

Texas A&M Law Review

Volume 1 | Issue 3

2014

Kelsey Smith Act: An Analysis of the Warrantless Seizure of Cell Phone Locational Information in Emergency Situations

Maxwell B. Brown

Follow this and additional works at: https://scholarship.law.tamu.edu/lawreview



Part of the Law Commons

Recommended Citation

Maxwell B. Brown, Kelsey Smith Act: An Analysis of the Warrantless Seizure of Cell Phone Locational Information in Emergency Situations, 1 Tex. A&M L. Rev. 681 (2014).

Available at: https://doi.org/10.37419/LR.V1.I3.6

This Comment is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Texas A&M Law Review by an authorized editor of Texas A&M Law Scholarship. For more information, please contact aretteen@law.tamu.edu.

COMMENTS

KELSEY SMITH ACT: AN ANALYSIS OF THE WARRANTLESS SEIZURE OF CELL PHONE LOCATIONAL INFORMATION IN EMERGENCY SITUATIONS

By: Maxwell B. Brown

ABSTRACT

The Kelsey Smith Act mandates cell phone carriers to release locational information of their subscribers to law enforcement officials in emergency situations in the absence of a warrant. Further, the Act releases said carriers from liability when the aforementioned requests are made. Currently, nine states have enacted the Kelsey Smith Act. Prior to the existence of the Act, the carriers were required to make a good faith assessment of the emergency as well as the subsequent request by law enforcement officials. The Kelsey Smith Act is an attempt to create a more efficient means of accommodating the operational needs of law enforcement in times of emergency without improperly infringing on individuals' privacy rights.

This Comment aims to analyze the implications associated with the enacted legislation of the states that have adopted versions of the Kelsey Smith Act. More specifically, this Comment will examine whether privacy concerns are proper in light of the Act or whether they are without merit. In doing so, this Comment will provide relevant historical and background information associated with electronic communication; an examination of the most recent arguments disfavoring the Act; and a discussion of whether the operational needs of law enforcement have been properly balanced with cell phone service subscribers' individual privacy rights as provided by the United States Constitution.

TABLE OF CONTENTS

I.	Introduction	682
II.	TECHNOLOGICAL AND STATUTORY BACKGROUND	684
	A. Surveillance Technology Used by Law Enforcement	
	Officials	684
	1. Radio Communication	685
	2. Global Positioning System	685
	3. Overview of Cell-Site Location Information	
	B. Constitutional and Statutory Foundation of	
	Surveillance Technology	687
	1. Fourth Amendment	687

a. Katz v. United States: Reasonable	
Expectation of Privacy	(
b. Smith v. Maryland: Legitimate Business	
Purpose	(
2. Electronic Communications Privacy Act of 1986	
("ECPA")	
a. Historic Cell-Site Data	
b. Real-Time Cell-Site Data	
III. The Kelsey Smith Act	
A. Is the Kelsey Smith Act Constitutional?	
ECPA?	
a. Is There Conflict Preemption Between the	
Kelsey Smith Act and the ECPA?	
b. Is There Field Preemption Between the	
Kelsey Smith Act and the ECPA?	
c. The Kelsey Smith Act Is Not Preempted by	
the ECPA	
2. Are There Other Constitutional Issues Raised	
by the Kelsey Smith Act?	
IV. BALANCING COMPETING VIEWS	
A. Proponents Views	
B. Opponents Views	
C. More States Should Adopt the Kelsey Smith Act	
V. Conclusion	

I. Introduction

On June 2, 2007, Kelsey Smith was abducted in a department store parking lot in Overland Park, Kansas.¹ In an effort to locate the missing teenage girl, local law enforcement officials contacted Kelsey's wireless provider to obtain locational data associated with her cell phone.² Due to resistance by the wireless provider to disclose the information in the absence of a warrant, it took three days before the officers were able to retrieve the locational information.³ Only forty-five minutes after receiving the information, police detectives were able to locate Kelsey's body using a "cell phone ping."⁴ Kelsey was only eighteen years old at the time of her death.⁵

The abduction and murder of Kelsey Smith attracted substantial media coverage. Further, controversy arose as to what took law enforcement officials so long to retrieve the locational information from

^{1.} Alex Tresniowski, *Taken from Target*, People, at 72, 73, June 25, 2007 *available at* http://www.people.com/people/archive/article/0,,20061260,00.html.

^{2.} *Id*.

^{3.} *Id*.

^{4.} *Id*.

^{5.} *Id*.

her cell phone.⁶ In response to her death and the delayed receipt of Kelsey's cell phone records, Kelsey's parents proposed the Kelsey Smith Act, and it was signed into Kansas law on April 17, 2009.⁷ Today, versions of the law have been adopted by nine states: Kansas, Nebraska, New Hampshire, North Dakota, Hawaii, Tennessee, Minnesota, Missouri, and Utah.⁸

Prior to the development of the Kelsey Smith Act, law enforcement officials were required to obtain a warrant to receive cell phone records from wireless providers. In contrast, the Act *requires* telecommunications carries and commercial mobile service providers to release the location information of their users to local law enforcement officials *without a warrant* in emergency situations involving death or serious bodily injury. Additionally, the Act protects carriers and service providers from being sued in any court of law for providing the aforementioned information to law enforcement officials.

Proponents of the Act believe it creates a more time-efficient method to obtain vital information in emergency situations and could ultimately save lives. 11 Conversely, opponents question the Act's constitutionality. 12 For example, a lawsuit was recently filed in Missouri, the most recent state to enact the legislation, under the premise that the Act violates the Supremacy Clause of the United States Constitution. 13 More specifically, the complaint alleged that the law frustrates Congress's intent to provide a uniform system of privacy rights under the Electronic Communications Privacy Act of 1986 and prevents cell phone subscribers from bringing civil action against cell phone carriers, which directly conflicts with an individual's right to bring such an action under federal law. 14

This Comment aims to analyze the implications associated with the enacted legislation of the states that have adopted versions of the Kelsey Smith Act. The first part of the Comment will provide relevant technological and historical background information involved with

^{6.} See Abby Simons, Parents of Murdered Kansas Teen Lobby for Cell Phone 'Ping' Law, StarTribune, Feb. 18, 2010, available at http://www.startribune.com/politics/statelocal/84750807.html.

^{7.} Tresniowski, supra note 1, at 73.

^{8.} Cristina Corbin, *Mother of murdered teen pushes for law forcing cellphone carriers to release life-saving information*, Fox News (Apr. 13, 2013), http://www.fox news.com/politics/2013/04/13/mother-murdered-teen-pushes-for-law-mandating-cell-phone-carriers-to-release/.

^{9.} H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{10.} Id.

^{11.} See Corbin, supra note 8.

^{12.} See William Browning, Missouri Law Firm Challenges New Kelsey's Law YA-HOO! News (Aug. 29, 2012), http://news.yahoo.com/missouri-law-firm-challenges-kelsey-law-173200050.html.

^{13.} See Verified Complaint for Declaratory Judgment and Injunctive Relief, Hopwood v. Missouri, No. 12-CV-04238 (W.D. Mo. 2012) [hereinafter Hopwood Complaint].

^{14.} *Id*.

tracking and surveillance technology. First, an overview of the technology that is currently being used to locate wireless devices will be provided. Next, historical background detailing the constitutional and statutory foundation leading up to the Kelsey Smith Act will be discussed.

The second part of this Comment will examine the Kelsey Smith Act, focusing on the constitutional issues that may be raised in opposition to the Act. First, the Comment will look at the constitutionality of the Act in light of the lawsuit that was recently filed in Missouri. More specifically, the first section of the second part will attempt to determine whether the Kelsey Smith Act is preempted by the Electronic Communications Privacy Act of 1986 and is thus unconstitutional under the Supremacy Clause of the United States Constitution. Next, the existence of other constitutional issues associated with the Act will be discussed.

Finally, the third part of this Comment will discuss why more states should ultimately adopt versions of the Kelsey Smith Act. This Part will address the various policy considerations of both proponents and opponents of the Act. Specifically, the policy considerations will be balanced to determine that the benefits of the Kelsey Smith Act outweigh the privacy concerns raised by those opposed to the Act.

II. TECHNOLOGICAL AND STATUTORY BACKGROUND

A. Surveillance Technology Used by Law Enforcement Officials

In accordance with expansive technological developments, the methods used by law enforcement for tracking and surveillance have evolved through the years. For example, Kelsey Smith's body was found through law enforcement's utilization of her cell phone records. Upon receipt of the records, a technician was able to pinpoint a transmission tower and directed investigators to search 1.1 miles north of the tower. In approximately forty-five minutes Kelsey's body was successfully located.

However, the technology used to locate Kelsey's body is not without contest. The increasingly pervasive methods used for tracking and surveillance raise a number of concerns, including infringement on individual privacy rights.¹⁸ Further, on numerous occasions, legislation

^{15.} Vicky Newman, *New Law Will Help in Missing Person Cases*, News-Herald (Apr. 17, 2012, 8:43 AM), http://www.news-herald.net/story/13739.

^{16.} Kelsey Smith Cell Phone Records, Cell Phone Servs., https://sites.google.com/site/cellsphonesservices/my-forms (last visited Feb. 19, 2013).

^{17.} Mike Lear, *Bill Would Require 'Pings' of Missing Persons' Cell Phones*, Missourinet (Feb. 3, 2012), http://www.missourinet.com/2012/02/03/bill-would-require-pings-of-missing-persons-cell-phones/.

^{18.} Catherine Crump, Location Tracking After United States v. Jones: Continued Uncertainty Harms Americans' Privacy, Telecommunications Monitor (Aug. 8, 2012).

has changed to accommodate law enforcement's use of new technology. Accordingly, it is important to understand the history and development of the currently-used technology to analyze the issues that their use subsequently raises.

1. Radio Communication

For decades, law enforcement officials have been utilizing various forms of surveillance technology to facilitate searches of suspects and victims involved in criminal investigations.¹⁹ Initially, Congress defined "electronic tracking devices" as "one-way radio communication devices that emit a signal on a specific radio frequency."²⁰ In essence, the device defined by Congress was a beeper.²¹

The courts defined a beeper as, "a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver." The "beeper" emitted signals to a radio receiver, which would beep at various speeds based on movement. The "beeper" technology was used by law enforcement for many years; however, it eventually became obsolete due to the emergence of satellite-based tracking devices. ²⁴

2. Global Positioning System

Generally, satellite-based tracking devices involve GPS technology. Thitially developed for military use, GPS technology triangulates satellite signals to locate a specific target. That is, continuous emissions of various frequencies are sent to multiple satellites in order to determine the latitude and longitude of the target GPS receiver. In order to determine the specific location of a particular receiver, the locations of at least three satellites and the receiver's location in relation to those satellites must be identified. After determining this information, the receiver basically draws a sphere around the three satellites that were located. The three spheres intersect at two points, and the point of intersection is the exact location of the GPS receiver. This process is commonly referred to as "trilateration."

^{19.} See generally Stephen B. Wicker, Cellular Telephony and the Question of Privacy, 54 Communications of the ACM, no. 1, July 2011, at 88.

^{20.} S. Rep. No. 99-541, at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564.

^{21.} United States v. Knotts, 460 U.S. 276, 277 (1983).

^{22.} *Id*.

^{23.} *Id*.

^{24.} *Id*.

^{25.} Id.

^{26.} Marshall Brain & Tom Harris, *How GPS Receivers Work*, HowStuffWorks, *http://electronics.howstuffworks.com/gadgets/travel/gps.htm* (last visited Feb. 22, 2013). 27. *Knotts*, 460 U.S. at 277.

^{28.} See Tracy V. Wilson, How GPS Phones Work, HowStuffWorks, http://electronics.howstuffworks.com/gps-phone.htm (last visited Feb. 22, 2013).

^{29.} Id.

^{30.} Id.

Today, most mobile phones contain GPS receivers and are capable of receiving signals from GPS satellites.³² Accordingly, wireless carriers are usually able to accurately locate a specific device's location through the use of GPS trilateration.³³ For example, the United States Federal Communications Commission ("FCC") enacted a program called "enhanced 911" ("E911") requiring that all cell phones transmit its phone number and location when dialing 911.³⁴ Under the E911 program, the user's location is determined through utilizing the GPS technology that has been installed on almost all modern-day cell phones.³⁵ Thus, in essence, law enforcement officials have the potential ability to compel wireless carriers to disclose the locational information of specific cell phone users for investigative purposes. Similarly, wireless phone providers have access to records that are produced using cell-site location information.

3. Overview of Cell-Site Location Information

Cell-site tracking identifies the location of a wireless phone by pinpointing the specific cellular transmission towers that the phone is using.³⁶ Regardless of whether the cell phone is currently being used, it continuously sends signals, commonly known as "pings," to the nearest transmission tower and mobile switching center while the cell phone is turned on.³⁷ Upon receipt of locational data, the mobile switching center is able to route incoming calls and messages to the nearest transmission tower.³⁸

Additionally, wireless providers maintain detailed records of the data produced, primarily for the purposes of diagnostics and billing.³⁹ The records contain the calls that were made and received by wireless users and information regarding the specific transmission towers that were used.⁴⁰ Thus, wireless providers are able to track individual carriers based on the "pings" received by the switching center and entered into the customer's cell-site record.⁴¹

Similar to GPS, the data that accumulates from multiple transmission towers can triangulate to locate the latitude and longitude of a

^{31.} Id.

^{32.} Id.

^{33.} *Id*.

^{34.} *Id.* 35. *Id.*

^{36.} Lewis R. Katz, *Right of Privacy—E-mail, Instant Messaging, and Cell Phones*, Baldwin's Ohio Handbook Series Ohio Arrest, Search and Seizure § 1:17 (2012).

^{37.} Martin A. Dolan, et al., Chicago Bar Association, Use of Cell Phone Records and Gps Tracking, 24 CBA Rec. at 38, 39 (Jan. 2010).

^{38.} *Id*.

^{39.} See Declan McCullagh, Feds Push for Tracking Cell Phones, CNET News (Feb. 11, 2010), http://news.cnet.com/8301-13578_3-10451518-38.html.

^{40.} Id.

^{41.} Id.

specific wireless phone user.⁴² As described in the Kelsey Smith investigation, this method of tracking is capable of producing extremely accurate results.⁴³ Accordingly, its use by law enforcement during investigations is becoming increasingly more prevalent; as a result, legislatures are proposing and enacting laws to facilitate more efficient uses of the technology.

B. Constitutional and Statutory Foundation of Surveillance Technology

As technology's prevalence in our lives steadily increases with rapid new developments, the law too must increasingly develop to accommodate the issues that are raised as a result; however, it seems the former often outruns the latter. Since the development of radio frequency "beepers," police surveillance and tracking procedures have been subject to debate. Frequently, questions arise as to what is reasonable and what constitutes an invasion of privacy. Accordingly, states have adopted various statutes and regulations throughout the years in an attempt to clarify the acceptable methods and devices law enforcement officials may use during police investigations.⁴⁴

1. Fourth Amendment

The Fourth Amendment of the United States Constitution protects against "unreasonable searches and seizures" and states that warrants should not be issued "but upon probable cause."⁴⁵ Of course, the Amendment's language does not address telephone or electronic communication.⁴⁶ Thus, legal protection of telephone and electronic communication has been primarily based on judicial interpretation of the Fourth Amendment.

In 1928, the United States Supreme Court made the first significant telecommunications-surveillance decision in *Olmstead v. United States*,⁴⁷ a case involving wiretapping.⁴⁸ The Court held that police wiretapping did not constitute "search and seizure" because "evidence was secured by use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."⁴⁹ At this point, it is apparent that the Court maintained a narrow textual interpretation of

^{42.} See generally ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 81-85, 93-94 (2010).

^{43.} See Kelsey Smith Cell Phone Records, Cell Phone Servs., https://sites.google.com/site/cellsphonesservices/my-forms (last visited Feb. 19, 2013).

^{44.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012); 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2002).

^{45.} U.S. Const. amend. IV.

^{46.} Wicker, supra note 19, at 89.

^{47.} See generally Olmstead v. United States, 277 U.S. 438 (1928).

^{48.} Wicker, supra note 19, at 89.

^{49.} Olmstead, 277 U.S. at 464.

the Fourth Amendment, unwilling to depart from actual searches and seizures of tangible property. However, the holding in *Olmstead* was directly overturned by *Katz v. United States* in 1967.⁵⁰

a. Katz v. United States: Reasonable Expectation of Privacy

In *Katz*, the Court held that tapping phone calls from a phone booth required a police warrant because the Fourth Amendment protects "people, not places." Further, Justice Harlan established a two-part test in his concurring opinion to determine whether the Fourth Amendment is applicable.⁵² According to Harlan, the person must have: (1) "an actual (subjective) expectation of privacy" and (2) the expectation must be one that "society is prepared to recognize as 'reasonable'." Significantly, *Katz* was the first instance where the Court applied the Fourth Amendment to telephone calls.⁵⁴

b. Smith v. Maryland: Legitimate Business Purpose

In 1979 the court applied the *Katz* test in *Smith v. Maryland.*⁵⁵ In *Smith*, at the request of investigators, a telephone company installed a pen register, a device used to record the numbers dialed on a specific telephone line, at Smith's home and office.⁵⁶ The Court held that the pen register did not violate Smith's Fourth Amendment rights because "it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial."⁵⁷

The Court further explained that telephone users generally know that "they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes." Ultimately, the Court distinguished the privacy rights associated with the content of telephone calls from those relating to the context of telephone calls. Subsequently, this distinction was further defined when Congress passed the Electronic Communication Privacy Act of 1986.

2. Electronic Communications Privacy Act of 1986 ("ECPA")

The ECPA was enacted as a means of updating the Federal Wiretap Act of 1968, which only applied to the interception of conversations

```
50. See Katz v. United States, 389 U.S. 347 (1967).
```

^{51.} Id. at 351.

^{52.} Id. at 361.

^{53.} *Id*.

^{54.} Wicker, supra note 19, at 90.

^{55.} See generally Smith v. Maryland, 442 U.S. 735 (1979).

^{56.} Id. at 737.

^{57.} Id. at 735.

^{58.} *Id*.

^{59.} Wicker, supra note 19, at 91.

^{60.} Id.

made over actual telephone lines.⁶¹ In regards to electronic surveillance, the ECPA regulates three separate titles of surveillance.⁶² Title I, also known as the Wire Tap Act ("WTA"), concerns the interception of wire, electronic, and oral communications.⁶³ Title II, also known as the Stored Communications Act ("SCA"), concerns government access to "stored wire and electronic communications and transactional records."64 Finally, Title III concerns "pen registers and trap and trace devices."65

Further, there is much debate as to which of the three titles governs the information compiled by wireless providers.⁶⁶ Deciding which of the three titles governs is important because "it determines the legal burdens that law enforcement must overcome to obtain the data."67 For example, Title I generally requires a warrant for the disclosure of the content, whereas Title II allows law enforcement to obtain information by providing "specific and articulable facts" showing that the information is "relevant to an ongoing investigation," a significantly lower standard.⁶⁸ Moreover, Title III provides minimal legal protection. Title III requires only "that an attorney for the government certify that the information to be obtained is relevant to an ongoing criminal investigation."69

Additionally, this determination is in the end based on the type of information that is sought by law enforcement officials, that is, whether the information is historic cell-site location data or whether it is real-time cell-site location data.⁷⁰ Cell-site data is ordinarily classified as either historic or real-time data.⁷¹ Historic cell-site location data records consist of a list of the wireless subscriber's prior contact with various cellular transmission towers.⁷² In contrast, real-time cellsite location data, also known as prospective cell-site data, includes a continuous update of all the cellular towers contacted by a subscriber in "real-time." The distinction between the two types of cell-site location data is important in that it determines the appropriate burden that courts will apply to law enforcement officials when attempting to obtain the information during an investigation.⁷⁴ Ultimately, this de-

^{61.} U.S. Department of Justice, Privacy and Civil Liberties, http://www.it.ojp.gov/ default.aspx?area=privacy &page=1285 (last updated Mar. 21, 2012).

^{62.} See generally 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2006).

^{63.} *Id.* §§ 2510–2522 (2002). 64. *Id.* §§ 2701–2712.

^{65.} Id. §§ 3121-3127.

^{66.} Wicker, supra note 19, at 91.

^{67.} Id.

^{68.} *Id*.

^{69.} Id.

^{70.} Id.

^{71.} See id.

^{72.} Id.

^{73.} Id.

^{74.} Id.

termination depends on whether the courts consider cell phones to be tracking devices under the ECPA.⁷⁵

a. Historic Cell-Site Data

Title II of the ECPA "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses." Further, Title II generally covers historic cell-site data; that is, a list of the cell-sites or transmission towers visited by a particular wireless service subscriber. As stated above, in obtaining this information, Title II requires law enforcement to provide "specific and articulable facts," and they must show that the information needed is "relevant and material to an ongoing investigation." Thus, the burden for acquiring historic cell-site information is lower than the probable cause requirement for a warrant as described in Title I.

b. Real-Time Cell-Site Data

The majority of courts have found that real-time cell-site data does not constitute a "record" because it is not stored communication. These courts compared real-time data to the numbers dialed by the cell phone user, concluding that Title III of the ECPA should govern real-time data. As stated above, under Title III it is only required that "an attorney for the government certify that the information collected is relevant to an ongoing criminal investigation. In contrast, the minority of courts consider real-time data a record under the ECPA. Under the minority view, although real-time data is continuous, the wireless service providers still record the information prior to delivering it to law enforcement officials. Thus, the minority view considers a cellphone a tracking device that therefore should require a showing of probable cause to access real-time cell-site data. The debate over whether a standard less than probable cause is appropriate when attempting to obtain real-time data is ongoing.

^{75.} *See id*

^{76.} U.S. Department of Justice, *supra* note 61; 18 U.S.C. §§ 2701–2712.

^{77.} See In re Applications, 509 F. Supp. 2d 76 (D. Mass. 2007); In re Application, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007).

^{78. 18} U.S.C. § 2703(d).

^{79.} See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005).

^{80.} Wicker, supra note 19, at 91.

^{81.} *Id*.

^{82.} See, e.g., In re Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 445 (S.D.N.Y. 2005).

^{83.} *Id*.

^{84.} Wicker, supra note 19, at 91.

III. THE KELSEY SMITH ACT

Despite the relevant statutory foundation, the Kelsey Smith Act mandates wireless service providers to provide location-based data to law enforcement officials in emergency situations that involve the risk of death or serious bodily injury.⁸⁵ Specifically, the Act states:

Upon request, a telecommunications carrier or commercial mobile service provider as identified in 47 U.S.C. Section 332(d)(1) and 47 CFR Parts 22 or 24 shall provide call location information concerning the user of a telecommunications service or a wireless communications service, in an emergency situation to a law enforcement official or agency in order to respond to a call for emergency service by a subscriber, customer, or user of such service, or to provide caller location information (or do a ping locate) in an emergency situation that involves danger of death or serious physical injury to any person where disclosure of communications relating to the emergency is required without delay.⁸⁶

The Act further states:

No cause of action shall lie in any court of law against any telecommunications carrier or telecommunications service or commercial mobile service provider, or against any telecommunications service or wireless communications service, or its officers, employees, agents, or other specified persons, for providing any information, facilities, or assistance to a law enforcement official or agency in accordance with the terms of this section. Notwithstanding any other provision of law, nothing in this section prohibits a telecommunications carrier or commercial mobile service provider from establishing protocols by which such carrier or provider could voluntarily disclose call location information.⁸⁷

Thus, the Act ultimately provides an exception to the burdens imposed by ECPA in times of emergency.⁸⁸ However, the exception provided by the Act is not without contest, as seen by a recent Missouri complaint alleging that the Act is unconstitutional.⁸⁹

A. Is the Kelsey Smith Act Constitutional?

Recently, a lawsuit was filed in Missouri, the most recent state to adopt the Act, alleging that the Act is unconstitutional.⁹⁰ Subsequently, the plaintiff voluntarily dismissed the suit. However, as more and more states continue to enact similar amendments to the ECPA, an analysis of the plaintiff's original complaint will provide valuable insight to the various constitutional issues possibly raised in opposi-

^{85.} H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{86.} *Id*.

^{87.} Id.

^{88.} See id.

^{89.} Hopwood Complaint, supra note 13.

^{90.} Id.

tion to similar Acts in the future. Specifically, the complaint alleged that the Act violates the Supremacy Clause of the United States Constitution. The Supremacy Clause provides:

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, anything in the constitution or laws of any state to the contrary notwithstanding.⁹²

Further, "the Supremacy Clause prohibits state laws that conflict with federal law where congress has expressed an intent to regulate." Thus, it was the plaintiff's contention in the Missouri suit that the Kelsey Smith Act conflicted with the ECPA and was therefore preempted. 94

1. Is the Kelsey Smith Act Preempted by the ECPA?

A state law is preempted by federal law when the federal government has exercised its power to regulate, and there is either (1) a conflict or (2) a potential conflict between the federal law and the state law. Further, there are two types of preemption: express preemption and implied preemption. Express preemption occurs when preemptive statutory language is found; in other words, a federal statute explicitly confirms Congress's intent to preempt state law. Here, the ECPA does not appear to explicitly confirm the intent to preempt state laws concerning the privacy and disclosure of electronic and telecommunications records in emergency situations. Thus, the Court probably would not have found that the Kelsey Smith Act expressly preempted by the ECPA. However, the court may still find implied preemption in the absence of express preemption when there is either (a) conflict preemption or (b) field preemption.

a. Is There Conflict Preemption Between the Kelsey Smith Act and the ECPA?

A conflict is present when a party is unable to comply with both the state and federal laws in question. Further, even if an actual conflict does not exist, a conflict may be arise if the state law creates an obstacle to the accomplishment and execution of the full purposes and

^{91.} *Id*.

^{92.} U.S. Const. art. VI, cl. 2.

^{93.} Hopwood Complaint, supra note 13.

⁰⁴ Id

^{95.} See Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 89 (1992).

^{96.} Id. at 98.

^{97.} English v. Gen. Elec. Co., 496 U.S. 72, 79 (1990).

^{98.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{99.} Gade, 505 U.S. at 89.

^{100.} Florida Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142-43 (1963).

objectives of Congress.¹⁰¹ Thus, had the Missouri plaintiff not voluntarily dismissed the claim, she would have had to show one of two things for her claim to succeed: (1) compliance with both the ECPA and the Kelsey Smith Act was physically impossible; or (2) the Kelsey Smith Act stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress in enacting the ECPA.¹⁰²

In regards to the existence of an actual conflict, the plaintiff claimed the Kelsey Smith Act "makes it impossible for a phone company/provider to comply with the federal act, which states they may disclose records and location information, and the state law, which states they must disclose the information." Further, under 18 U.S.C.A. § 2702 of the ECPA, a telephone provider is given "discretion to provide the 'contents of a communication' to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." Whereas, the Kelsey Smith Act states, upon request by law enforcement, a telephone provider "shall" provide such information in situations involving an emergency situation that "involves danger of death or serious physical injury to any person." Thus, the plaintiff contended the Act eliminated any discretion given to the telecommunications provider in emergency situations by eradicating the ability of the provider to make a good faith evaluation of the request by law enforcement as provided by the ECPA.¹⁰⁶

Although the plaintiff alleged that the Act eliminated all discretion granted to telephone providers, after examining both regulations, this allegation does not appear to be accurate. For example, if an emergency situation does indeed exist but law enforcement does not make a request for locational information pertaining to the situation, the telephone company appears to retain discretion to voluntarily disclose such information to law enforcement.¹⁰⁷ Thus, the Kelsey Smith Act does not seem to eliminate any discretion to telephone providers as the plaintiff proposed; in actuality the Act only eliminates discretion in those situations where officers make a request for the information. Nonetheless, it logically follows that in an emergency situation, where a law enforcement official does indeed make a request upon the provider for locational information, compliance with both the Kelsey Smith Act and section 2702 of the ECPA would probably be physically

^{101.} Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 372-73 (2000).

^{102.} See Gade, 505 U.S. at 89.

^{103.} Hopwood Complaint, supra note 13 [emphasis added].

^{104.} Id.; see also 18 U.S.C. § 2702 (2012).

^{105.} H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{106.} Hopwood Complaint, supra note 13.

^{107.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

impossible. Moreover, section 2702 deals with voluntary disclosures by providers not requests for disclosure by law enforcement officials, and the Kelsey Smith Act explicitly states: "Nothing in this section prohibits a telecommunications carrier or commercial mobile service provider from establishing protocols by which such carrier or provider could voluntarily disclose call location information." Thus, the plaintiff probably did not have a claim that an actual conflict exists between the Kelsey Smith Act and the ECPA.

Additionally, in regards to creating an obstacle to Congress's purposes and objectives, the plaintiff contended that the Kelsey Smith Act "frustrates what seems to be the evident congressional intention to establish a uniform federal regime controlling when telecommunications records are disclosed and by whom." Further, the plaintiff's complaint stated the Act "frustrates the clear congressional intention to give a citizen the right to a civil action for violation of the privacy of their phone records." However, while it seems Congress did intend to create these two purposes in enacting the ECPA, it does not appear that they are necessarily frustrated by the Kelsey Smith Act as the plaintiff proposed. Rather, the Kelsey Smith Act may actually be interpreted to complement the ECPA.

Both the ECPA and the Kelsey Smith Act grant warrantless seizure of telephone records in emergency situations involving death or serious injury. The purpose of both section 2702 of the ECPA and the Kelsey Smith Act appears to be creating a quick and effective means of providing law enforcement with helpful information in life-threatening situations. However, in order to increase efficiency in emergency situations, the Kelsey Smith Act transfers discretion from telephone providers to law enforcement officials when a request is made. For example, after Kelsey had been abducted, it took her cell phone provider several days to release the locational information that ultimately led law enforcement to her body. Conversely, had there been a law in effect in Kansas similar to the Kelsey Smith Act, law enforcement would have been able to gain access to the locational information immediately, decreasing the amount of time it would have taken to locate her body.

Further, the delay that occurred in providing law enforcement with Kelsey's cell phone records was most likely the result of the phone company attempting to make a good faith evaluation of the situation to confirm the existence of an "emergency" as defined by the ECPA.

^{108.} Id.

^{109.} Hopwood Complaint, supra note 13.

^{110.} Id.

^{111.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012); 18 U.S.C. § 2702 (2012).

^{112.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{113.} Tresniowski, supra note 1, at 73.

In doing so, the provider was probably ensuring that they would not be held liable for releasing the information without a warrant. Because the Kelsey Smith Act ultimately eliminates the telephone providers' good faith evaluation in these situations, it is necessary that the providers be protected from suit as a matter of fairness.

Additionally, under section 2712 of the ECPA, any person affected by a violation "may commence an action in United States District Court against the United States to recover money damages."114 Therefore, even though the Act may prevent citizens from bringing a civil action against the telephone provider when law enforcement officials request disclosure in emergency situations, citizens are still afforded the opportunity to bring an action against the government. Likewise, as previously stated, the Act does not apply to voluntary disclosures by providers. 115 Accordingly, in situations where a provider voluntary discloses locational information to a governmental entity in violation of the ECPA, a citizen can bring a civil action against that provider. The purpose of the Kelsey Smith Act's provision protecting providers from liability is not meant to frustrate Congress's intent to give citizens a right to civil action if their privacy rights are violated. Rather, it is a means of furthering Congress's intent to provide law enforcement with a quick and efficient method to locate citizens in times of emergency.

b. Is There Field Preemption Between the Kelsey Smith Act and the ECPA?

Field preemption occurs when it is clear that Congress intended to have a federal law occupy a particular area of law through a scheme of federal regulation that is so pervasive as to reasonably conclude that Congress left no room for the states to supplement it. The complaint did not appear to claim that Congress left no room for the states to supplement the ECPA. However, as a matter of policy, it would be extremely difficult for Congress to establish field preemption in an increasingly dynamic area such as electronic and telecommunication privacy. Advances in technology occur at such a rapid pace in our society that it would nearly be impossible for Congress to keep up with these changes and the effects they have on individual privacy rights. Thus, it is reasonable to assume that Congress anticipated states would begin to supplement the ECPA as new technological advances arose.

^{114. 18} U.S.C. § 2712 (2002).

^{115.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{116.} Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 89 (1992).

^{117.} See Hopwood Complaint, supra note 13.

c. The Kelsey Smith Act Is Not Preempted by the ECPA

The Kelsey Smith Act will probably not be deemed unconstitutional under the Supremacy Clause of the United States Constitution. First, the ECPA does not contain an express provision preempting state laws that supplement the process of disclosing locational information to requesting law enforcement officers in emergency situations. 118 Second, the exception provided by section 2702 of the ECPA, requiring providers to make a good faith evaluation before disclosing locational information to law enforcement, pertains to voluntary disclosures—not to disclosures upon request; therefore, there does not appear to be an actual conflict between the Kelsey Smith Act and the ECPA.¹¹⁹ Third, the Kelsey Smith Act does not frustrate Congress's intent to provide a uniform standard for when and to whom disclosures are made; nor does the Act attempt to frustrate Congress's intent to provide citizens with civil remedies in the occurrence of a violation. 120 Rather, the Act advances Congress's intent to make locational information readily available in emergency situations through a more efficient process.¹²¹ Finally, due to the ever-expansive field of technology, it seems unreasonable to assume Congress intended to include every aspect of electronic communication privacy in the ECPA so as to occupy the entire field and prevent the states from supplementing the Act.

2. Are There Other Constitutional Issues Raised by the Kelsey Smith Act?

Despite the possibility that the Kelsey Smith Act is federally preempted by the ECPA, some opponents of the Act may attempt to argue that the Kelsey Smith Act is unconstitutional under the Fourth Amendment of the United States Constitution; however, this claim is without merit. The Fourth Amendment establishes "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Further, as discussed above, there is still much debate as to whether the Fourth Amendment applies to cell phone locational information as well as what procedural hurdles law enforcement officials must jump through to obtain certain types of data under the ECPA. 123

However, in regards to searches and seizures under the Fourth Amendment not pertaining to cell phone data, the courts have ruled that warrantless searches and seizures are nonetheless valid in emer-

^{118.} See 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127.

^{119.} Id. § 2702.

^{120.} See H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

^{121.} Id.

^{122.} U.S. Const. amend. IV.

^{123.} See Wicker, supra note 19, at 91.

gency situations.¹²⁴ For example, in *Mincey v. Arizona*, the Court stated that "the Fourth Amendment does not bar police officers from making warrantless entries and searches when they reasonably believe that a person within is in need of immediate aid."¹²⁵ Furthermore, in regards to warrantless searches, the court in *Wayne v. United States* stated, "The need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency."¹²⁶ Likewise, as previously discussed, it appears that Congress intended to provide an exception to obtaining a warrant for cell phone data in emergency situations in the ECPA.¹²⁷ Thus, it follows that regardless of whether or not the Fourth Amendment applies, the Kelsey Smith Act will not be held unconstitutional when it deals solely with obtaining locational information in emergency situations involving death or serious injury.

IV. BALANCING COMPETING VIEWS

Although it appears that the Kelsey Smith Act is constitutionally valid, the question remains as to whether more states should adopt the Act. The primary goal in adopting legislation that allows law enforcement officials to obtain locational cell phone information without a warrant is to find a balance between the operational needs of law enforcement and individual expectations of privacy. For almost a decade, warrantless seizures of cell phone data have been the subject of much debate. Further, the debate has become increasingly more relevant with the integration of "smart phones" into our daily lives. Today, our cell phones contain extremely personal information including website search histories, emails, pictures, text messages, and locational information. In addition, because cell phones commonly contain extremely intimate personal information, it is important that the pros and cons of each piece of legislation regarding the seizure of these devices are balanced carefully before adopting said legislation.

A. Proponents Views

Proponents of the Kelsey Smith Act believe that the Act provides an effective and necessary tool for law enforcement officials to locate missing persons in emergency situations.¹²⁹ Prior to the enactment of the Act, in states such as Kansas, Missouri, and Tennessee, law enforcement could obtain only a "ping" location on a victim's cell phone

^{124.} Mincey v. Arizona, 437 U.S. 385, 292 (1978).

^{125.} *Id*

^{126.} Wayne v. United States, 318 F.2d 205, 212 (D.C. Cir. 1963).

^{127.} See 18 U.S.C. § 2702 (2002).

^{128.} See Eric Lichtblau, Wireless Firms Are Flooded by Requests to Aid Surveillance, N.Y. Times (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all.

^{129.} See Browning, supra note 12.

if the victim had initially called 911.¹³⁰ The FCC governed these "ping" locates through the E911 rules.¹³¹ Any other request would require a warrant, which could often take days to obtain.¹³²

E911 regulations require cellular service providers to provide certain minimum pieces of information to 911 operators to ensure that the operator is able to locate the cell phone making the emergency call. More specifically, the E911 rules require cellular service providers to give 911 operators "the location of 911 calls by longitude and latitude," which is normally determined using GPS technology. However, in emergency situations where no 911 calls are made, such as in the abduction of Kelsey Smith, law enforcement officials were required to obtain a warrant before seizing cell-site data from cellular providers in compliance with the ECPA.

Thus, proponents argue that the Kelsey Smith Act fills this void, providing law enforcement with important locational information, in the absence of a 911 call or a warrant, which could ultimately cut down response time and save lives. In support of this argument, proponents focus on the criticalness of the first hours of the abduction. For example, in a 2006 Child Abduction Murder Study, the Criminal Division of the Washington State Office of the Attorney General reviewed over seven hundred cases and found that "in 76 percent of the missing children homicide cases studied, the child was dead within three hours of the abduction—and in 88.5 percent of the cases the child was dead within twenty-four hours." Therefore, proponents believe the Act ultimately cuts down the response time in such emergencies by providing law enforcement officials with the ability to quickly retrieve extremely accurate locational information.

Additionally, proponents argue that cell-phone company employers do not train their employees as to whether a particular situation constitutes an emergency. According to Overland Park, Kansas¹³⁸ Police Chief John Douglass, a cell-phone provider's job is to make money, whereas, law enforcement's job is to protect and rescue people when

^{130.} Kelsey Smith Act Would Help Locate Crime Victims Through Cell Phone Technology, Tennessee Republican Senate Caucus (Mar. 9, 2012), http://www.tnsenate.com/_blog/Newsroom/post/Kelsey_Smith_Act_would_help_locate_crime_victims_through_cell_phone_technology/ [hereinafter Tennessee Senate].

^{131.} See 47 C.F.R. § 20.18 (2012).

^{132.} Tennessee Senate, supra note 130.

^{133.} *Id*.

^{134.} Id. § 20.18(f).

^{135.} See Tennessee Senate, supra note 130.

^{136.} Corbin, supra note 8.

^{137.} Criminal Division of the Washington State Office of the Attorney General, 2006 Child Abduction Murder Study, Child Abduction Murder Research, http://www.atg.wa.gov/ChildAbductionResearch.aspx#.UQhknTk_5UQ (1993).

^{138.} Overland Park, Kansas is the city where the abduction of Kelsey Smith occurred on June 2, 2007.

it is necessary.¹³⁹ Thus, proponents ultimately argue that law enforcement officials are more competent to make a determination of an emergency situation than are cell-phone company employees, and the Kelsey Smith Act properly places this discretion into law enforcement's hands.

B. Opponent Views

In contrast, opponents argue that the Act raises privacy concerns under the Fourth Amendment of the United States Constitution, and that the Act prevents cell phone customers from filing suits against cell-phone companies for making improper disclosures. However, as discussed above, emergency situations generally constitute exceptions to obtaining a warrant under the Fourth Amendment. For example, even privacy advocates such as the ACLU have stated that "in certain emergency situations, for example to locate a missing person, tracking a cell phone without a warrant is acceptable." Nonetheless, opponents may be skeptical that enacting legislation such as the Kelsey Smith Act will begin to pave the way for more and more warrantless searches and seizures of cell phone information and will therefore create what is commonly referred to as a "slippery slope."

In addition, the potential for abuse by law enforcement officials raises concerns with many privacy advocates.¹⁴³ According to an accounting of responses by wireless carriers, Congressman Ed Markey found state and local law enforcement agencies made more than 1.3 million requests of wireless carriers for the cell phone records of consumers.¹⁴⁴ Thus, based on the sheer volume of requests made by law enforcement officials, it is easy to see the potential for abuse. For example, a law enforcement official could falsely claim to be acting in response to an emergency to obtain valuable information about a criminal suspect in the absence of a warrant. Likewise, the accountings reported a large number of the requests made by law enforcement official were for "cell tower dumps." "Cell tower dumps"

^{139.} Browning, supra note 12.

^{140.} See Corbin, supra note 8; see also Hopwood Complaint, supra note 13.

^{141.} See Mincey v. Arizona, 437 U.S. 385, 292 (1978).

^{142.} American Civil Liberties Union, *Cell Phone Location Tracking Public Records Request*, Protecting Civil Liberties in the Digital Age (Sept. 10, 2012), http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public -records-request.

^{143.} See Éric Lictblau, Police Are Using Phone Tracking as a Routine Tool, N.Y. Times (Mar. 31, 2012), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cell phones-raises-privacy-fears.html?_r=1&pagewanted=all.

^{144.} Eric Lietblau, Wireless Firms are Flooded by Requests to Aid Surveillance, N.Y. Times (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all.

^{145.} See David Kravets, Mobile-Phone Surveillance by Police Targets Millions Annually, Wired (July, 9 2012), http://www.wired.com/threatlevel/2012/07/massive-phone-surveillance/.

occur when cell-phone carriers provide all the phone numbers of cell-phone users that connect with a specific cell tower at a particular time, including innocent people who are uninvolved with the crime or emergency for which the request was made. Such practices raise privacy concerns as to how law enforcement officials differentiate between the records of innocent people and those that are subject to the investigation, as well as how they handle, administer, and dispose of the information. At the control of the information.

C. More States Should Adopt the Kelsey Smith Act

As stated above, there must be a balance between the operational needs of law enforcement and individual expectations of privacy. Here, the Kelsey Smith Act seems to do a very good job of balancing the two interests. The law is narrowly tailored in furtherance of citizen safety in emergency situations. Additionally, the law successfully fills a void that was not anticipated by Congress at the time the ECPA was enacted.

However, the law should further define the process of obtaining and later disposing of locational information. That is, the procedural methods should be specifically defined rather than merely stating that carriers "shall provide call location information." Doing so dismantles many of the privacy advocates' concerns. Ultimately, the Act appears to be constitutionally valid, and it appears to provide an efficient manner by which law enforcement officials are able to obtain important information in emergency situations. Therefore, more states should consider adopting the Kelsey Smith Act.

V. Conclusion

After careful review, it appears that the Kelsey Smith Act is constitutionally valid. First, the ECPA of 1986 does not appear to preempt the Act. That is, the Act does not create an obstacle to the accomplishment and execution of the full purposes and objectives of Congress. Therefore, the recent Missouri lawsuit is meritless. Second, the Act does not appear to violate the Fourth Amendment of the United States Constitution. The courts generally acknowledge emergency situations as an exception to obtaining a warrant to conduct a search or seizure under the Fourth Amendment.

Additionally, more states should probably adopt the Act as a means of taking advantage of technological advancements to ensure the safety of constituents. For example, as stated above, when a person is

^{146.} Jeffrey Brown, What Type of Process Is Required for a Cell Tower Dump?, CYBERCRIME REVIEW (May 16, 2012), http://www.cybercrimereview.com/2012/05/what-type-of-process-is-required-for.html.

^{147.} See Kravets, supra note 145.

^{148.} H.B. 1108, 96th Gen. Assemb., 2d Reg. Sess. (Mo. 2012).

abducted, the first hours are very critical to the successful recovery of the abductee. In the case of Kelsey Smith, her chances of survival would most likely have been greater if the Act was in place at the time of her abduction. The Act ultimately gives law enforcement officials the ability to determine whether a situation constitutes an emergency. Thus, it makes more sense to give this burden to officials who deal with emergency situations on a daily basis rather than cell phone carriers who are in the business of making money, not saving lives. However, states should be cautious in drafting similar legislation and include the entire process associated with accessing the locational information in order to prevent infringement upon individual privacy rights. The impact of cell phone surveillance on users is becoming increasingly important as the cellular platform continues to play a significant role in social, economic, and political contexts.¹⁴⁹ When analyzing the impact of a law that allows an exception to the probable cause and warrant requirements of the Fourth Amendment of the United States Constitution, as does the Kelsey Smith Act, the government interests, such as crime prevention and officer safety, should always be balanced against individual privacy rights. Legislators should draft any legislation using cellular technology with extreme caution because such technology is becoming more and more personally invasive.

^{149.} Wicker, supra note 19, at 98.