary rule rests primarily—if not solely—on the role of deterrence, a consideration wholly absent in the Seventh Circuit’s analysis. The majority tossed aside any meaningful culpability on MPD’s part, rationalizing that although the MPD purposefully concealed their intent to use a cell-site simulator, and misrepresented to the state judge that they would use phone company data to locate Patrick, “[a] fugitive cannot be picky about how he is run to ground.”\(^ {261}\) Even if one agrees with the majority, that the circumstances of Patrick’s arrest (in public, with probable cause and pursuant to an arrest warrant) did not justify the exclusionary rule, the majority remains at fault for its failure to offer discussion on the role of deterrence as to the MPD’s misleading conduct.\(^ {262}\)

---

\(^{257}\) *Id.* at 545.

\(^{258}\) *Strieff*, 136 S. Ct. at 2064.

\(^{259}\) *Id.*

\(^{260}\) *Patrick*, 842 F.3d at 550 (Wood, C.J., dissenting).

\(^{261}\) *Id.* at 545.

\(^{262}\) Admittedly, the NDA signed by the MPD affected its candor, but this Note offers no opinion on how this should impact the purpose and flagrancy factor analysis. This Note rather argues the majority should have acknowledged that *Strieff* tolerates negligence, while the MPD remained conscious of their deception. The
B. Is the Use of a Stingray Device a “Search” Under the Fourth Amendment?

Although the United States conceded that the use of a Stingray constituted a search in Patrick, the Seventh Circuit discussed, but did not definitively resolve, whether the use of a cell-site simulator constitutes a search under the Fourth Amendment. To be fair, the Seventh Circuit did not need to resolve the issue. But, the court also lacked the requisite facts to offer a fair assessment both generally and in Patrick’s case. Still, it weighed in, and in doing so, made unwarranted factual assumptions.

The majority cited to a Department of Justice Policy Guideline on the use of cell-simulator technology (“DOJ Policy Guidance”), which states the Department must configure a cell-site simulator as a pen register. The majority said a Stingray would then resemble the kind of pen register used in Smith, because it would not reveal communicative content, and also the beeper in Knotts, because it would obtain only location information and nothing else. First, the DOJ Policy Guidance is not binding on local law enforcement agencies like the MPD. MPD used the Stingray, not the Department, so that renders any guarantees made in the DOJ Policy Guidance immaterial. Second, the DOJ Policy Guidance did not provide any detail on the Stingray or its capabilities, just that one must configure it as a pen register as to not catch “emails, texts, contact lists, images or

---

majority should have seen “purposeful evasion of judicial oversight of potentially illegal searches as exactly the kind of police misconduct most in need of deterrence.” Id. at 550 (Wood, C.J., dissenting) (quoting Strieff, 136 S. Ct. at 2063).

263 Id. at 544 (majority opinion)

264 Id. at 542–53 (citing DOJ Policy Guidance, supra note 30, at 2).

265 Id. at 543 (citing Smith v. Maryland, 442 U.S. 735 (1979)).

266 Id. (citing United States v. Knotts, 460 U.S. 276 (1983)).

267 DOJ Policy Guidance, supra note 30, at 2 n.2 (“This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility . . . .”).
any other data from the phone.” Chief Judge Wood pointed out, Stingrays include exactly these capabilities, so it oversimplifies the inquiry to analogize it to a “high-tech pen register.” Depending on the features of the particular Stingray and the way it is configured, a Stingray can intercept communications as well as location data. The court in Patrick knew nothing concrete about the general extent of its surveillance capabilities or the specific way the MPD configured the Stingray in Patrick’s case. Yet, to make the analogy, the majority suggested an uninformed assumption that the location information was all that was collected because that was all that police revealed.

Regarding the beeper, the majority’s analysis only got it half right. In discussing Knotts, the majority zeroed in on the fact that a beeper does not give precise location data and rather indicates a general block where a suspect may be located. But, this was not the only reason why the Court held in Knotts that the use of a beeper was not a search. Properly read, Knotts held that no Fourth Amendment violation occurred when police used a beeper to track the movements of the container, because it revealed only location information that police also obtained simultaneously through visual surveillance. Specifically, by following the car that held the container. Crucially different is that the police in Patrick obtained the warrant to find Patrick. Police did not know where he was, so fundamentally, they could not follow him.

To the majority’s credit, it did recognize that another line of case law offers support for finding that the use of a Stingray constitutes a search. It acknowledged that one could analogize a cell-site simulator

268 *Id.* at 2.
269 *Patrick*, 842 F.3d at 547 (Wood, C.J., dissenting).
270 *Id.*
271 See *id.* 542–43 (majority opinion).
272 *Id.* at 543.
274 *Id.* at 281.
275 See *Patrick*, 842 F.3d at 542.
device to a GPS locator, which the *Jones* Court treated as a search.\(^{276}\) And per the concurring justices, the length of time police used the device and the precision of the location data collected remained relevant.\(^{277}\) It also noted technology that intrudes into the home where there is a heightened privacy interest is a search under *Kyllo*.\(^{278}\) This was the extent of the court’s analysis, however.

Though the Seventh Circuit is the first court of appeals to discuss whether the use of a Stingray device is a search, other courts have had the occasion to weigh in. As a general matter, this Note takes the position that the use of a Stingray device constitutes a search within the meaning of the Fourth Amendment. And, virtually all case law agrees.\(^{279}\) Based on Supreme Court precedent, ultimately critical to any challenge of a search utilizing stingray technology will be the nature of the Stingray technology as it implicates the manner of a search in a constitutionally protected place under *Kyllo*, the location of the target phone as *Karo* and *Kyllo* both highlighted, the length of the tracking the Court in *Jones* emphasized, and whether the Stingray searched the contents of the phone, the kind of search the *Riley* Court held required a warrant.

To begin, Stingray devices fall right on par with the thermal imaging device at issue in *Kyllo*. One cannot plausibly characterize a

\(^{276}\) *Id.* at 544 (citing United States v. *Jones*, 565 U.S. 400 (2012))

\(^{277}\) *Id.* (citing *Jones*, 565 U.S. at 954–65) (concurring opinions of Sotomayor and Alito, JJ.).

\(^{278}\) *Id.* (citing *Kyllo* v. United States, 533 U.S. 27 (2001)).

\(^{279}\) State v. Andrews, 134 A.3d 324, 350 (Md. Ct. Spec. App. 2016) (holding that the use of a cell site simulator to obtain location information directly from an individual’s cell phone is a search under the Fourth Amendment and requires a search warrant; United States v. Lambis, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016) (holding the government use of a cell-site simulator constituted a search under the Fourth Amendment that required a warrant); States v. Tutis, No. CR 14-699 (JBS), 2016 WL 6136577, at *5 (D.N.J. Oct. 20, 2016) (same). *See also* Patrick, 842 F.3d at 543 (government conceded the use of a Stingray is a search); United States v. Rigmaiden, 844 F. Supp. 2d 982, 997 (D. Ariz. 2012) (the government conceded that the search for the aircard constituted a Fourth Amendment search).
Stingray as “in general public use.” These devices are not within the general public’s reach because federal law enforcement agencies and police departments receive offers for the devices exclusively through directly mailed vendor letters. And parallel to Kyllo’s thermal imagining technology, a Stingray sends electronic signals that penetrate the walls of a home, allowing police to explore the details of a home and obtain information that they could not obtain otherwise without physically intruding into the home. Under this rationale, two courts have ruled that law enforcement’s use of the cell-site simulator to locate the defendant’s apartment was an unreasonable search, given the “pings” from the defendant’s cell phone to the nearest cell site were not readily available “to anyone who wanted to look” without the use of a cell-site simulator.

The Court has repeatedly demonstrated impatience with searches conducted in private residences that failed to comport with the Fourth Amendment. Discussing Karo and Kyllo in tandem, two scholars understand the Court’s position as follows: the “Fourth Amendment draws a line at the entrance of the house, and the line “must be not only firm but also bright which requires clear specification of those methods of surveillance that require a warrant.”

Though the case law weighs against finding a Fourth Amendment search when police utilize a Stingray to monitor phones in public areas, it is not so simple. A Stingray is blind to any distinction of public versus private; when utilized, it recognizes all cell phones

---

280 Lambis, 197 F. Supp. 3d at 610. The most basic model also costs approximately $75,000, well beyond the affordability of the public to purchase. See Andrew Hemmer, Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches, 91 CHI.-KENT L. REV. 295, 308 (2016).

281 Hemmer, supra note 280, at 308.

282 Lambis, 197 F. Supp. 3d at 610 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001)).

283 Id. at 610–11 (“The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of Kyllo.”); Andrews, 134 A.3d at 324.

within an area of several kilometers. And a reasonable assumption that follows is that at least some affected cellphones will be inside private homes. If the searches in *Karo* and *Kyllo* were Fourth Amendment violations, so too is the use of a cell-site simulator to determine a suspect’s location inside a private home, even if the Stingray limits its signals to that target. A court should likewise find a Fourth Amendment violation in a Stingray search that collaterally searches cellphones inside third parties’ homes as a mechanism to ascertain the target cellphone’s location. We must take caution to remember we are in an era where 95 percent of individuals own a cellphone. It is precisely such sensitivity that led the one court to conclude that “[b]ecause the vast majority of the population uses cell phones lawfully on a daily basis, one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful.” Compared with a canine sniff of luggage at the airport, which does not intrude upon any legitimate privacy interest since the sniff reveals nothing about non-contraband items, a Stingray device is a completely different animal.

The scant case law does not discuss Stingray searches under the backdrop of the “long-term tracking” issues *Jones* raised. If police know the target’s number, a Stingray search could move fast. Indeed,
in *Patrick*, the police located Patrick one day after it obtained the location tracking warrant. But, police do not always know the target’s number. For example, a suspect may rely on pre-paid disposable phones commonly known as “burner phones,” which make tracking harder, but not impossible, to track. Police would then need use the Stingray to intercept data from an unknown quantity of devices, and eventually, through a process of elimination, the collected information would provide calling and messaging patterns that identify a suspect’s phone. In this scenario, the timeline and degree of intrusiveness greatly increases.

The majority’s analysis was not only limited, but it was also selective. Nowhere did the majority mention *Riley v. California*. Though factually different than *Patrick*, *Riley* suggested that the Court would highly scrutinize Stingray searches if the device searched the contents of the phone and data to determine the target location, for after *Riley*, police must obtain a warrant to search cell-phone data. As Chief Justice Wood explained, “the location warrant authorized only methods of fixing Patrick’s location that involved gathering information that would reveal his phone’s connection with cellphone towers,” and the “authorization of the collection of location data cannot be expanded to permit a search of the contents of Patrick’s cell

---

292 United States v. Patrick, 842 F.3d 540, 541 (7th Cir. 2016).
295 *Riley v. California*, 134 S. Ct. 2473, 2485 (2014); see also id at 2493 (“We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.”).
If the Stingray gathered information from Patrick’s phone that went beyond his location, “such a ‘search’ of his phone would have been unauthorized.” But, the court had no information on whether the Stingray gathered information that went beyond his location information and whether it searched the contents of the cellphone itself to determine the location.

In its brief discussion on the issue, the majority conveyed a strange reluctance to find, as a general matter, that the use of a Stingray constitutes a “search.” Ultimately, it did not illicit what one would hope a court would express: a strong sense of unease regarding the factual holes, especially given the intrusive nature of the devices.

C. Warrants Requirements for Stingray Searches

Patrick raised two intertwined yet distinctive challenges to the Stingray use, both of which ultimately turn on whether a judge is entitled to know how a warrant will be executed. The majority took a stance wholly deferential to law enforcement, concluding that the Fourth Amendment forbids ex ante limitations and confines the judiciary only to the ex post assessments of whether the method of execution was reasonable. Though the majority in Patrick relied heavily on United States v. Dalia, where the Court noted “the specificity required by the Fourth Amendment does not generally extend to how warrants are executed,” Chief Judge Wood rightfully pointed out that this statement must be understood in context. The Stingray device itself was at issue in Patrick, and because of its

---

296 Patrick, 842 F.3d at 547 ((Wood C.J. dissenting) (citing Riley, 134 S. Ct. at 2494–95)).
297 Id.
298 Id.
299 Id. at 544–45 (majority opinion).
300 Id. at 544 (citing Dalia v. United States, 441 U.S. 238, 256 (1979)).
301 Id. at 548 (Wood, C.J., dissenting) (citing Dalia, 441 U.S. at 257).
sophisticated capabilities, “the way it was used could affect the scope and location of the search itself.”

Given their novel nature, only a handful of courts have had the occasion to address questions pertaining to Stingrays and warrants requirements. *United States v. Rigmaiden* was one of the first cases that dealt with Stingrays. In *Rigmaiden*, police suspected the defendant of perpetrating a fraudulent tax scheme where he used identity data of third parties to electronically file tax returns and claim tax refunds.

Police obtained a tracking warrant that authorized a “mobile tracking device” to monitor the defendant’s aircard but failed to describe the specific technology and how it would generate the signal to fix the defendant’s location. Police ultimately used a device that functioned akin to a cell-site simulator to track and locate the location of the defendant’s aircard contained in his laptop. The defendant then filed a motion to suppress the evidence police obtained through their use of this parallel device, arguing the search exceeded the scope of the warrant issued.

It was the defendant’s position that the tracking warrant police obtained authorized not the government, but Verizon Wireless, the carrier associated with his aircard, to track and locate the aircard. He argued that the warrant directed Verizon to assist the government by operating the tracking device and turning over information.
The government also stipulated that the tracking device it used sent signals to the defendant’s aircard that Verizon would not have sent in the normal course of its operation, meaning the government would not have found the defendant solely relying on Verizon. The government also admitted that it failed to disclose in its application for the warrant that “the mobile tracking device would capture signals from other cell phones and aircards in the area of Defendant’s apartment.” This was a “detail of execution” that the court in *Rigmaiden* said need not be specified. Though that court itself admitted the warrant was not “a model of clarity,” it still denied the defendant’s motion to suppress because the issuing judge found the requisite probable cause to authorize the use of a tracking device.

Following *Rigmaiden*’s lead, a New Jersey district court in *United States v. Tutis* held that the while it “might have been helpful to include the words ‘cell-site simulator’ in the warrant” it was not required under the Fourth Amendment. *Tutis* is distinguishable from *Rigmaiden*, however, because the government in *Tutis* did specifically describe the device’s capabilities in the warrant application. It provided that the only function of equipment is to obtain the listed unique identification numbers, and it also described how the technology would obtain data points. Since this sufficiently described how the technology operated, the court found it insignificant that the warrant did not explicitly refer to a “cell-site simulator.”

---

311 Id. at *20.
312 Id.
313 Id. at *19–*20.
315 Id. at *2.
316 Id. at *2.
317 Id. at *6.
But, courts that have taken a more thorough look at the high stakes implicated by Stingray searches and have held that the use of a cell-site simulator requires a search warrant “based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.”

In *State v. Andrews*, the court concluded that an order authorizing the use of a cellular tracking device to locate a suspect’s cell phone did not constitute sufficient judicial authorization to use a cell-site simulator. In *Andrews*, the police’s use of a cell-site simulator revealed information about the defendant’s residence, specifically, that the defendant’s cellphone, and logically the defendant himself, were inside. The court observed that cell site simulators can locate and track the movements of a cellphone and its user across both public and private spaces. While it acknowledged that police frequently do not know whether officers will find a target phone in a constitutionally protected space, it nonetheless found it impractical to create a rule that prohibited a warrantless search only retrospectively when the search resulted in locating the cellphone inside a home or another constitutionally protected area. This provides “neither guidance nor deterrence, and would do nothing to thwart unconstitutional intrusions.” For these reasons, the court held the government must disclose the manner of execution if it intends to use a cell-site simulator to satisfy the Fourth Amendment requirements.

Most recently, a court applied the exclusionary rule to suppress evidence police through the use of a Stingray in *United States v.*

---

319 Id. at 355. Police obtained a pen register order and a trap and trace order, which the court in *Andrews* held was not the functional equivalent of a warrant for a cell-site simulator. Id. at 358.
320 Id. at 348.
321 Id.
322 Id.
323 Id. at 350.
324 Id.
Lambis.\textsuperscript{325} DEA agents in Lambis had a warrant for the defendant’s cell-site location information (“CSLI”).\textsuperscript{326} The CSLI provided the agents with a specific intersection of target phone’s location.\textsuperscript{327} But, this did not identify the precise information that police needed—the defendant’s specific apartment building and thus where he was located—to make the arrest.\textsuperscript{328} So, officers used a Stingray device to obtain this information and subsequently uncovered narcotics in the defendant’s apartment.\textsuperscript{329}

The court in Lambis warned, and held that the original warrant application did not contemplate the use of a cell-site simulator, finding CSLI and cell-site similar generated location information not one in the same.\textsuperscript{330} The court rationalized that “if the Government had wished to use a cell-site simulator, it could have obtained a warrant,” adding “the fact that [the government] previously demonstrated probable cause and obtained a warrant for CSLI . . . suggests [it] could have obtained a warrant to use a cell-site simulator, if it had wished to do so.”\textsuperscript{331} The court concluded with a clear message: “[a]bsent a search warrant, the Government may not turn a citizen’s cell phone into a tracking device.”\textsuperscript{332}

In Patrick’s case, the warrant indicated that only location data was to be searched and obtained, not a search of the phone’s contents.\textsuperscript{333} If
the Stingray gathered information from the phone that went beyond his location, such a search of his phone would have been unauthorized, and “suppression of the additional information (which might have pinpointed Patrick’s location) would likely be required.”334 And the warrant in Patrick “authorize[d] the identification of the physical location of the target cellular phone,” in a context that implied that the service provider would release information that would then allow police to identify Patrick’s location.335 These were built-in qualifications that confined the grant of the warrant’s authority, as Chief Justice Wood explained, just like a physical limitation to the house, but not the shed, or vice versa, would do.336

Though the Court has understood the manner of the warrant’s execution to fall within the officer’s discretion, such cases call into question whether the judiciary can sufficiently protect Fourth amendment rights with an after-the-fact review. How police conduct a search impacts the constitutionality of the search, at least when it comes to searches that utilize specialized technology, as Kyllo held. Stingrays can depart greatly from other information gathering methods, both in function and in their level of intrusiveness. Leaving the entirety of the manner in an officer’s discretion in the traditional sense means an officer can get a warrant for one technology and then use a different form, like a dragnet, but still argue this fell within his discretionary power to decide the manner of execution. It is difficult to see how an ex post reasonableness assessment can sufficiently protect privacy rights when the damage has already been done, and with Stingrays, to a countless number of people.

To Judge Easterbrook’s surprise, a magistrate in the Northern District of Illinois recently imposed both ex ante and ex post restrictions on the government’s use of a Stingray device “to bring the surveillance into compliance with the Fourth Amendment.”337 The

334 Id. at 548.
335 Id.
336 Id.
337 Rachel Levinson-Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public, 66 EMORY L.J. 527,
judge was particularly concerned with the Stingray’s “inevitable collection of innocent third parties’ information.”\textsuperscript{338} It thus required the government to take three steps to limit the collection, retention, and use of the information gathered when it used the cell-simulator.\textsuperscript{339}

The first restriction indicated law enforcement “make reasonable efforts to minimize the capture of signals from cell phones used by people other than the target of the investigation.”\textsuperscript{340} The order also prohibited law enforcement from using the Stingray “when, because of the location and time, an inordinate number of innocent third parties’ information will be collected.”\textsuperscript{341} The second restriction directed law enforcement to delete all extraneous data, which is all data other than the data that identified the target’s cellphone, within 48 hours after its capture.\textsuperscript{342} The last restriction banned law enforcement from using any information beyond what was actually necessary to determine the target’s location.\textsuperscript{343} The court significantly noted “a cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization

\textsuperscript{338}\textit{In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed, 2015 WL 6871289, at *3.}
\textsuperscript{339}\textit{Id.}
\textsuperscript{340}\textit{Id.}
\textsuperscript{341}\textit{Id.} As examples, the court stated it would be inappropriate for law enforcement to use the Stingray near a large arena while a sporting event or high school graduation takes place. \textit{Id.}
\textsuperscript{342}\textit{Id. at *4.}
\textsuperscript{343}\textit{Id.}
from a fully informed court. Minimizing procedures... are necessary to protect the goals of the Fourth Amendment.  

The stress on a “fully informed court” falls directly in line with arguments made by both judges and scholarly commentators that government agents owe a “duty of candor” to judicial officers when presenting warrant applications.  

In United States v. Comprehensive Drug Testing, Inc., Chief Judge Kozinski, wrote a concurring opinion that offered guidelines to magistrates on how to deal with issuing search warrants for electronic data. The Chief Judge emphasized, “[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].” This duty, the kind that Patrick raised, would require the government to fairly disclose in a warrant application aspects of the process and the scope of the intended search, including the implications on third parties.

By not knowing (or caring) how the Stingray specifically conducted a search, the court in Patrick should not have taken the approach “less is enough.” Lambis and Andrews rejected point-blank that the use of a cell-site simulator was “close enough” to a warrant for cell-site location information, noting the many ways the two devices are different in kind. As Chief Judge Wood noted, the Seventh Circuit was likely not dealing with “two interchangeable tools

---

344 Id.  
347 Id.  
348 United States v. Patrick, 842 F.3d 540, 544 (7th Cir. 2016) (“This means that the police could have sought a warrant authorizing them to find Patrick’s cell phone and kept silent about how they would do it.”).  
for gathering exactly the same information.”

On the facts, the Seventh Circuit could not definitively provide an answer.

CONCLUSION

The Seventh Circuit in *Patrick* was undoubtedly presented with weighty questions. It confronted whether the use of a cell-site simulator Stingray device constitutes a search that falls within the Fourth Amendment and whether the Fourth Amendment requires the warrant to authorize specifically the use of such a device, all issues of first impression. Unfortunately, its analysis provided a painful bite at privacy rights. Though the Seventh Circuit got the first word, fortunately, it did not get the last.

The mystique surrounding Stingrays ultimately illuminates the harsh reality of this unregulated and technologically unmediated surveillance technology. As Chief Judge Wood pointed out, the government has gone so far as to dismiss cases, withdraw evidence, and negotiate lesser plea agreements rather than reveal that the technology was used.

Standing issues will continue to severely limit which law enforcement activities are challenged. As the court in *Patrick* briefly addressed, Patrick had no standing to challenge the Stingray search on the grounds that it was too broad: “if the problem with simulators is that they are too comprehensive, that would not lead to suppression—though it might create a right to damages by other persons whose interests were unreasonably invaded.” If the secrecy lingers, and courts decline to remand the issues for further fact finding, third

---

350 *Patrick*, 842 F.3d at 549 (Wood, C.J., dissenting).
351 *See generally* Pell & Soghoian, *supra* note 4. Police track thousands of cellphones every year, and generally, neither the target nor the public ever learns of a tracking order. Rothstein, *supra* note 30, at 491 (2012). Requests to track cellphones are sealed, and the judges who consider tracking requests rarely publish opinions. *Id.* In fact, “one federal magistrate judge has estimated that federal courts alone approve 20,000-30,000 tracking requests annually, and the number is rising.” *Id.*
352 *Patrick*, 842 F.3d at 546 (Wood, C.J., dissenting).
353 United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016).
parties will find it extremely difficult, if not impossible, to discover whether their information was collected.

This creates a paradoxical question: how can courts deter unlawful police conduct if those that have standing never know they have a viable claim? The uncomfortable reality is that if a Stingray search was unreasonably sweeping, those that have standing to invoke a Fourth Amendment claim will likely never know, because the defendant before the court likely does not have standing to explore the question. Indeed, a court will deem these issues as irrelevant unless the defendant can successfully allege the conduct violated his own constitutional rights. And since the Court does not extend the interest of the exclusionary rule’s deterrent function to unconstitutional police conduct affecting third parties, Stingrays that collaterally searched third parties’ phones and scooped up their data will proceed uncontested. The collection of innocent third party information unfortunately then becomes tolerable collateral damage.

The Seventh Circuit’s attitude in *Patrick* evokes questions of whether devices such as Stingrays should prompt a change in what a warrant requires, both in substance and in procedure, to satisfy the Fourth Amendment’s requirements. Judicial review after-the-fact is no longer an effective safeguard. The Stingray device, by its very nature, calls for greater supervision.

The solution may rest with the legislature. All three states within the Seventh Circuit, Illinois, Indiana and Wisconsin, now require police to get a warrant to conduct real-time cellphone tracking. Nine other states—California, Maine, Maryland, Minnesota, Montana, New Hampshire, Utah, Virginia, and Washington—require the same.

---

354 Id.
355 See 725 ILL. COMP. STAT. ANN. 168/10 (West 2017); IND. CODE ANN. § 35-33-5-12 (West 2014); WIS. STAT. ANN. § 968.373(2) (West 2014). Wisconsin’s statute was enacted in April of 2014, after the search in Patrick’s case, which occurred in October 2013.
356 CAL. PENAL CODE § 1546 (West 2017); ME. REV. STAT. tit. 16, § 648 (2014); MD. CODE ANN., CRIM. PROC. 1-203.1(b)(1) (West 2014); MINN. STAT. ANN. §§ 626A.28(3)(d), 626A.42(1)(d) (West 2014); MONT. CODE ANN. § 46-5-110(1)(a)
Still, courts should approach questions regarding Stingray searches with increased caution. As an initial matter, courts should find that the use of a Stingray is a search under the Fourth Amendment, which then triggers the requirements of a warrant supported by probable cause. To be clear, this Note does not question law enforcement discretion regarding the use of the Stingray nor does it pass judgment on the propriety of these devices as a matter of public policy. But, as Stingrays confirm, surveillance technology no longer operates in the clean vacuum as it once did, directed only at a target. Numerous third parties enter the equation with Stingrays. The manner in which police gather information now becomes relevant with Stingrays because the collection of the data itself can invoke a Fourth Amendment violation. Of course, this disclosure can vary on a case-by-case basis, but a judicial officer cannot protect who he or she does not know is vulnerable. With Stingrays, the manner of the search implicates constitutional rights in a way that information gathering methodologies in the past have not.

Ultimately, we know little about Stingray devices, and until more information surfaces, its veil of secrecy precludes courts from meaningfully resolving constitutional questions. Until then, the question remains, who is pinging your phone?