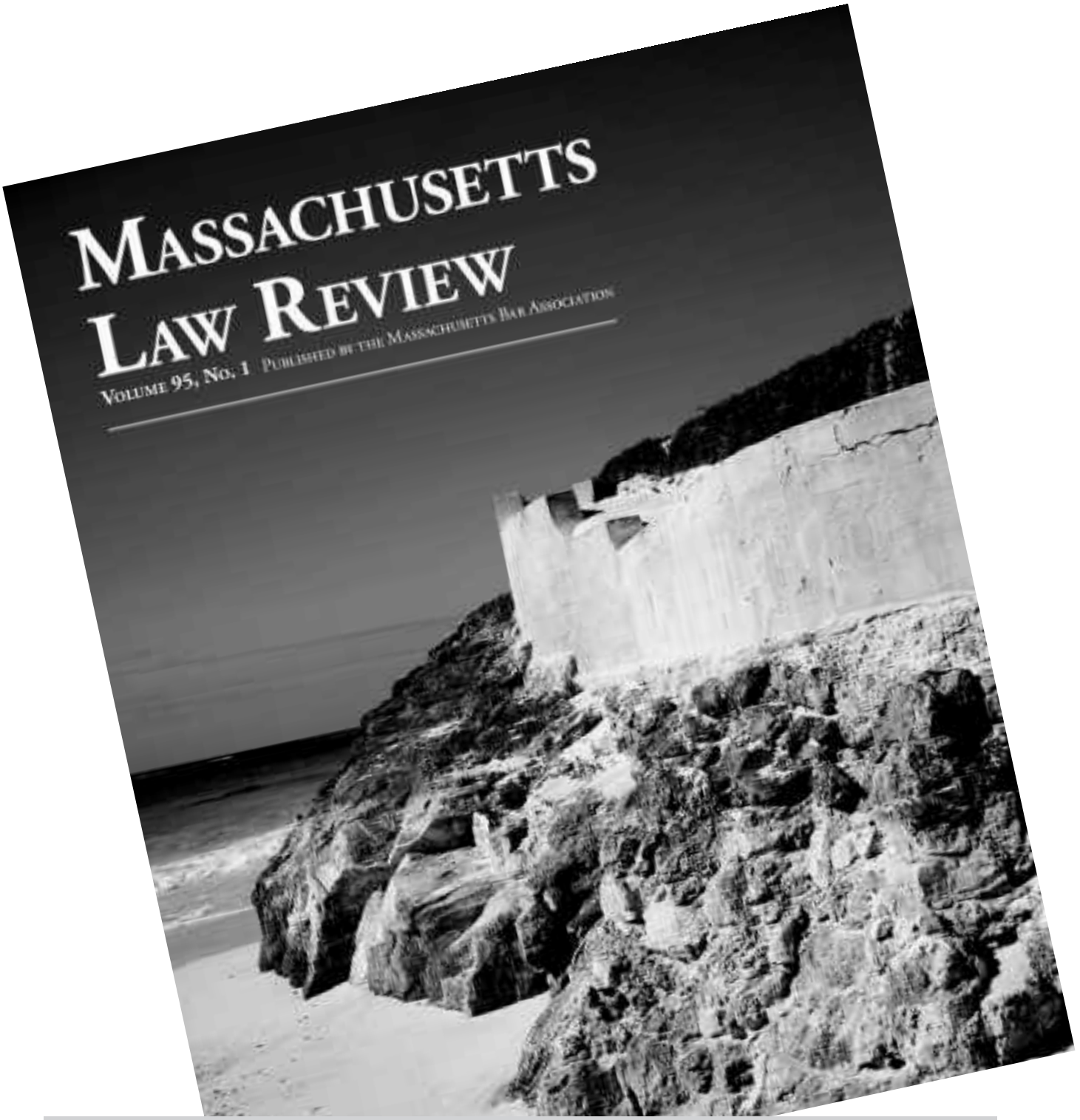
Massachusetts Law Review

Volume 98, No. 3 Published by the Massachusetts Bar Association



Massachusetts Law Review seeks submissions

The Massachusetts Bar Association is seeking submissions for its quarterly publication, the *Massachusetts Law Review*, the longest continually run law review in the country. A scholarly journal of the MBA, the *Massachusetts Law Review* is circulated around the world and contains comprehensive analyses of Massachusetts law and commentary on groundbreaking cases and legislation. To submit articles or proposals for articles, email JScally@MassBar.org, mail to *Massachusetts Law Review*, 20 West St., Boston, MA 02111 or call (617) 338-0682.

Massachusetts Law Review

VOLUME 98 NUMBER 3

April 2017

IN THIS ISSUE

The Massachusetts Law Review is supported in part by the Massachusetts Bar Association Insurance Agency

Cover: A stairwell in the Brooke Courthouse. Photo by Hon. David S. Ross.

MASSACHUSETTS BAR ASSOCIATION
20 WEST STREET, BOSTON, MA 02111-1204

Massachusetts Law Review (ISSN 0163-1411) is published quarterly by the Massachusetts Bar Association, 20 West Street, Boston, MA 02111-1204. Periodicals postage paid at Boston, MA 02205. Postmaster: Send address changes to Massachusetts Bar Association Member Services Center, 20 West Street, Boston, MA 02111-1204.

Subscriptions are free for members and are available to libraries at $50 and those not eligible for membership in the Massachusetts Bar Association at $75 per calendar year. Single copies are $25.

Case notes, legislative notes, book reviews, and editorials are generally prepared by the Board of Editors or designated members of the Board of Editors of the *Review*. Feature articles are generally prepared by authors who are not members of the board. The selection of feature articles for publication by the Board of Editors does not imply endorsement of any thesis presented in the articles, nor do the views expressed necessarily reflect official positions of the Massachusetts Bar Association unless so stated. MBA positions are adopted by vote of the association's Board of Delegates or Executive Committee. Proposed feature article contributions or outlines of proposed feature article contributions should be sent to Director of Media and Communications Jason Scally at jscally@massbar.org or to *Massachusetts Law Review*, 20 West St., Boston, MA 02111-1204. Unsolicited materials cannot be returned.

Commonwealth v. Augustine: The Supreme Judicial Court's Misapplication of Jurisprudence to Technology

by Owen Murphy

I. INTRODUCTION

As technology constantly develops, courts applying Fourth Amendment and Article 14 jurisprudence must balance each new technology's legitimate law enforcement uses with the threats that government use of it poses to individual privacy rights. Recently, courts have grappled with the use of electronic devices that can be used to track a target's location. The significance of that issue has grown exponentially due to the prevalence of cell phones, which can be tracked, not only in real time, but historically, through Cell Site Location Information (CSLI).

Whenever a cell phone is powered on, it connects to a tower within a cellular service provider's network. For business purposes, cellular service providers create call detail records, which include CSLI. CSLI can include documentation of which cell site a phone connected to when it engaged in a call or text message. As a result of this data collection, the date, time and tower(s) to which the phone connected in the course of a communication are recorded and maintained by the provider.

The Supreme Judicial Court recently analyzed the constitutional implications of this practice in *Commonwealth v. Augustine*.[1] It held that the defendant had a reasonable expectation of privacy in two weeks of CSLI records which were maintained by his cellular service provider.[2] As a result, the court concluded that Article 14 of the Massachusetts Declaration of Rights protected the data, and thus, that the commonwealth was required to procure a warrant before obtaining those CSLI records.[3] In reaching this decision, the court found that the Stored Communications Act,[4] a federal statutory scheme that governs when a warrant is required to obtain documents from a cellular service provider, did not provide protection commensurate with that of Article 14.[5] The court further reasoned that, although CSLI is a business record, the third-party exception to the warrant requirement was not applicable.[6]

This article examines the *Augustine* decision and similar decisions from other jurisdictions. First, it compares CSLI to the Global Positioning System (GPS), a precise and contemporaneous location technique previously analyzed by the Supreme Judicial Court and the United States Supreme Court. It then discusses the Federal Stored Communications Act,[7] which provides the federally-mandated procedure that the government must follow when obtaining CSLI from cell service providers. Next, the article examines the reasoning of the Supreme Judicial Court and United States Supreme Court in pre-*Augustine* decisions that analyzed electronic tracking issues and pronounced the contours of the privacy right in location. The article argues that, in the *Augustine* decision, the court unduly conflated CSLI with GPS tracking, and, in doing so, dramatically expanded the contours of the privacy right that it had established in earlier opinions. Drawing on the *Augustine* dissent, the article criticizes the court's attempt to justify its departure from the traditional third-party doctrine search warrant exception. Ultimately, the article concludes that the court should approach future concerns posed by developing technology with more technical understanding and judicial restraint.

A 2012 Boston College Law School graduate, Owen Murphy has served as a prosecutor in Massachusetts and, currently, at the Rhode Island Attorney General's Office. Much of his work, including both appellate and trial court matters, focuses on cyber crime, such as the Michelle Carter homicide case. He is presently a master's degree candidate in the Harvard Extension School's Software Engineering program, concentrating in cyber security.

II. TECHNICAL BACKGROUND

A. Cell site location information

Cellular networks service large geographic areas, which they divide into smaller coverage areas, named cells.[8] The division allows a network to reuse the limited number of radio frequencies and thus permits it to support a larger number of calls.[9] Put otherwise, a

1. 467 Mass. 230 (2014).
2. *Id.* at 254.
3. *Id*. at 255.
4. Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§2701-2712 (1986).
5. *Augustine*, 467 Mass. at 236, 244.
6. Commonwealth v. Augustine, 467 Mass. 230, 249-52 (2014).
7. 18 U.S.C. §§2701-2712 (1986).
8. Wayne Jansen & Rick Ayers, *Guidelines on Cell Phone Forensics,* Special Publication 800-101, at 7, National Institute of Standards and Technology (2007)(hereinafter "*Cell Phone Forensics*") available at www.crime-scene-investigator.net/GuidelinesCellPhoneForensics.pdf.
9. *Id.*; Mark Eckenwiler, *Electronic Communications Privacy Act (ECPA, Part 2): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 50, at 43 (April. 25, 2013) (testimony of Professor Matt Blaze) (hereinafter "Blaze Testimony") available at https://judiciary.house.gov/_files/hearings/113th/04252013/Eckenwiler%2004252013.pdf.

number of cells are each serviced by specific sets of equipment that can each use the limited amount of available radio frequencies. For relevant purposes, the equipment exists on three levels.[10] The first level is the cell site, or tower, which is equipped with the radio transceiver equipment that communicates with mobile phones.[11] A series of cell sites are managed by a controller, which governs the transceiver equipment and performs channel assignment.[12] Last, there is a switching system which manages a group of controllers.[13]

The number and location of the towers vary based on the volume of cell phone use in a given area.[14] For instance, densely populated areas that experience high call volume generally have more towers, which results in the towers being closer to each other.[15] As a result, phones in those areas are, on average, closer to the towers to which they connect.[16] A tower's radio transceiver can be configured in a variety ways. Most typically, the transceivers are divided into three 120-degree sectors: 0 degrees North to 120 degrees Southeast, 120 degrees Southeast to 240 degrees Southwest, and 240 degrees Southwest to 360 degrees North.[17] The signal radius of an individual tower is thus generally subdivided into three specific sectors.

The switching station manages the overall network communications.[18] In doing so, it relies on several databases, including the Home Location Register. That database contains subscriber account information, such as a subscriber's billing address, as well as information pertinent to network connectivity, such as the location of a phone when it last registered within the network.[19] The switching station uses this information to route calls and messages and to generate CSLI records.[20]

When a phone is powered on, it registers — relays its location — with the nearest tower about every seven seconds.[21] When the phone makes a transmission, the switching system, on the basis of the registration data, locates the phone and directs it to the nearest tower.[22] During a call, when a phone moves from an area covered by one tower to that covered by another, the phone is transferred, or "handed off," to the closer tower.[23]

In order to identify the patterns of cell phone use for business purposes, carriers store call location data for varying periods of time.[24] Those records, which are based on CSLI, ordinarily identify the transmitting cellular tower at two points: the commencement of the call and the termination of the call.[25] This information reflects not only which tower the phone connected to, but, in most instances, the particular 120-degree sector of that tower.

B. The differences between CSLI and GPS

Using historical CSLI data to locate when and where a call took place is distinct from GPS tracking.[26] The latter technique leverages a phone's global positioning capability to locate its precise whereabouts.[27] CSLI records, in contrast, are the product of network-based location,[28] which yields imprecise location information, namely the direction of where a phone was in relation to the tower with which it connected. Typically, CSLI will show the tower nearest to a phone at the time it connected.[29] It is possible, however, that at the time of the transmission, the nearest tower was unavailable. This can take place for a number of reasons, such as when a physical object is blocking the nearest tower's signal, or if heavy call volume requires the switching station to direct the call to a more distant tower with available radio frequencies.[30]

Network-based location, and therefore CSLI, is not as precise as GPS. As towers continue to be installed, however, CSLI precision increases.[31] Specifically, more towers result in smaller coverage areas, and, in turn, a reading of which phone a tower connected to will generally provide a more precise record of where the phone was located. As a result, future call detail records might contain more precise location information.[32] In fact, some service providers have experimented with extremely localized cell sites, which cover geographic areas as small as an individual home or office.[33] Although the saturation point of this trend is unclear, it is possible that, at some unknown time, CSLI might show that a call was placed from a specific building.

As it relates to call detail records, however, even more precise CSLI would still be distinct from GPS tracking. A more precise record of where a phone was when it placed a call is different than a history of where a phone traveled throughout the course of time. As

10. *See Cell Phone Forensics, supra* note 8, at 7-8.
11. *Id.*
12. *Id.*
13. *Id.*
14. Commonwealth v. Princiotta, 31 Mass. L. Rep. 68, at *6 (2013) (*citing* In re Application of the United States, 747 F. Supp. 827, 831 (S.D. Tex. 2010)).
15. *Id.*
16. *Id.*
17. *Cell Phone Forensics, supra* note 8, at 8.
18. *Id.*
19. *Id.*
20. *Id.*
21. Commonwealth v. Princiotta, 31 Mass. L. Rep. 68, at *6 (2013) (*citing* Kevin McLaughlin, *The Fourth Amendment and Cell Phone Tracking: Where Are We?*, 29 Hastings Comm. & Ent. L.J. 421, 426 (2006-2007)).
22. *Id.* (*citing* In re Application of the United States, 747 F. Supp. 827, 831 (S.D. Tex. 2010)).
23. *Id.*
24. *Id.* at *4. Some carriers publish their policies on location-based services. T-Mobile's policy, for example, states:

> Our network detects your device's approximate location whenever it is turned on (subject to coverage limitations). This location technology makes the routing of wireless communications possible, and is also the basis for providing enhanced emergency 9-1-1 service which permits us to provide your general location to a public safety answering point, emergency medical provider, or emergency dispatch provider. We may also use this technology to disclose, without a user's consent, the approximate location of a wireless device to a governmental entity, or law enforcement authority when we are served with lawful process or reasonably believe there is an emergency involving risk of death, or serious physical harm.

Id. at *9.
25. *Id.* at *7.
26. Blaze Testimony, *supra* note 9, at 50-51.
27. *Id.*
28. *Id.* at 52-53.
29. *Id.*
30. *See, e.g.,* Wilson Electronics, *The Top 5 Things That Block Your Cellular Signal* (Jan. 8, 2013), www.wilsonelectronics.com/uploads/files/164_The_Top_5_Things_That_Block_Your_Cellular_SignalL.pdf (last visited May 21, 2015).
31. Blaze Testimony, *supra* note 9, at 44.
32. Commonwealth v. Augustine, 467 Mass. 230, 253 (2014).
33. Blaze Testimony, *supra* note 9, at 43-44.

the *Augustine* dissent observed:

> There are at least two different types of [CSLI]. Telephone call CSLI … provides the approximate physical location (location points) of a cellular telephone *only* when a telephone call is made or received by that telephone. Registration CSLI … provides the approximate physical location of a cellular telephone every seven seconds unless the telephone is "powered off," regardless of whether any telephone call is made to or from the telephone. Telephone call CSLI is episodic; the frequency of the location points depends on the frequency and duration of the telephone calls to and from the telephone. Registration CSLI, for all practical purposes, is continuous, and therefore is comparable to monitoring the past whereabouts of the telephone user through a global positioning system (GPS) tracking device on the telephone, although it provides less precision than a GPS device regarding the telephone's location.[34]

Ultimately, even substantial increases in localization of cell towers would not result in CSLI tracking comparable to GPS tracking, because CSLI is recorded only when a telephone call occurs.

Although carriers have the ability to record registration data, that is not their current practice. Whether they will do so in the future remains unclear. On the one hand, the business value of that information is limited because carriers are generally interested in where people use their phones and thus where coverage needs to improve.[35] Where a phone travels throughout the course of a day seems to be an ancillary consideration.[36] Second, because of the volume of phones and the fact that registration occurs every seven seconds, it might be impractical for a network to store all signal communications for every phone.[37] On the other hand, there is some belief that precise tracking data might be useful for network management and advertising.[38] In any event, regardless of whether network carriers begin to record registration information, there is no reason to surmise that they would insert that information into the call detail records sought by law enforcement.

C. Other location techniques

There are at least two techniques which can be used to locate the precise location of a cell phone. First, a cell service provider can locate a phone on its network through a "ping."[39] Pinging a phone involves locating it through its GPS capabilities.[40] Hence, a ping will reveal a phone's specific location. A ping occurs when a service provider sends a signal to a particular cell phone, requesting the phone to respond with its GPS coordinates. Thus, although a ping requires the use of a cell tower, the location of a cell tower is only incidentally related. In other words, the information obtained consists of specific coordinates, not a tower that the phone was connected to at the time of a ping.[41]

With older analog cell phones and other non-GPS capable phones, the network provider can use triangulation to determine the location of a cell phone within an accuracy of about a hundred feet. Triangulation involves using multiple towers to communicate with a phone and then comparing the relative signal strength of those towers.[42]

III. THE STORED COMMUNICATIONS ACT

As part of the Electronic Communications Privacy Act of 1986,[43] the federal government passed the Stored Communications Act (SCA).[44] The SCA strives to achieve balance between an individual's reasonable expectation of privacy under the Fourth Amendment and the government's need to procure information necessary for the investigation and prosecution of criminal and national security matters.[45] In other words, the SCA is a legislative attempt to balance the tension between traditional Fourth Amendment jurisprudence and the complications posed by society's reliance on electronic communication. That tension largely exists because, although the Fourth Amendment does not protect information that is purposely revealed to third parties, such as a cellular service provider, electronic communication has become necessary to modern life. Further, the use of electronic communication necessarily reveals the content and

34. *Augustine*, 467 Mass. at 258-59 (Gants, J. dissenting) (emphasis in original).

35. Commonwealth v. Princiotta, 31 Mass. L. Rep. 68, at *7 (2013) (information about where subscribers use phones helps carriers identify use patterns and plan for installing new towers) (*citing* In re Application of the United States, 747 F. Supp. 827, 831 (S.D. Tex. 2010)).

36. *Id.*

37. *See id.* at *8 ("According to T-Mobile, its system would be unable to store all cellular tower/cell phone signals.").

38. Commonwealth v. Augustine, 467 Mass. 230, 238 n.19 (2014) (*citing* Blaze Testimony, *supra* note 9, at 57); *see* Blaze Testimony, *supra* note 9, at 58:

> Some carriers will also store this location information not just when calls are made or received, but also about "idle" phones as they move about the network. Creating and maintaining detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect the trend toward more, and more precise, location data collection to continue as part of the natural progression of commercial wireless technology. Once the infrastructure to collect it is installed, the marginal cost of collecting and storing high-resolution location data about every customer is relatively small. Such information will be collected because it is extraordinarily valuable for network management, for marketing, and for developing new services.

39. L. Scott Harrell, *Locating Mobile Phones through Pinging and Triangulation*, Pursuit Magazine (Jul. 1, 2008) (hereinafter "*Locating Mobile Phones*"), http://pursuitmag.com/locating-mobile-phones-through-pinging-and-triangulation/; *see, e.g.,* United States v. Evans, 786 F.3d 779, 781 (9th Cir. 2015) (police "received GPS ping data showing that the cell phone was leaving Nevada, traveling westbound. Later that night, the cell phone pinged from a parking lot of a Super 8 Motel in Sacramento.").

40. *Locating Mobile Phones, supra* note 39; *Evans*, 786 F.3d at 4.

41. *Locating Mobile Phones, supra* note 39.

42. *See id.*

43. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

44. 18 U.S.C. §§2701-2712 (1986).

45. *See* Commonwealth v. Augustine, 467 Mass. 230, 235 (2014); Congressional Research Service, H.R. 4952 (Passed Senate Amended), Summary (The act "Prohibits any person or entity providing an electronic communication service, with specified exceptions, from knowingly divulging the contents of any communication carried on that service.") (Oct. 1, 1986), www.congress.gov/bill/99th-congress/house-bill/4952/summary/195458; *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-13 n.48 (2004) (discussing the purpose of the Stored Communications Act).

circumstances of the communication to the third-party service provider. Accordingly, the SCA regulates the relationship between government entities and electronic and computer service providers in possession of private user information.[46]

The statute distinguishes between "content" communication information,[47] such as the substance of phone recordings or text messages; "non-content" communication information, such as CSLI;[48] and "subscriber information," such as user account information.[49]

Relevant to cellular service providers, the statute functions in two ways.[50] Section 2702 limits electronic service providers[51] from voluntarily disclosing user information to the government.[52] With certain exceptions,[53] therefore, section 2702 generally prohibits public providers from disclosing content and non-content communication records.[54]

Next, section 2703 limits the government's ability to compel cellular service providers to disclose user information.[55] Section 2703(d) further describes what has become known as the "section 2703(d) order," which is a mix between a subpoena and a search warrant.[56] To obtain the order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe" that the information to be compelled is "relevant and material to an ongoing criminal investigation."[57] A section 2703(d) order is sufficient to compel a cellular service provider to disclose CSLI.[58]

IV. PROTECTION AGAINST EXTENDED CONTEMPORANEOUS MONITORING

Shortly before *Augustine*, both the Supreme Judicial Court and the United States Supreme Court analyzed the constitutional implications of electronic tracking. The most recent example was *Commonwealth v. Rousseau*,[59] where the Supreme Judicial Court held that the government cannot "extensively" and "contemporaneously" monitor an individual's location without first obtaining a warrant, and further ruled that monitoring for a 30-day period constituted extensive monitoring.[60]

The posture of the *Rousseau* case had a significant effect on the holding. Rousseau was a passenger in a truck subjected to GPS surveillance. He was convicted with evidence that was obtained through a warrant, which allowed police to place a GPS device on that truck.[61] He did not own or borrow the truck, nor was he the driver.[62] When he challenged the validity of the warrant, the court was required to address the issue of standing.[63] Specifically, the court faced the question of whether Rousseau had grounds to challenge a warrant that permitted police to place a GPS device on a truck in which he had no property interest.[64]

The *Rousseau* court set the table for its standing analysis by discussing its decision in *Commonwealth v. Connolly*,[65] as well as the Supreme Court's *United States v. Jones*[66] opinion. In those cases, each court asked whether the government's attachment of a GPS device to a vehicle constituted a search or seizure. As the *Rousseau* court noted, an important part of those decisions lay in what they did not address.[67]

In analyzing whether the Fourth Amendment was implicated, each court employed a property-based trespasser test, rather than directly analyzing whether electronic tracking had affected a privacy interest.[68] In *Connolly*, the Supreme Judicial Court concluded that both "the initial installation of [a GPS] device on the defendant's vehicle" and "the police use of the defendant's [vehicle] to conduct GPS monitoring for their own purposes constituted a seizure."[69] About three years later in *Jones*, a majority of the Supreme Court similarly held that attaching a GPS device to a vehicle, and then using it to monitor the vehicle's movement on public streets, "constitutes a search *or* seizure."[70] Both *Connolly* and *Jones* thus focused on the government's physical trespass to, and unpermitted use of, a vehicle.[71] Each decision thereby sidestepped the reality and concern that physical intrusion is unnecessary for some forms of electronic surveillance. Nevertheless, the concurring justices took up the issue.[72]

In his *Connolly* concurrence, which was joined by Justices Cordy and Botsford, Justice Gants wrote that "[t]he court's decision suggests that our constitutional analysis of contemporaneous GPS monitoring may depend on whether the monitoring can be

46. *Augustine*, 467 Mass. at 235.

47. "[C]ontents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. §2510(8).

48. *See* 18 U.S.C. §2510(12)(an electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce").

49. 18 U.S.C. §2703(c)(2).

50. For a fuller discussion of the statute, including information not relevant to CSLI, *see Kerr, supra* note 45, at 1215 n.48.

51. An electronic service provider is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §2510(15).

52. 18 U.S.C. §2702(a)(3).

53. 18 U.S.C. §2702(b).

54. 18 U.S.C. §2702(a).

55. 18 U.S.C. §2703(b), (c).

56. *See* Commonwealth v. Augustine, 467 Mass. 230, 236 (2014) ("The standard required for a §2703(d) order thus is less than probable cause; it is 'essentially a reasonable suspicion standard'") (*quoting* In re Application of the United States for an Order Pursuant to 18 U.S.C. §2703(d), 707 F.3d 283, 287 (4th Cir. 2013)).

57. 18 U.S.C. §2703(d).

58. 18 U.S.C. §2703(c)(1)(B).

59. 465 Mass. 372 (2013).

60. *Id.* at 382.

61. *Id.* at 375, 377.

62. *Id.* at 375.

63. *Id.* at 378-83.

64. *Id.* at 382.

65. 454 Mass. 808 (2009).

66. 132 S.Ct. 945 (2012).

67. *See* Commonwealth v. Rousseau, 465 Mass. 372, 381-82 (2013).

68. *Jones*, 132 S.Ct. at 949; *Connolly*, 454 Mass. at 822-23.

69. *Connolly*, 454 Mass. at 822-23; *accord Rousseau*, 465 Mass. at 379.

70. *Jones*, 132 S.Ct. at 948 (emphasis added).

71. Commonwealth v. Connolly, 454 Mass. 808, 822-23 (2009); *accord Rousseau*, 465 Mass. at 379.

72. United States v. Jones, 132 S.Ct. 945, 955, 962 (2012) (Sotomayor, J., concurring); *Connolly*, 454 Mass. at 835 (Gants, J., concurring).

accomplished without a law enforcement officer attaching a GPS device to anyone's property, even when the invasion of the reasonable expectation of privacy would be the same."[73] Justice Gants concluded that the defendant had a reasonable expectation that his "comings and goings will not be continuously and contemporaneously monitored except through physical surveillance, which requires far greater investment of police resources and generates far less information than police monitoring."[74]

Similarly, in her *Jones* concurrence, Justice Sotomayor opined that, "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But 'situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.'"[75] Justice Sotomayor continued:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information for years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices ....[76]

On the other hand, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[77]

After discussing these cases, the *Rousseau* court held that, as a passenger with no property interest in the truck, *Rousseau* lacked standing to challenge the warrant under the *Connolly* and *Jones* property-based tests.[78] The court was thus required to resolve the question that the *Connolly* and *Jones* courts avoided: whether "the government's contemporaneous electronic monitoring of one's comings and goings in public places invades one's reasonable expectation of privacy."[79] The court held that, "under art. 14, a person may reasonably expect not to be subject to extended[[80]] GPS electronic surveillance by the government, targeted at his movements, without judicial oversight and a showing of probable cause."[81] Ultimately, because of this right, Rousseau had standing to challenge the use of the GPS device.[82]

V. THE *AUGUSTINE* DECISION AND RELATED AUTHORITY

A. Background

In *Commonwealth v. Augustine*, murder investigators obtained a section 2703(d) order, which compelled a cellular service provider to disclose two weeks of the defendant's CSLI records.[83] The defendant filed a motion to suppress the CSLI evidence, arguing that the government had intruded upon his right to privacy.[84] On appeal, the Supreme Judicial Court held that an individual has a reasonable expectation of privacy in two weeks of call detail records containing CSLI.[85] Although the court did not add the CSLI records to the appellate record, it recognized that the records merely revealed the location of the cell sites to which the defendant's phone connected during calls.[86] Despite that observation, the court reasoned that CSLI provides the same detailed "tracking" information as GPS location techniques, which can pinpoint a device's location.[87] Moreover, the court reasoned that CSLI required a new approach to the so-called "third-party doctrine."

The third-party doctrine is an exception to the search warrant requirement. The doctrine is based upon the reasoning that, where a party voluntarily discloses information to a third-party, he or she implicitly waives any objective privacy interest in that information.[88] Therefore, the Fourth Amendment does not prohibit the government from obtaining that information from that third-party. So, for example, where an individual voluntarily conveys the phone numbers dialed to the phone company, the individual has no reasonable basis to claim a privacy interest in those phone numbers when the government subpoenas that information from the phone company.[89]

The *Augustine* court reasoned that the third party doctrine did not apply where the government obtains CSLI from a cell service provider, blandly reasoning that the prospect of an individual's comings and goings being contemporaneously monitored — risks not presented by CSLI — are new and distinctive privacy issues begot by the "digital age."[90] With no factual support, the court further justified its new third-party doctrine approach on the grounds that cell phone users do not voluntarily transmit CSLI and are, in

73. *Connolly*, 454 Mass. at 835-36 (Gants, J., concurring).

74. *Id.* at 833.

75. *Jones,* 132 S.Ct. at 955 (Sotomayor, J., concurring) (*quoting Jones,* 132 S.Ct. at 953 (emphasis in original)).

76. *Id.* at 955-56 (internal citations omitted).

77. *Id.* at 964.

78. Commonwealth v. Rousseau, 465 Mass. 372, 382 (2013).

79. *Id.*

80. The minimum time span that constitutes "extended" monitoring, thus requiring the government to obtain a warrant, remains unclear. In *Rousseau*, the monitoring was found to be extensive where the state police "installed the GPS on July 20, 2007, and collected information until August 19, 2007." *Id.* at 376. Subsequently, the *Augustine* court held that the analysis of two weeks of CSLI records also constitutes extended monitoring. 467 Mass. at 254-55. However, in dicta, the *Augustine* court noted that:

> ... it is likely that the duration of the period for which historical CSLI is sought will be a relevant consideration in the reasonable expectation of privacy calculus — that there is some period of time for which the Commonwealth may obtain a person's historical CSLI by meeting the standard for a §2703(d) order alone, because the duration is too brief to implicate the person's reasonable privacy interest. Commonwealth v. Augustine, 467 Mass. 230, 255 (2014). The court later decided that six hours or less of CSLI records fell outside a person's reasonable expectation of privacy. Commonwealth v. Estabrook, 472 Mass. 852, 858 (2015). In United States v. Skinner, the Court of Appeals for the Sixth Circuit found that leveraging a cell phone's GPS capabilities to track a defendant for a three-day period was reasonable, relatively short-term tracking. 690 F.3d 772, 780 (6th Cir. 2012).

81. *Rousseau*, 465 Mass. at 382 (*citing* United States v. Jones, 132 S.Ct. 945, 954-55 (2012) (Sotomayor, J., concurring) (footnote inserted)).

82. Because the warrant affidavit contained a sufficient showing of probable cause, Rousseau's conviction was upheld. *Id.* at 383-84.

83. 467 Mass. at 233-34.

84. *Id.* at 234.

85. *Id.* at 232.

86. Commonwealth v. Augustine, 467 Mass. 230, 239 (2014).

87. *Id.* at 247-48.

88. *Id.* at 241-43.

89. *Id.* at 243 (discussing Smith v. Maryland, 442 U.S. 735, 737 (1979)).

90. *Id.* at 245.

general, unaware that cell service providers document CSLI for business purposes.[91]

There is no doubt that electronic communication, and in particular cell phone use, raises new and significant privacy concerns that warrant judicial oversight. That said, the *Augustine* court's reasoning is flawed. The opinion blurs significant differences between GPS technology and CSLI, particularly regarding their respective pervasiveness, contemporaneousness, and precision. Of further concern, the court's distinction of Article 14 third-party doctrine jurisprudence is judicially active and forced, relying on the court's own dubious assertions of cell phone users' knowledge and privacy expectations.

B. Constitutional differences between GPS and CSLI

The *Augustine* opinion offers a rather cursory conclusion that historical CSLI records pose the same privacy threat as GPS tracking. For example, the court states that "there is no question that [CSLI] tracks the location of a cellular telephone user"[92] and that "[i]t is evident that CSLI implicates the same nature of privacy concerns as a GPS tracking device."[93]

But, unlike the GPS devices in *Rousseau* and *Connolly*, call detail record CSLI is not contemporaneous. It consists of historical call and text message records, obtained after the fact. Moreover, as the *Augustine* dissent states, the records are "episodic, not continuous" and therefore not pervasive.[94] Call detail records show the particular sector of a tower that a phone connected to, and thus the general location of a phone at the time that it engaged in a call or text message. For example, in *Augustine* the CSLI "was limited to the defendant's movements while he was engaged in a telephone call for ninety-one consecutive minutes."[95] Unlike GPS, therefore, CSLI does not "subject[a person] to extended [] electronic surveillance by the government, targeted at his movements."[96] In fact, unlike what may have been the case in *Augustine*, most CSLI records only reveal the tower that a phone connected to at the commencement and termination of a call.[97]

Granted, cell phones register their location about every seven seconds and it is possible for a carrier to record each tower with which a phone registers. Such a record would be pervasive. Carriers, however, do not presently record registration data and do not appear to be planning to record it in the foreseeable future.[98] Regardless, if pervasiveness was truly the concern, it would seem that the court could have sufficiently protected against it by requiring the government to obtain a warrant where it seeks registration data. As stated by the dissent:

> A search warrant may appropriately be required where the CSLI, because of its duration and the number of location points it will identify, will reveal so much about the private life and personal affiliations of the telephone user as to invade the reasonable expectation of privacy, but it is not appropriate where the duration will reveal only where the telephone user was at a particular time or over a brief period of time.[99]

Similar to its discussion of pervasiveness and contemporaneousness, the court brushed aside the fact that CSLI is not as precise as GPS.[100] The court found it "unnecessary to consider [that] argument because whatever the specific facts about the relative precision of GPS data and the CSLI at issue …, the commonwealth agrees that CSLI does track location and that, as indicated in the text, it seeks the CSLI precisely because of its location-tracking abilities."[101]

But the precision of the location information is the very parameter on which a would-be privacy intrusion depends. Indeed, the precision of the location information was the paramount concern in the decisions analyzing GPS, which began crafting the location privacy right on which the *Augustine* court's analysis relied. The *Jones* court explained that, "[b]y means of signals from multiple satellites, the [GPS] device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the four-week period."[102] On that record, Justice Sotomayor's concurrence, cited by the *Augustine* court, expressed a reasonable concern that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[103] The *Augustine* court further relied on a New Jersey Supreme Court decision, which posited that:

> [l]ocation information gleaned from a [cellular telephone] provider can reveal not just where people go — which doctors, religious services, and stores they visit — but also the people and groups they choose to affiliate with and when they actually do so. That information cuts across a broad range of personal ties with family, friends, political groups, health care providers, and others …. In other words, details about the location of a [cellular telephone] can provide an intimate picture of one's daily life.[104]

That New Jersey Supreme Court case, *State v. Earls*,[105] also conflated GPS and CSLI, after expressly stating that the precision of

91. *Id.* at 249-50.

92. Commonwealth v. Augustine, 467 Mass. 230, 246 (2014).

93. *Id.* at 248-49.

94. *Augustine*, 467 Mass. at 266 (Gants, J., dissenting).

95. *Id.* at 246 n.30.

96. *Id.* at 247-48 (*citing* Commonwealth v. Rousseau, 465 Mass. 372, 382 97.

97. Commonwealth v. Princiotta, 31 Mass. L. Rep. 68, at *9 (2013).

98. Commonwealth v. Augustine, 467 Mass. 230, 265 n.5 (2014) (Gants, J., dissenting) (discussing the fact that the majority's opinion rests on speculation that CSLI will become more precise at some time in the future).

99. *Id.* at 267.

100. *Id.* at 248 n.31.

101. *Id.*

102. United States v. Jones, 132 S.Ct. 945, 948 (2012).

103. *Id.* at 955 (Sotomayor, J., concurring) (*citing* People v. Weaver, 12 N.Y.3d 433, 441-42 (2009)), *cited in Augustine*, 467 Mass. at 248.

104. Commonwealth v. Augustine, 467 Mass. 230, 248 (2014) (*quoting* State v. Earls, 214 N.J. 564, 586 (2013)) (alterations in the original, internal quotation marks omitted).

105. 214 N.J. 564 (2013).

the location data is paramount to whether the right to privacy has been violated.[106]

The *Augustine* court also reasoned that the precision of the location information was of the utmost importance:

> … as the defendant contends, because of the nature of cellular telephone use and technology, there is a strong argument that CSLI raises even greater privacy concerns than a GPS tracking device. In contrast to such a device attached to a vehicle, see, e.g., *Rousseau*, 465 Mass. at 374; *Connolly*, 454 Mass. at 810, because a cellular telephone is carried on the person of its user, it tracks the user's location far beyond the limitations of where a car can travel. As a result, CSLI clearly has the potential to track a cellular telephone user's location in constitutionally protected areas.[107]

In a subsequent opinion explaining *Augustine, Commonwealth v. Collins*, the court stated the importance of precision expressly.[108] In that case, the court found that a call detail record containing "repoll numbers" — that is, information identifying mobile switching stations through which a call was routed — did not implicate the defendant's right to privacy because that information did not provide the type of pinpoint location details that reveal information about a person's comings and goings. In distinguishing the non-precise location information in *Collins* from the non-precise location information in *Augustine*, the court explained that only the latter raised privacy concerns because it:

> … tracks the location of a cellular telephone user with such precision that it "implicates the same nature of privacy concerns as a [global positioning system] tracking device" and "may yield a treasure trove of very detailed and extensive information about the individual's 'comings and goings' in both public and private places."[109]

Although information about what tower a phone connected to is indeed more precise than information about what switching station handled a call, they are each unlike GPS because neither set of information yields a pin-point picture of where a person or object is. Like repoll numbers, CSLI merely shows that a cell phone connected to a particular portion of a cell network's infrastructure, not whether a person was within a private or public location. In fact, because of factors such as signal interference and user call volume, the tower or switching station that a phone connects to might not even be the geographically closest to that phone.[110]

It would seem, then, that the differences and consistencies between GPS and CSLI are paramount to whether CSLI implicates the Fourth Amendment. But the *Augustine* court did not delve into what CSLI actually reveals; in fact, the CSLI in that case was not even part of the appellate record.[111] Ultimately, despite its express concern about the precision of a location that a tracking technology reveals, the court was satisfied to conflate GPS and CSLI "because whatever the specific facts about the relative precision of GPS data and the CSLI at issue [], the commonwealth agrees that CSLI does track location and that … it [sought] the CSLI precisely because of its location-tracking abilities."[112]

To be sure, as more cell site towers are installed, the precision of CSLI will likely increase. But the prospective increase in precision is a matter of speculation[113] well outside the court's expertise. Moreover, aside from experimentation with building-specific cell sites,[114] there is no reason to conclude that historical CSLI will ever show where, precisely, a mobile phone is located.[115] In fact, logic dictates that cell tower construction within a particular area will reach its saturation point well before the number of towers necessary to achieve pin-point CSLI would be reached. As the *Augustine* opinion imparts, towers installed in major metropolitan areas are already sufficient to service cell phones for a seemingly vast majority of the public.[116]

The appreciable differences between GPS and CSLI technology have been addressed elsewhere. In *United States v. Davis*,[117] the Court of Appeals for the Eleventh Circuit conducted a rehearing en banc and then overturned its prior decision,[118] ultimately holding that a section 2703(d) order compelling a service provider to disclose 67 days of CSLI did not violate the defendant's Fourth Amendment

106. *Id.* at 587-88; *see also infra* Section VI(a) (discussing *Earls*).

107. *Augustine*, 467 Mass. at 248-49 (citation omitted).

108. 470 Mass. 255, 270 (2014).

109. *Id*. at 270 (*quoting Augustine*, 467 Mass. at 248, 251).

110. *See, e.g., id.* at 269 ("The records custodian testified that a repoll number reveals the general area where the cellular telephone is at the time of a call, but does not provide a pinpoint location; that a repolling site can cover an area of up to 100 miles; and that a repoll number from the Washington, D.C., area would indicate that the cellular telephone for that call was 'more likely' in Virginia, Maryland, or Washington, D.C., and 'definitely not the Boston area.' Taken together, the evidence indicated that the cellular telephone that the defendant was regularly using was in the Washington, D.C., area after December 7, 2006, which the Commonwealth suggested reflected that he fled Massachusetts for Washington, D.C., shortly after the killing, showing his consciousness of guilt.").

111. Commonwealth v. Augustine, 467 Mass. 230, 234 n.12 (2014) ("Based on the information about the CSLI records that the parties provided at that hearing, and in light of the Commonwealth's objection, we will not expand the record, having determined that a review of the CSLI evidence is not essential to resolution of the issues before us.").

112. *Id.* at 247 n.31.

113. *See Augustine,* 467 Mass. at 253 ("we cannot ignore the probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas"); *id*. at 265 n.5 (Gants, J., dissenting) ("The [majority] contends that there is the 'probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas'") (*quoting Augustine*, 467 Mass. at 253).

114. *See* Blaze Testimony, *supra* note 9, at 44.

115. Moreover, it is unclear how a person has a reasonable expectation of privacy of "being in their home." Indeed, an officer is clearly within his right to stake out a home and await the residents' return. It is, rather, the activity that takes place therein which has traditionally been protected.

116. *Compare Augustine*, 467 Mass. at 246 ("As anyone knows who has walked down the street or taken public transportation in a city like Boston, many if not most of one's fellow pedestrians or travelers are constantly using their cellular telephones") with *id.* at 261 (Gants, J., dissenting) ("there are more cellular telephones in the United States than United States residents").

117. 785 F.3d 498 (11th Cir. 2015).

118. United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

rights because CSLI and GPS reveal significantly different information. As the *Davis* court discussed:

> ... historical cell tower location data is materially distinguishable from the precise, real-time GPS tracking in *Jones* .... Historical cell tower location data does not identify the cell phone user's location with pinpoint precision — it identifies the cell tower that routed the user's call. The range of a given cell tower will vary given the strength of its signal and the number of other towers in the area used by the same provider. While the location of a user may be further defined by the sector of a given cell tower which relays the cell user's signal, the user may be anywhere in that sector. This evidence still does not pinpoint the user's location. Historical cell site location data does not paint the "intimate portrait of personal, social, religious, medical, and other activities and interactions" that [the defendant] claims.[119]

The *Davis* court further noted that the CSLI "was not continuous; it was generated only when [the defendant] was making or receiving calls on his phone."[120] The Fifth Circuit Court of Appeals also has implied that differences between the respective technologies affects the appropriate legal analysis.[121]

The *Davis* court also responded to a frequently cited but flawed argument that, because a cell phone follows its user, CSLI implicates activities occurring within the home.[122]

In so doing, the court took note of evidence elicited at trial, which showed that a cell phone placing a call from within a person's home may not even connect to the cell tower closest to that home, depending on certain conditions affecting the cellular network.[123] The court continued that the defendant,

> [a] prolific cell phone user, made approximately 86 calls a day. Without question, the number of calls made by [the defendant] over the course of 67 days could, when closely analyzed, reveal certain patterns with regard to his physical location in the general vicinity of his home, work, and indeed the robbery locations. But no record evidence here indicates that the cell tower data contained within these business records produces precise locations or anything close to the "intimate portrait" of [the defendant's] life.[124]

Relying on the above analysis, the *Davis* court concluded that, if there were any intrusion on the defendant's reasonable expectation of privacy, it was minimal.[125] The court observed that "first, there was no overhearing or recording of any conversations. Second, there [was] no GPS real-time tracking of precise movements of a person or vehicle. Even in an urban area, [the service provider's] records [did] not show, and the examiner [could not] pinpoint, the location of the cell user."[126] The court continued, all of this non-specific location information was available to the government only by a process involving judicial oversight, namely, a section 2703(d) order.[127]

Although it did not analyze these considerations in depth, the Fifth Circuit, in *In re Application of the United States for Historical Cell Site Data*,[128] discussed similar points. The court cited to the Code of Federal Regulations, which contained a regulation that required cell service providers to develop the ability "to locate phones within 100 meters of 67 percent of calls and 300 meters for 95 percent of calls for network based calls, and to be able to locate phones

119. *Davis*, 785 F.3d at 515; *see also* People v. Bussey, 19 N.Y.3d 231, 234 (2012) (CSLI showed that suspect was "in the Poughkeepsie area"); People v. Arafet, 13 N.Y.3d 460, 462 (2009) (cell phone records show that the defendant traveled north, and later returned south); *id.* at 474 (CSLI showed "that calls were made from one of defendant's cell phones that ostensibly track the same route"); State v. Tate, 2014 WI 89, at 8 (2014) (police "were receiving information with the cell tower information, what that cell tower is currently on ... the phone signal 'was bouncing between three different cell phone towers on three different sectors which if you were to map it out were to give you an angle or an area of probability of where you believe the suspect would be ... at that time'"); Zuninga v. State, 2012 Nev. Unpub. LEXIS 1626, *1 (Nev. 2012) (noting that CSLI was used to show defendant was "in the vicinity" of the victim's home, as opposed to the vicinity of his office).

120. *Davis*, 785 F.3d at 512.

121. *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013):

> Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain historical cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders requesting data from all phones that use a tower during a particular interval, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods). Nor do we address situations where the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS, with or without the service provider's help.

122. *Davis*, 785 F.3d at 516.

123. *Id.*

124. United States v. Davis, 785 F.3d 498, 516 (11th Cir. 2015).

125. *Id.* at 517.

126. *Id.*

127. *See Davis*, 785 F.3d at 517 (*quoting* Brock v. Emerson Elec. Co., Elec. & Space Div., 834 F.2d 994, 996 (11th Cir. 1987))

> ... a §2703(d) court order functions as a judicial subpoena, but one which incorporates additional privacy protections that keep any intrusion minimal. The SCA guards against the improper acquisition or use of any personal information theoretically discoverable from such records. Under §2703(d), investigative authorities may not request such customer-related records merely to satisfy prurient or otherwise insubstantial governmental interests. Instead, a neutral and detached magistrate must find, based on "specific and articulable facts," that there are "reasonable grounds to believe" that the requested records are "relevant and material to an ongoing criminal investigation." Such protections are sufficient to satisfy "the primary purpose of the Fourth Amendment," which is "to prevent arbitrary invasions of privacy."

128. 724 F.3d 600, 609 (5th Cir. 2013)

within 50 meters of 67 percent of calls and 150 meters of 95 percent of calls for hand-set based calls" by 2012.[129] This regulation is part of the Wireless Communications and Public Safety Act of 1999,[130] also known as the 911 Act. It appears that carriers have met this requirement by producing cell phones with GPS.[131] In any event, the possibility that cell sites can be used to produce more precise location data than that contained in CSLI records does not mean that such data appears in CSLI records; and in fact, that information is largely irrelevant to the business purposes of CSLI records.

In contrast to *Davis*, a number of other decisions reveal confusion similar to that which affected *Augustine*. For example, in *Tracey v. State*,[132] the Supreme Court of Florida purportedly analyzed tracking conducted through "real time CSLI." The court strongly implied that the CSLI at issue allowed police to pinpoint the defendant's location in a specific house.[133] The record, on some unknown basis, also seems to have asserted that the "real time CSLI tracking" only occurred while the defendant traveled upon public roads.[134] These circumstances suggest that the *Tracey* court conflated CSLI with GPS location information gained through pinging.[135]

Like historical CSLI, pings are a product of cell tower use, but the location of a cell site is only incidentally related to a ping.[136] As discussed in Section II, *supra*, pings are unlike CSLI because they reveal the precise location of a cell phone. Pinging involves sending a signal to a particular cell phone, requesting that the cell phone respond with coordinates obtained through its GPS capabilities. Moreover, pinging, unlike CSLI location, is conducted in real time.[137]

Given that the *Tracey* court found that the defendant's location was obtained in real time and that it revealed that he was traveling on specific roads and then entered a specific house, the court was likely discussing information obtained through a ping. The tracking information before the court was like that in *United States v. Evans*,[138] where the Ninth Circuit specifically noted that, through the use of a ping which revealed the defendant's location by leveraging the phone's GPS capabilities, police tracked the defendant as he drove out of the state and later located his phone in a specific hotel parking lot. A similar problem also appears to have affected the Ninth Circuit's decision in *United States v. Skinner*.[139] There, as a result of "continuously 'pinging'" the defendant's cell phone, police learned that a truck was traveling on a specific interstate, and that it came to rest at a particular truck stop.[140] In the course of finding that there was no Fourth Amendment violation, the *Skinner* court referenced the information obtained through pinging as "cell site information."[141] Comparably, in both *State v. Tate*[142] and *State v. Subdiaz-Osorio*,[143] the Supreme Court of Wisconsin seems to have confused CSLI with triangulation. Again, although the use of towers makes triangulation possible, it is unlike CSLI, which strictly indicates which tower a phone connected to during a particular call.

Likewise, the New Jersey Supreme Court, although describing the differences in GPS and CSLI technologies in *State v. Earls*,[144] ultimately appeared to have ignored them. In that case, police were seeking the defendant pursuant to an arrest warrant when a cell service provider gave them information that the defendant's phone had connected to a cell site which serviced a general area around a particular highway.[145] After searching the area for several hours, police located and arrested the defendant.[146] On appeal from the denial of the defendant's motion to suppress, the *Earls* court noted the differences between CSLI and GPS,[147] and further stated that, "[a]s a general rule, the more sophisticated and precise the tracking, the greater the privacy concern."[148] Yet ultimately, in a case where police obtained only general location information from CSLI, the *Earls* court crafted an extremely broad rule of law: the New Jersey Constitution protects an individual's "privacy interest in the location of his or her cell phone."[149]

Despite noting the differences between GPS and CSLI, as well as the fact that the precision of the information is a paramount concern, the court implied that both CSLI and GPS reveal the same intimate private details of a person's life.[150] That reasoning was particularly odd, given that the facts of *Earls* demonstrate that CSLI did not provide police with information about the defendant's specific location. Rather, the CSLI merely indicated that the defendant had traveled to several general areas — in two of which, he could not be located at all — and was discovered only after police searched those areas for hours. Against this backdrop, the court conflated CSLI

129. *Id.* (*citing* 47 C.F.R. §20.18(h)(1)(2012)).

130. Public Law 106-81, 113 Stat. 1286 (1999).

131. *See Locating Mobile Phones, supra* note 39 ("New generation cell phones and mobile service providers are required by federal mandate, via the 'E-911' program, to be or become GPS capable so that 911 operators will be able to determine the location of a caller who is making an emergency phone call.").

132. Tracey v. State, 152 So.3d 504 (Fla. 2014).

133. *Id.* at 507.

134. *Id.* at 508, 525 (*citing* Tracey v. State, 69 So.3d 992, 994 (Fla. 2011)).

135. The Florida Supreme Court states that "CSLI refers to location information generated when a cell phone call occurs ... the location of the cell phone can be pinpointed with varying degrees of accuracy depending on the size of the geographic area served by each cell tower, and is determined by reference to data generated by cell sites pertaining to a specific cell phone." *Tracey*, 152 So.3d at 507 n.1. This definition is akin to the type of non-precise, historical CSLI that the police in Tracey were permitted to obtain. *See Tracey,* 69 So.3d at 994 ("the order [in Tracey] directed the cell phone company to provide the sheriff's office, '[i]n accordance' with 18 U.S.C §2703(d), 'historical Cell Site Information indicating the physical location of cell sites, along with cell site sectors, utilized for the calls ....' The order did not address prospective or real time CSLI."). That kind of historical record, of course, is not obtained in "real time."

136. *See Locating Mobile Phones, supra* note 39.

137. *See, e.g.,* United States v. Evans, 786 F.3d 779, 781 (9th Cir. 2015).

138. *Id.*

139. 690 F.3d 772 (6th Cir. 2012).

140. *Id.* at 776.

141. *Id.* at 778, 780.

142. 2014 WI 89, at 7 (2014) (CSLI "allows law enforcement to locate a cell phone by triangulation").

143. 2014 WI 87, at 45 & n.19 (2014) (implying that CSLI involves the use of triangulation).

144. 214 N.J. 564 (2013).

145. *Id.* at 571.

146. *Id.*

147. *Id.* at 577-79.

148. *Id.* at 587.

149. *Id.* at 588.

150. *See* State v. Earls, 214 N.J. 564, 588 (2013).

and GPS, stating that today's cell phones "can be pinpointed with great precision — to within feet in some instances," and that such information is "updated every seven seconds through interactions with cell towers" which "can reveal a great deal of private information about a person's life."[151] As discussed, call detail record CSLI cannot pinpoint a defendant's location within a number of feet, is not recorded every seven seconds, and does not reveal information beyond the fact that a cell phone connected to a particular cell tower. Moreover, the *Earls* court implicitly reasoned that the defendant, who was subject to an arrest warrant, had an objective expectation of privacy in his location. The *Augustine* court relied on *Earls*.[152]

C. Third-party doctrine

Although CSLI presents novel challenges to traditional third-party doctrine jurisprudence, the Supreme Judicial Court's departure from precedent in *Augustine* is activist. To justify its new methodology, the court reasoned that "all the distinctive characteristics of cellular telephone technology and CSLI … require … a different approach" to the third-party doctrine.[153] In other words, "the individual's justifiable interest in not having 'his comings and goings continuously and contemporaneously monitored' by the government" warranted departure from the prevailing rule.[154] But as discussed *supra* Section II, CSLI does not provide the government with a detailed record of a person's comings and goings. This flaw in reasoning was addressed by the *Augustine* dissent, which critiqued the majority on the grounds that it "recognizes the differences between telephone call CSLI and registration CSLI, [but] conducts its analysis under art. 14 of the Massachusetts Declaration of Rights as if those differences have no constitutional consequence or as if the court ordered the production of registration CSLI."[155]

But even putting aside the fact that the CSLI records in *Augustine* did not infringe on the privacy rights apparently recognized by the court, its rationale remains untenable. Foremost, the court reasoned that the third-party doctrine can be invoked only "when one voluntarily conveys information to [a] company, such as the telephone numbers one is dialing, and knows that the company records this information for legitimate business purposes."[156] But the conveyance of CSLI, reasoned the court, is not voluntary because a subscriber does not identify and transmit CSLI to the cellular service provider.[157] For instance, unlike dialing a number or submitting a bank deposit slip, the court observed, CSLI is "purely the function and product of … telephone technology."[158] Thus, the court concluded, the treatment of CSLI should be distinguished from cases where the telephone number dialed "was exactly the same information that the telephone subscriber had knowingly provided to the telephone company when he took the affirmative step of dialing the calls … ."[159]

This parsing of voluntariness is off-base. A voluntary action is not necessarily the product of desire, but one that is willfully and knowingly undertaken.[160] The fact that CSLI is not consciously and affirmatively identified and communicated does not render its transmission involuntary. By way of analogy, a person who decides to play football does not volunteer, or even desire, to be tackled, but, as an effect of his decision to play football, voluntarily assumes that risk.[161]

The *Augustine* dissent offered a similar conclusion:

> Every person who uses a cellular telephone recognizes that the location of the telephone matters in determining whether there is cellular service and, where there is such service, in determining the quality of the telephone connection, which is why at least one cellular telephone company advertises "more bars in more places." Therefore, every person who uses a cellular telephone recognizes, at least implicitly, that a cellular telephone company must identify the location of a cellular telephone, as well as the telephone number called, before a call can be successfully made from a cellular telephone. Accordingly, although a cellular telephone user may not know that the telephone company records and keeps this information, or want it kept, the user should know that location information, as well as the telephone number, must be provided to the telephone company whenever he makes or receives a telephone call.[162]

In contrast, the *Augustine* majority offered no reason to support its premise that cell phone users "unknowingly" transmit CSLI. At best, the extent to which cell phone users are aware that CSLI is transmitted by phone use is unclear. At least one poll — though by no means definitive — indicates that an overwhelming majority of cell phone users are aware that CSLI is recorded.[163]

Even when applying the court's definition of voluntariness, it is not a convincing ground to distinguish CSLI from prior third-party doctrine analysis of telephones. The dissent's assessment is far more practical:

> Today, a telephone caller no more voluntarily conveys a number to the telephone company than he voluntarily conveys his location to the telephone company, but he implicitly knows that the telephone company's computers need to know both for the call to be successfully connected. Second, for incoming telephone calls, the person receiving the call does not dial any number or otherwise convey any number, but the telephone

151. *Id.* at 587.

152. *See* Commonwealth v. Augustine, 467 Mass. 230, 248 (2014) (*quoting* State v. Earls, 214 N.J. 564, 586 (2013)).

153. *Augustine*, 467 Mass. at 251-52.

154. *See id.* at 251 (*quoting* Commonwealth v. Connolly, 454 Mass. 808, 835 (2009) (Gants, J., concurring)) (internal quotation marks omitted).

155. *Id.* at 259 (Gants, J., dissenting).

156. *Id.* at 249.

157. *Id.*

158. Commonwealth v. Augustine, 467 Mass. 230, 250 (2014).

159. *Id.*

160. Black's Law Dictionary 1569 (7th ed. 1999) (defining voluntary as "[d]one by design or intention; Unconstrained by interference; not impelled by outside influence").

161. *See Augustine*, 467 Mass. at 259-60 (Gants, J., dissenting).

162. *Id.* at 263-64.

163. Orin S. Kerr, "Eleventh Circuit, disagreeing with the Fifth, holds Fourth Amendment protects cell-site records," The Washington Post (June 11, 2014) http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/11/eleventh-circuit-disagreeing-with-the-fifth-holds-fourth-amendment-protects-cell-site-records.

> number of the caller is nonetheless included in the cellular telephone toll records.[164]

Finally, the court asserted that CSLI is unrelated to the "primary purpose for owning and using [a phone]."[165] To the contrary, the ability to remotely transmit information is the primary reason that cell phones have become an inescapable part of modern life. As the court effectively stated earlier in its opinion, cell phones have skyrocketed in popularity because of the fact that they are mobile:

> As anyone knows who has walked down the street or taken public transportation in a city like Boston, many if not most of one's fellow pedestrians or travelers are constantly using their cellular telephones as they walk or ride … . As people do so, they are constantly connecting to cell sites, and those connections are recorded as CSLI by their cellular service providers.[166]

Plainly, people use cell phones to place calls within the infrastructure of their carrier's wireless network, which is improved through the use of data demonstrating where cell phone use tends to occur. It is simply not the case that "CSLI has no connection at all to the reason people use cellular phones."[167]

In addition to appreciating the differences between CSLI and GPS, other jurisdictions have been more reluctant to depart from the third-party doctrine. In *United States v. Davis*, for example, the Court of Appeals for the Eleventh Circuit reasoned that a defendant had no expectation of privacy in his cell service provider's CSLI records.[168] As to the subjective expectation of privacy, the Eleventh Circuit joined the Fifth Circuit's view:

> that cell users know that they must transmit signals to cell towers within range, that the cell tower functions as the equipment that connects the calls, that users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower's range, and that cell phone companies make records of cell-tower usage.[169]

Citing *Smith v. Maryland*,[170] a third-party doctrine case relied upon by the *Augustine* court,[171] the *Davis* court additionally held that there is no objective privacy expectation in CSLI. Specifically, the *Davis* court wrote that, in *Smith*, "the Supreme Court presumed that phone users knew of uncontroverted and publicly available facts about technologies and practices that the phone company used to connect calls, document charges, and assist in legitimate law-enforcement investigations" and that "[c]ell towers and related records are used for all three of those purposes."[172] The court found "no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers recording cell tower usage."[173]

VI. CONCLUSION

Cell Site Location Information is a novel technology that implicates an important privacy concern and the *Augustine* court was prudent to cautiously analyze its effect on privacy rights. Unfortunately, the court's concern overshadowed its consideration of CSLI's technological limits, resulting in speculative analysis that is focused not on what CSLI actually reveals, but on how CSLI might develop over the course of time.

The novelty of the issue apparently increased the court's willingness to depart from established precedent. Although the court cited to its determinations in *Rousseau* and *Connolly* — that an individual's privacy right protects against contemporaneous and pervasive monitoring — it vastly expanded the rights recognized in those cases. Moreover, the court's attempt to distinguish third-party jurisprudence was a product of creative reasoning, as opposed to sound logic and deference to precedent.

As an institution, the judiciary may be ill-equipped to analyze the technical points presented in *Augustine*. In fact, both the Court of Appeals for the Sixth Circuit and the Florida Supreme Court demonstrated a similar inability to parse the technological differences implicated by GPS and CSLI. For example, the Florida Supreme Court defined CSLI as location information "generated when a cell phone call occurs," but then analyzed precise location information, which was most likely obtained through a ping, before concluding that "[a]ll of [the] concerns and conclusions about GPS tracking also apply to tracking and monitoring by use of real time cell site location information."[174] Similarly, the Sixth Circuit found that police used "cell site information" by leveraging the defendant's cell phone's GPS capabilities.[175]

The outcome is unfortunate. Stored telephone records serve compelling government interests in criminal cases. For example, historical cell tower location records are routinely used to investigate

164. Commonwealth v. Augustine, 467 Mass. 230, 265 (2014) (Gants, J., dissenting).

165. *Id.* at 250.

166. *Id.* at 245.

167. *Id.* at 250.

168. United States v. Davis, 785 F.3d 498, 511-13 (11th Cir. 2015).

169. *Id.* at 511 (*citing* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 613-14 (5th Cir. 2013)); *see also* State v. Griffin, 834 N.W.2d 688, 696-97 (Minn. 2013) (defendant, who was not the subscriber to cell phone service, failed to present evidence that he expected a service provider to keep his phone usage private).

170. 442 U.S. 735, 742-46 (1979).

171. Commonwealth v. Augustine, 467 Mass. 230, 243 (2014).

172. *Davis*, 785 F.3d at 511.

173. *Id.; see also* United States v. Guerrero, 768 F.3d 351, 358-59 (5th Cir. 2014) (cell phone users voluntarily convey location information); *In re Application of the United States for Historical Cell Site Data,* 724 F.3d at 605-15 (cell phone users are aware that calls convey CSLI and that providers retain that information; thus, there is no reasonable expectation of privacy in third-party cell service provider's CSLI records).

174. Tracey v. State, 152 So.3d 504, 519 (Fla. 2014).

175. United States v. Skinner, 690 F.3d 772, 776-77, 778 (6th Cir. 2012).

child abductions, bombings, kidnappings, murders, robberies, sex offenses and terrorism-related offenses.[176]

> Such evidence is particularly valuable during the early stages of an investigation, when the police lack probable cause and are confronted with multiple suspects. In such cases, § 2703(d) orders — like other forms of compulsory process not subject to the search warrant procedure — help to build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources … . Cell tower location records have the capacity to tell the police investigators that an individual suspect was in the general vicinity of the crime scene or far away in another city or state. In sum, a traditional balancing of interests amply supports the reasonableness of the § 2703(d) order at issue here.[177]

Ultimately, the court should have deferred to the SCA's privacy protection scheme, at least until it had the opportunity to adjudicate a case presenting a more apparent invasion of privacy. Indeed, the court is not in the best position to determine what a cell phone user reasonably considers private, and it seems that, in most ways, the treatment of a novel technical matter involving public opinion, such as this, is best left to the legislature.[178]

176. United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015).

177. *Id.*

178. *See* United States v. Jones, 132 S.Ct. 945, 964 (2012) (Sotomayor, concurring) ("[p]erhaps, as Justice Alito notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not.") (citation omitted); *Davis*, 785 F.3d at 515 (Justice Alito's *Jones* concurrence "suggests that a legislative solution is needed"); *id.* at 512.

> The use of cell phones is ubiquitous now and some citizens may want to stop telephone companies from compiling cell tower location data or from producing it to the government. *Davis* and amici advance thoughtful arguments for changing the underlying and prevailing law; but these proposals should be directed to Congress and the state legislatures rather than to the federal courts.

In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 614-15 (5th Cir. 2013)) ("Congress has crafted such a legislative solution in the SCA. The statute conforms to existing Supreme Court Fourth Amendment precedent.").

Case Comment

Coghlin Elec. Contractors, Inc. v. Gilbane Building Co., 472 Mass. 549 (2015)

One of the ancient, bedrock principles of construction law is that where "the contractor is bound to build according to plans and specifications prepared by the owner, the contractor will not be responsible for the consequences of defects in the plans and specifications."[1] Known as the "*Spearin* doctrine," the Supreme Judicial Court recognized it as a maxim of Massachusetts law in 1970.[2] In 1981, immediately following the issuance of the Ward Commission's final report, Massachusetts General Laws chapter 149, section 44F went into effect, requiring that "[e]very contract [for public building construction] shall include specifications and, if deemed necessary or convenient by the awarding authority, plans, detailing all labor and materials to be furnished thereunder."[3] Until 2004, the *Spearin* doctrine applied to every contract for the construction of municipal or state buildings in the commonwealth.[4]

In 2004, the legislature passed Massachusetts General Laws chapter 149A, sections 1 through 13, the "construction management at risk" ("CMAR") statute, authorizing awarding authorities to solicit for the construction of public buildings from contracts based only on "detailed information concerning the project scope including any preliminary design information, geotechnical reports, existing condition surveys and specifications," and "a detailed description of the [scope of] work."[5] Instead of accepting bids based on plans and specifications "detailing all labor and materials,"[6] awarding authorities now could select a contractor before complete development of the project design.[7] After being selected, the CMAR contractor may provide "a range of construction management services to the public owner as the design is being developed… includ[ing] cost estimation and consultation regarding the design of the building project, preparation and coordination of bid packages, scheduling, cost control, and value engineering."[8] The expectation under the CMAR statutory scheme is that "the final design may reflect or incorporate substantial input from the [contractor]."[9]

In *Coghlin Elec. Contractors Inc. v. Gilbane Building Co.,* the Supreme Judicial Court tackled the question of whether the *Spearin* doctrine applied to a chapter 149A CMAR contractor, or whether participation in the design process negates the contractor's common law protection.[10] That case arose from a project at the Worcester State Hospital (the Project) where the Division of Capital Asset Management and Maintenance (DCAM) elected to utilize the CMAR statutory scheme in contracting to build a psychiatric facility.[11] Pursuant to the statutory scheme, DCAM selected Gilbane Building Company (Gilbane) as the CMAR contractor, before completion of the Project design.[12] Gilbane subcontracted electrical work to Coghlin Electrical Contractors, Inc. (Coghlin).[13]

Coghlin alleged that it suffered a 49 percent increase in labor hours on the Project because of Gilbane's poor management and due to design defects.[14] The alleged design defect was that the project design called for a two-foot deep interstitial space between floors to allow for the building's mechanical, electrical and other systems.[15] This conflicted with another part of the design, however, that called for mechanical and electrical systems occupying five feet of interstitial depth.[16] Coghlin did not receive direction on how to proceed with installation of the electrical systems for more than six weeks, before being told to "place the electrical work as high as possible in the ceiling," allowing the project designer to "address the issue later" with the mechanical subcontractor.[17]

Coghlin filed a contract claim, and then later a suit in superior court against Gilbane (and its surety).[18] Gilbane brought a third-party complaint against DCAM "effectively alleg[ing] that DCAM should indemnify Gilbane for 'damages caused by design changes and design errors' that were 'unrelated to any wrongdoing on Gilbane's part.'"[19] DCAM moved to dismiss the third-party complaint, arguing that the CMAR statutory scheme and the terms of its contract with Gilbane, requiring Gilbane to "indemnify, defend and hold harmless" DCAM from "all claims… arising out of or resulting from the performance of the Work," trumped the *Spearin* doctrine.[20] The superior court allowed DCAM's motion to dismiss the third-party complaint, and Gilbane appealed.[21] Upon Gilbane's

1. United States v. Spearin, 248 U.S. 132, 136 (1918).
2. Alpert v. Commonwealth, 357 Mass. 306, 320 (1970).
3. Mass. Gen. Laws ch. 149, §44F(1)(a) (2012).
4. *See id.; Spearin,* 248 U.S. at 136; *Alpert*, 357 Mass. at 320 .
5. Mass. Gen. Laws ch. 149A, §6(b)(3), (5) (2005).
6. *See* Mass. Gen. Laws ch. 149, §44F(1)(a) (2012).
7. *See* Mass. Gen. Laws ch. 149A, §7 (2005).
8. Gregory W. Sullivan, Office of the Inspector Gen., Experience of Massachusetts Public Agencies with Construction Management at Risk under M.G.L. c. 149A 9 (2009), available at http://www.mass.gov/ig/public-design-and-construction/alternative-construction-methods/cmatrisk.pdf.
9. *Id.*
10. Coghlin Elec. Contractors, Inc. v. Gilbane Bldg. Co., 472 Mass. 549, 550-51 (2015).
11. *Id.* at 551.
12. *Id.*
13. *Id.*
14. *Id.* at 552.
15. *Id.*
16. Coghlin Elec. Contractors, Inc. v. Gilbane Bldg. Co., 472 Mass. 549, 552 (2015).
17. *Id.*
18. *Id.* at 551.
19. *Id.* at 553 (*quoting* Coghlin Elec. Contractors, Inc. v. Gilbane Bldg. Co., No. 2013-1300-D, at 2, 9 (Mass. Sup. Ct. June 24, 2014).
20. *See* Coghlin Elec. Contractors, Inc. v. Gilbane Bldg. Co., No. 2013-1300-D, at 3 (Mass. Sup. Ct. June 24, 2014).
21. *Coghlin Elec. Contractors, Inc.*, 472 Mass. at 552-53.

motion, the Supreme Judicial Court took direct appellate review.[22]

The court compared the traditional design-bid-build method of government construction contracting, where "'the owner retains an engineer or an architect on a separate contract to complete the design of the public facility,' and once the design is complete, the design is made available to potential bidders and the construction contract is advertised for bid,"[23] leaving "'the risk of design'" with the architect or engineer, with design-build contracting (authorized only for certain public works projects by chapter 149A, sections 14 through 21), where "the owner contracts with a single party that assumes both the design and the construction responsibilities."[24] By comparison, the court found the CMAR method to be more "[s]imilar to the design-bid-build method, [because] the owner enters into separate contracts, one with the designer and one with the CMAR" contractor. Before reaching its conclusion, the court noted the CMAR contractor's consultation role during the finalization of the project design and the CMAR contractor's[25] ability to price a contingency to cover "project costs that are not associated with scope changes or latent conditions."[26] Nonetheless, the court found that an implied warranty of the design by the owner to the contractor still existed.[27] More specifically, the court stated that it was "not persuaded that the relationships [between the owner, the CMAR contractor and the designer] are so different that no implied warranty of the designer's plans and specifications should apply in construction management at risk contracts made pursuant to G.L. c. 149A and that the CMAR should bear all the additional costs caused by design defects."[28] The court further concluded that "a public owner of a construction management at risk project gives an implied warranty regarding the designer's plans and specifications," but noted that "the scope of liability arising from that implied warranty is more limited than in a design-bid-build project."[29]

The extent of the limitation depends on a number of case-specific factors, which could vary depending on the terms of the contracts in issue.[30] The factors identified in the instant case were (i) whether the owner is under any obligation to accept the CMAR's design suggestions or whether the owner's separately-contracted designer maintains control over the design, (ii) whether the CMAR acted reasonably in relying on the design, given the CMAR's contractual design participation role, and (iii) whether the contract language itself contains an express disclaimer of the *Spearin* doctrine protection for the contractor.[31]

As to Gilbane, the court found that DCAM retained control over the project design and that even the "significant design-related obligations" were limited by DCAM's "authority and control over the Project's design."[32] The court held that "Gilbane may be able to recover, but only to the extent that the additional costs were caused by Gilbane's reasonable and good faith reliance on the defective plans and specifications."[33]

The court also interpreted the indemnification provision of the contract in light of the ruling applying the *Spearin* doctrine, and held that "claims, damages, losses, and expenses that arise out of the Designer's performance, as opposed to Gilbane's design consultation and review performance, do not trigger the indemnification provision."[34]

With the applicability of the *Spearin* doctrine to CMAR projects now clarified as a matter contingent on the terms of the negotiable CMAR contract, awarding authorities and CMAR contractors likely will negotiate as to who should accept the risk of design errors. Because the awarding authorities already are mandated to obtain the services of a design professional,[35] who is obligated to carry professional liability insurance,[36] the parties may find the path of least resistance is to maintain the status quo, namely, leaving the risk for design defects with the awarding authority.

Michael P. Sams and Sakib A. Khan

22. Coghlin Elec. Contractors, Inc. v. Gilbane Building Co., 472 Mass. 549, 553 (2015).

23. *Id.* at 554-55 (*quoting* Associated Subcontractors of Mass., Inc. v. Univ. of Mass. Bldg. Auth., 442 Mass. 159, 165 n.8 (2004))

24. *Coghlin Elec. Contractors, Inc.,* 472 Mass. at 554-55 (*quoting* J. Lewin & C.E. Schaub Jr., *Construction Law* §2:6, at 14-15 (2012) (Lewin & Schaub Jr.)).

25. *Coghlin Elec. Contractors, Inc.*, 472 Mass. at 555.

26. *Id.* at 558.

27. *Id.* at 559.

28. Coghlin Elec. Contractors, Inc. v. Gilbane Building Co., 472 Mass. 549, 558 (2015).

29. *Id.* at 550.

30. *Id.* at 557-63. Unlike design-bid-build contracting under chapter 149, §§44A-44H, where the contract form is unilaterally drafted by the awarding authority and published to solicit the lowest bid, chapter 149A, §6 provides for non-price negotiations of the contract form between the awarding authority and the selected CMAR.

31. *Coghlin Elec. Contractors, Inc.*, 472 Mass. at 557-63.

32. *Id.* at 562.

33. *Id.* at 563.

34. Coghlin Elec. Contractors, Inc. v. Gilbane Building Co., 472 Mass. 549, 565 (2015). The court also affirmed the guidance that, "[b]ecause Rule 14 expressly allows what is in effect anticipatory litigation, a third-party defendant may not and should not object on the grounds that the defendant's liability has not yet been established," and rejected DCAM's argument that Gilbane's third-party complaint was premature. *See id*. at 566-67 (*quoting* Reporter's Notes to Mass. R. Civ. P. Rule 14).

35. Mass. Gen. Laws ch. 149A, §3(b).

36. Mass. Gen. Laws ch. 7C, §51(e).

Case Comment

Commonwealth v. Locke, 89 Mass. App. Ct. 497 (2016)

What investigative steps can a police officer take when he or she smells a strong smell of unburnt marijuana coming from a motor vehicle? In *Commonwealth v. Locke*,[1] the Massachusetts Appeals Court addressed that question and, finding itself bound by Supreme Judicial Court precedent, held, "none."

The facts

In *Locke*, Massachusetts State Troopers stopped a minivan on Route 84 after they saw it speeding, changing lanes erratically, and almost causing an accident.[2] When the troopers approached the van's passenger side window, they smelled the "very strong odor of fresh marijuana."[3] The driver was nervous, his chest was heaving, and he talked excessively; the passenger, meanwhile, sat quietly and stared straight ahead.[4] The van was a rental, for which the driver was not an authorized user.[5] Inside of the van, the trooper saw several air fresheners in various locations, which he knew from training and experience to be a tactic used to mask the odor of narcotics.[6] When the trooper explained to the driver the law regarding possession of marijuana, and asked him whether he was in possession of any marijuana or had smoked any, the driver said that he did not possess any marijuana, but that he and the passenger had smoked some earlier in the day.[7] The passenger denied that a smell of marijuana was emanating from the van, and denied smoking any with the driver earlier in the day.[8]

Several minutes later, a trooper with the canine unit arrived; the dog made a positive hit for narcotics near the rear lift gate of the minivan.[9] When the troopers opened the door to the minivan, they noticed that it was "quite stinky, the smell of a lot of marijuana."[10] During a search of the van, the troopers found seven fresh bundles of marijuana totaling 159 pounds.[11] In fact, there was too much marijuana to fit in the troopers' cruisers, so they had to have the van towed with the marijuana inside to the barracks to inventory it.[12] A trial judge suppressed evidence of the marijuana on the grounds that the mere odor of marijuana does not suggest that a criminal amount of marijuana is present.[13]

The Appeals Court rejected the commonwealth's argument that the very strong odor of marijuana (so strong, in fact, that three air fresheners and aerosol spray did not suffice to mask the smell), coupled with the nervous conduct of the defendant and the questionable rental agreement, provided the troopers with reasonable suspicion to believe that there was a criminal amount of marijuana, that is, more than one ounce, in the van.[14] In reaching its decision, the Appeals Court declared itself bound by the Supreme Judicial Court's decision in *Commonwealth v. Overmyer*,[15] in which the court held that, "although the odor of unburnt, rather than burnt, marijuana could be more consistent with the presence of larger quantities, ... it does not follow that such an odor reliability predicts the presence of a criminal amount of the substance, that is, more than one ounce, as would be necessary to constitute probable cause."[16]

The law as it existed before the 2008 voter initiative to decriminalize marijuana, and the post-initiative changes to the law

Locke is the latest example of the difficulty that the police, trial judges, and indeed, the Appeals Court, have had assessing the impact of "An Act establishing a sensible state marihuana policy"[17] ("2008 initiative") upon the ability of police to stop, order passengers from and search a motor vehicle based on the smell of marijuana. Prior to the passage of the 2008 initiative, the law as it related to an officer's ability to stop and search a motor vehicle based on the smell of marijuana was fairly straightforward: the smell of marijuana was sufficiently unique that, when an officer smelled some marijuana, burnt or raw, coming from a motor vehicle, he or she had probable cause to believe more marijuana was inside the vehicle, and hence, that a crime was being committed.[18] Thus, if a police officer smelled marijuana coming from a motor vehicle, he or she could pull that vehicle over or, if during a traffic stop, he or she smelled marijuana coming from inside the vehicle, he or she could issue an exit order and search the vehicle pursuant to the motor vehicle exception to the warrant requirement.[19]

1. 89 Mass. App. Ct. 497, *rev. denied*, 475 Mass. 1101 (2016).
2. *Id.* at 498.
3. *Id.* at 498 n. 3.
4. *Id.* at 498-99.
5. *Id.* at 499.
6. Commonwealth v. Locke, 89 Mass. App. Ct. 497, 499 (2016).
7. *Id.* at 499-500.
8. *Id.*
9. *Id.* at 500.
10. *Id.*
11. *Id.*
12. Commonwealth v. Locke, 89 Mass. App. Ct. 497, 500 (2016).
13. *Id.* at 498.
14. *Id.* at 503-04. The Appeals Court also held that the facts did not give rise to a fear for the officer's or another person's safety. *Id.* at 502-03.
15. 469 Mass. 16 (2014).
16. *Locke*, 89 Mass. App. Ct. at 503 (*quoting Overmyer*, 469 Mass. at 21).
17. St. 2008, c. 387. The passage of the 2008 initiative was codified in Mass. Gen. Laws ch. 94C, §§32L-32N (2016).
18. Commonwealth v. Garden, 451 Mass. 43, 48 (2008).
19. *Id.; see also* Commonwealth v. Daniel, 464 Mass. 746, 750-51 (2013) (discussing the automobile exception to the warrant requirement).

This changed in 2008, when the people of Massachusetts voted to make the possession of less than one ounce of marijuana a civil violation only, subjecting the possessor to a fine and forfeiture of the marijuana.[20,21] This "statutory decriminalization of possession of small amounts of marijuana has affected aspects of related criminal laws and, consequently, the law of search and seizure."[22] The effect of the 2008 initiative has spawned a series of cases that has significantly altered what the police may do when they smell marijuana coming from a vehicle.[23]

The court first addressed the impact of the 2008 initiative on the police's ability to order a person from a motor vehicle in *Commonwealth v. Cruz*.[24] In *Cruz*, the police, upon approaching a vehicle that was parked in front of a fire hydrant, and in which an individual was seen lighting a "blunt," could smell the "faint odor" of burnt marijuana coming from the car.[25] Based largely on the odor of marijuana coming from the car, the police ordered the defendant and another passenger from the car, searched the defendant, and recovered a rock of crack cocaine from his pocket.[26] The court noted that although, prior to 2008, the smell of burnt marijuana gave police probable cause to believe that the criminal activity was underway, it was necessary to reconsider its jurisprudence in the light of the 2008 initiative.[27] The court first held that, because an officer can only issue an exit order based on reasonable suspicion that a crime has been, is being, or is about to be committed, and because possession of less than one ounce of marijuana was no longer a crime, the police could not issue an exit order based solely on the belief that the person possessed marijuana unless they had reasonable suspicion that the person possessed more than an ounce of marijuana.[28] Succinctly put, "the odor of burnt marijuana alone cannot reasonably provide suspicion of criminal activity."[29] The court also held that, despite marijuana's continued status as "contraband,"[30] and despite case law that permitted officers to search a motor vehicle pursuant to the motor vehicle exception to the warrant requirement so long as the police had probable cause to believe that the vehicle contained contraband, the automobile exception only applied where there was probable cause to believe that a criminal amount of marijuana was in the car.[31,32]

Next, in *Commonwealth v. Overmyer*, the court considered whether the strong smell of unburnt marijuana coming from a vehicle, coupled with the removal of a "fat bag" of marijuana which was "rather large" from the car's glove box (with the defendant's consent), provided police with grounds to search the car for more marijuana — particularly where they could still smell a strong scent of marijuana despite having removed the "fat bag."[33] The answer to that question, according to the court, was "no."[34] Again noting that police can only search a car pursuant to the motor vehicle exception where there is probable cause to believe a crime is being committed, the court held that, unless an officer has undergone specialized training to use the smell of marijuana as a gauge of weight, "[a]s a subjective and variable measure, the strength of a smell is ... at best a dubious means for reliably detecting the presence of a criminal amount of marijuana."[35]

Most recently, in *Commonwealth v. Rodriguez*, the court considered whether the police can stop a moving motor vehicle from which they smell an odor of burnt marijuana in order to issue a citation and seize the marijuana, which, by statute, is subject to forfeiture.[36] Again, the answer was, "no."[37] The court first explicitly overruled its prior declaration in *Garden* that the smell of marijuana, whether burnt or unburnt, was sufficiently unique to create probable cause to believe that additional marijuana was nearby, and declared that the smell of burnt marijuana was "insufficiently nuanced" to provide an officer with probable cause to believe that additional marijuana could be inside of a vehicle.[38] Nevertheless, the court held that, although the smell of burnt marijuana did not give rise to probable cause to believe that additional marijuana was in the vehicle, it gave rise to reasonable suspicion to so believe.[39] It then balanced the intrusiveness of a motor vehicle stop against the governmental interests served by stopping vehicles from which the police smell

20. *See* Mass. Gen. Laws ch. 94C, §32L (2016).

21. Massachusetts law governing the possession of marijuana changed yet again in 2016 with the passage of Initiative Petition 15-27: *An Initiative Petition for a Law Relative to the Regulation and Taxation of Marijuana*. This will be discussed further below.

22. *Daniel*, 464 Mass. at 751.

23. The 2008 initiative has impacted other areas of the law as well. For example, in Commonwealth v. Jackson, 464 Mass. 758, 765-66 (2013), the court overruled the Appeals Court's decision in Commonwealth v. Lawrence, 69 Mass. App. Ct. 596, 602-03 (2007), which had held that the passing of a marijuana cigarette constituted distribution. In *Jackson*, the court first established the concept of "social sharing" of non-criminal amounts of marijuana. *Jackson*, 464 Mass. at 766.

24. 459 Mass. 459 (2011).

25. *Id.* at 462.

26. *Id.* at 462-63.

27. *Id.* at 464.

28. *Id.* at 469.

29. *Id.* at 472.

30. *See* Commonwealth v. Bostock, 450 Mass. 616, 624 (2008) (holding that the motor vehicle exception to the warrant requirement applies "to situations where the police have probable cause to believe that a motor vehicle parked in a public place and apparently capable of being moved contains contraband or evidence of a crime") (emphasis supplied).

31. Commonwealth v. Cruz, 459 Mass. 459, 473-76 (2011). In reaching the conclusion that officers could only search a vehicle based on probable cause to believe that there was a criminal amount of marijuana inside, the court relied upon Robinson v. Richardson, 79 Mass. 454 (1859). *Robinson* addressed the question whether an assignee of the estate of an insolvent debtor could obtain a warrant to search for property and books of account which they suspected had been concealed. *Id.*

32. In the wake of *Cruz*, the court held in Commonwealth v. Daniel, 464 Mass. 746, 756-57 (2013), and Commonwealth v. Pacheco, 464 Mass. 768, 769-70 (2013), that a police officer may not search a motor vehicle even if, during a lawful motor vehicle stop, the officer sees less than an ounce of marijuana inside of the vehicle. The court furthered this rule in Commonwealth v. Sheridan, 470 Mass. 752, 757 (2015), in which it held that police cannot search a car for marijuana merely because it is subject to forfeiture, even when they observe a bag of marijuana that weighs about an ounce. And, in Commonwealth v. Craan, 469 Mass. 24, 33 (2014), the court held that, when the 2008 initiative decriminalized possession of less than one ounce of marijuana in Massachusetts, it also had the effect of curtailing local and state police authority to enforce the Federal prohibition of a small amount of marijuana.

33. Commonwealth v. Overmyer, 469 Mass. 16, 20-23 (2014).

34. *Id.*

35. *Id.* at 22.

36. Commonwealth v. Rodriguez, 472 Mass. 767, 767-68 (2015).

37. *Id.*

38. *Id.* at 775.

39. *Id.*

marijuana, and held that the "humiliating, frightening, and embarrassing" effects of a motor vehicle stop outweighed the governmental interest in stopping a vehicle.[40] More particularly, the court held that, while a stop of a motor vehicle may be constitutionally permissible when police have a reasonable suspicion to believe that a traffic violation statute has been violated, such statutes promote public safety; "[n]o similar governmental interest supports allowing police to stop a motor vehicle based on reasonable suspicion that someone in the vehicle possesses an ounce or less of marijuana."[41] Because the officers in *Rodriguez* only stopped the vehicle to investigate whether a civil citation for possession of less than an ounce of marijuana was appropriate, the stop was unconstitutional.[42]

Justice Cordy authored a vigorous dissent in *Rodriguez*, which was joined by Justice Spina. To them, there was no principled difference between stopping a motor vehicle upon reasonable suspicion to believe that the vehicle had committed a civil traffic violation, and the belief that a non-criminal amount of marijuana was inside the car, in order to issue the requisite citation.[43] The dissenters also urged that "[n]othing has occurred that warrants a reconsideration of [the] common-sense conclusion [that the odor of marijuana is sufficiently unique that it alone can provide probable cause to believe that marijuana is nearby]."[44]

The Appeals Court's analysis in *Locke*

Against the backdrop of these cases, the Appeals Court held in *Locke* that the troopers could not search the defendant's vehicle, regardless of how strong and fresh the smell of marijuana emanating from the van.[45] The Appeals Court reached this conclusion grudgingly; it noted that although the "very strong" smell of raw marijuana that the trooper detected came from 159 pounds of marijuana in the vehicle (or, as the Appeals Court put it, 2,544 times the amount of marijuana it was not criminal to possess), the outcome of the case was controlled by *Overmyer's* conclusion that "one cannot reliably determine weight from smell alone."[46] In reaching its decision, the Appeals Court took the opportunity to opine that the Supreme Judicial Court's decision in *Overmyer* had, "in [the Appeals Court's view], driven our jurisprudence away from the intent of the 2008 ballot initiative."[47] In so opining, the Appeals Court stated:

> ... our sense of smell permits us to determine relative quantity as a matter of routine and with reliability; we may not know the precise number of loaves being baked at the bakery, but we know from the smell alone that it is more than one; a burning house does not cause us to exclaim, "I smell a match" ... It is difficult to imagine that, when the voters of the commonwealth chose to decriminalize the possession of less than one ounce of marijuana, they also intended to limit law enforcement's ability to investigate and curtail the interstate transport of 2,544 times that amount. After all, the 2008 initiative left intact the overarching proposition that "possession of marijuana, in any amount, remains illegal" and "any amount of marijuana is considered contraband." ... Here the smell of marijuana was "very strong" and that should have been enough to support a reasonable suspicion, or probable cause, that a criminal amount of marijuana was present.[48]

The Appeals Court's decision in *Locke* is noteworthy for at least three reasons. First, it serves as a reminder that all lower courts — including the Appeals Court — are duty-bound to follow the decisions of the Supreme Judicial Court, even when the lower courts may have a different view of the law.[49]

Second, the Appeals Court's decision in *Locke* goes a long way toward providing stability and predictability in an area of the law that has been in flux since the passage of the 2008 initiative. Citizens and police alike benefit from the predictability that comes with a bright line rule.[50] Given the inevitable path that has been set in place by decisions like *Cruz, Overmyer* and *Rodriguez*, the Appeals Court erased any lingering thoughts that an overpowering smell of unburnt marijuana could provide a basis to stop and search a motor vehicle by establishing a bright line rule: unless the officer specifically testifies that he or she has been trained to gauge the weight of marijuana based on odor, the smell of marijuana alone is, for all intents and purposes, meaningless, regardless of how overpowering it is. It is thus now clear that an officer cannot stop a motor vehicle based solely on an overwhelming smell of burnt marijuana coming from the vehicle; he or she cannot order passengers from a motor vehicle based solely on an overpowering scent of burnt or unburnt marijuana coming from a vehicle; and he or she cannot search a motor vehicle regardless of how strong and overpowering the smell of burnt or unburnt marijuana emanating from inside of the vehicle.[51] To the extent that *Locke* provides a bright line rule, it is a good thing.

Third, the Appeals Court was correct that, in reaching its decision, it was bound to follow decisions that have "driven our jurisprudence away from the intent of the 2008 ballot initiative."[52] In developing the law in this area since the 2008 initiative, the Supreme Judicial Court has gone to great lengths to give voice to what it considered to be the voters' intent in passing the 2008 initiative:[53]

40. *Id*. at 776.

41. *Id*. at 777. The court differentiated simple marijuana possession from the offense of operating a vehicle under the influence of marijuana, which it declared "a serious offense that may well present safety hazards requiring the immediate involvement of police." *Id.* at 777 n.16.

42. Commonwealth v. Rodriguez, 472 Mass. 767, 776-77 (2015). The court distinguished the stop of a motor vehicle based on the smell of burnt marijuana from a situation where an officer comes across a person smoking marijuana in a public park. *Id.* In such a situation, the court held, it would be permissible for the officer to stop the person to investigate whether a civil violation was being committed. *Id.*

43. *Id*. at 781 (Cordy, J., dissenting).

44. *Id.*

45. Commonwealth v. Locke, 89 Mass. App. Ct. 497, 503-04 (2016).

46. *Id*. at 503 n.9.

47. *Id.*

48. *Id*. (internal citation omitted).

49. *See* Commonwealth v. Dube, 59 Mass. App. Ct. 476, 485 (2003).

50. *See generally* Commonwealth v. Powell, 468 Mass. 272, 280-281 (2014).

51. The Supreme Judicial Court has implicitly blessed the Appeals Court's holding by denying the commonwealth's petition for further appellate review on the issue. *See* Commonwealth v. Locke, 475 Mass. 1101 (2016).

52. Commonwealth v. Locke, 89 Mass. App. Ct. 497, 503 n.9 (2016).

53. Indeed, in several of its decisions, it has referenced the intent of the voters. *See* Commonwealth v. Cruz, 459 Mass. 459, 470-71 (2011); Commonwealth v. Rodriguez, 472 Mass. 767, 777-78 (2015); *see also* Commonwealth v. Craan, 469 Mass. 24, 33-34 (2014) (referencing objective of 2008 initiative in holding that state and local agencies could not investigate federal crime of possession of marijuana).

in *Cruz*, the court relied on a case from 1859 which held that an assignee of the estate of an insolvent debtor could obtain a warrant to search for property and books of an account they suspected had been concealed, to reach the conclusion that, although police can search for contraband based on probable cause, they can only search for contraband that it is a crime to possess;[54] in *Overmyer*, the court reached the conclusion that an ordinary person cannot tell by smell alone whether marijuana weighs more than an ounce,[55] despite that, as the Appeals Court noted in *Locke*, we all make such distinctions on a near daily basis;[56] and in *Rodriguez*, the court did away with its previous declaration that, as a matter of common sense, the smell of some marijuana can supply probable cause to believe that more marijuana is nearby, and held that police could not stop a motor vehicle in order to investigate the civil violation of possessing less than one ounce of marijuana, even when police had reasonable suspicion to believe that a civil violation was being committed.[57]

Nothing in the 2008 initiative, however, suggests that the voters intended to divest the police of one of their most important and common-sense tools in investigating whether the civil violation of possessing less than one ounce of marijuana, or the criminal offense of possessing more than one ounce of marijuana, was being committed: the tell-tale smell of marijuana. Although the proponents of the initiative argued that decriminalization would free officers from making marijuana-based arrests and allow them to focus on investigating other crimes, they did not argue that the initiative would or should prevent officers from enforcing the civil fine and forfeiture provisions, or investigating marijuana-based crimes. To the contrary, the drafters of the ballot initiative took pains to make clear that "the possession of marijuana, in any amount, remains illegal," and "any amount of marijuana is considered contraband."[58] As Justice Cordy noted in dissent in *Rodriguez*, nothing in the initiative suggested that the voters intended to curtail an officer's ability to investigate the civil infraction of possessing less than an ounce of marijuana, particularly where officers are empowered to investigate similar civil infractions involving motor vehicle violations.[59] In fact, in their argument in favor of the 2008 initiative, proponents of the measure specifically likened the civil fine to a speeding ticket.[60] Nor, as the Appeals Court noted in *Locke*, is there anything to suggest that the voters intended to hinder an officer's ability to investigate the crime of possessing over an ounce of marijuana where the officer smells the "very strong" smell of marijuana,[61] particularly where the 2008 initiative made plain that nothing contained within it "shall be construed to repeal or modify existing laws ... or policies concerning ... possession of more than one ounce of marijuana."[62]

As John F. Kennedy said, however, "change is the law of life."[63] Just months after the Supreme Judicial Court denied further appellate review in *Locke*, the legal landscape involving the possession of marijuana shifted yet again. On November 8, 2016, Massachusetts voters approved a ballot initiative legalizing individual possession of less than one ounce of marijuana.[64] That voter-approved initiative, which was certified by the Governor's Council on December 14, 2016,[65] authorizes a person over the age of 21 to legally possess up to one ounce of marijuana outside of one's home, and up to 10 ounces of marijuana inside of one's home.[66]

Nevertheless, as with the 2008 initiative, the scope of the 2016 initiative is carefully circumscribed. It remains a criminal offense to possess more than two ounces of marijuana outside of one's home,[67] as does possession of marijuana with the intent to distribute or distribution of any amount for remuneration.[68] Indeed, the initiative itself declares that the intent of the Act is to control the production and distribution of marijuana under a regulated system in order to remove the production and distribution of marijuana from the illicit market.[69] In short, although the 2016 initiative legalized the possession of small amounts of marijuana, it did not wholesale legalize the possession or distribution of marijuana; to the contrary, the initiative decidedly intended for police to continue to investigate the illicit market of marijuana-based crimes.

Against this new backdrop, the rule set out in *Locke* and the rationale of the cases that it was bound to follow are sure to set the tone for future litigation involving the smell of marijuana. Even so, the practical concerns raised by the Appeals Court in *Locke* regarding the (in)ability of police to investigate the possession of a criminal amount of marijuana (at least while in public) based on the strong smell of marijuana will remain. Perhaps, in the future, the Supreme Judicial Court will be called upon to decide a case where the smell of marijuana was so overpowering that no other conclusion could be reached but that the smell came from a plainly criminal amount of marijuana. Until that day, the rule appears to be that, standing alone, the smell of marijuana, no matter how overpowering, means nothing.

Zachary Hillman

54. *Cruz*, 459 Mass. at 476 (*citing* Robinson v. Richardson, 79 Mass. 454, 456-57 (1859)).

55. Commonwealth v. Overmyer, 469 Mass. 16, 21-22 (2014).

56. *Locke*, 89 Mass. App. Ct. at 503 n.9.

57. *Rodriguez*, 472 Mass. at 775-76.

58. *Cruz*, 459 Mass. at 473.

59. Commonwealth v. Rodriguez, 472 Mass. 767, 778-82 (2015) (Cordy, J., dissenting).

60. *Information for Voters: 2008 Ballot Questions, Question 2: Law Proposed by Initiative Petition, Possession of Marijuana: Arguments*, Sec'y of the Commonwealth of Mass., available at http://www.sec.state.ma.us/ele/ele08/ballot_questions_08/quest_2.htm.

61. Commonwealth v. Locke, 89 Mass. App. Ct. 497, 503 n.9 (2016).

62. An Act Establishing a Sensible State Marihuana Policy, St. 2008, ch. 387 (codified at Mass. Gen. Laws ch. 94C, §§32L-N (2012)).

63. Address in the Assembly Hall at the Paulskirche in Frankfurt (266), June 25, 1963, *Public Papers of the Presidents: John F. Kennedy*, 1963.

64. Petition 15-27: *An Initiative Petition for a Law Relative to the Regulation and Taxation of Marijuana.*

65. The Regulation and Taxation of Marijuana Act, St. 2016, ch. 334 (codified at Mass. Gen. Laws ch. 94G, §§1-14 (2016)).

66. Mass. Gen. Laws ch. 94G, §7(a).

67. Under the new regime, it is a civil offense punishable by a fine to possess between one and two ounces of marijuana outside of one's home. Mass. Gen. Laws ch. 94G, §13(e).

68. Mass. Gen. Laws ch. 94G, §7(a).

69. Petition 15-27, §1.

Book Review

Future Crimes

by Marc Goodman, Anchor Books (Reprint ed. 2016), 608 pages

On the Internet, creativity is king and that is both good and bad. Focus for a moment on the bad. For example, suppose you want to crowd source a bank robbery. You can do it. In fact, Anthony Curcio did. On Craigslist, he solicited construction workers for a $30 an hour road maintenance job. To qualify, workers had to provide their own equipment including a yellow safety vest, goggles, a blue work shirt, tool belt, hard hat and respiratory mask. So equipped, they were to appear at a designated location near a downtown Seattle Bank of America at 11 a.m. on a specified date. At 11 a.m. on the appointed day, an armored truck arrived at the bank to deliver its weekly supply of cash. As a guard was carrying bags of cash into the bank, a man wearing a yellow safety vest, goggles, a blue work shirt, tool belt, hard hat and respiratory mask suddenly appeared. That was Anthony. After pepper spraying the guard, he grabbed several bags of cash, stuck them in a large duffel bag and disappeared down the street. It took the guard a little time to recover but upon recovery he called police and described the robber perfectly. As police cars converged on the scene from all directions, multiple officers began to report that they had successfully taken the suspect into custody. They each had a different suspect, of course, but Anthony was not among them. In fact, Anthony, who had quickly ditched his construction gear, was nowhere to be found.[1]

Suppose, though, that you want something a little more, shall we say, corporate. Everyone on the Internet is concerned about virus infestations, so how about an anti-virus product. That's the route taken by Innovative Marketing, a small Ukrainian startup that aggressively marketed and sold software to detect and remove viruses and other undesirable software from home and business computers. As the company grew from a handful of programmers, it moved to increasingly larger offices in Kiev and organized itself into various departments — quality assurance, billing, marketing, human resources and the like — to keep up with its increasing volume of business. Ultimately, the company employed some 600 employees marketing products to customers in 60 countries.

Those customers could buy and install the company's software, called "System Defender," by responding to Internet advertising. Most customers, however, encountered the product when an audible alarm interrupted their online sessions and the words "Warning: Serious Virus Detected" appeared on their screens. Within seconds, the company's "System Defender" logo appeared on the screen accompanied by a magnifying glass through which the software appeared to be processing files the computer held. When the processing sequence ended, a new message stated the number of viruses or other spyware the scan had discovered. That message was accompanied by a red button containing the words "remove threats." Clicking on the button took the user to a page where the company's "System Defender" program was available for $49. Clicking elsewhere or even rebooting did not remove the screen. Eventually, most people purchased the program, installed it and watched it periodically sweep their computers to detect and remove various threats the sweeps detected.

In reality, however, Innovative Marketing was selling crimeware, a term for products designed to rob unsuspecting customers of their money and often their identities. The "scans" the user saw before and after installing "System Defender" were an illusion. Nothing was scanned and nothing was really detected. Instead, the "System Defender" program busily removed any real antivirus software it encountered and established a method for others engaged in the crimeware trade to install programs designed to fleece the user. In three years of operation before it was shut down, Innovative Marketing had $500 million in global sales.[2]

Both of those creative approaches to self-enrichment, along with a great many others, are recounted in Marc Goodman's *Future Crimes,* a richly detailed and heavily annotated account of Internet criminal activity. The book made several bestseller lists when first published in 2015 and the updated paperback edition published in January, 2016 remains widely read. Though the title suggests a look ahead, much of the book's content would lead a reasonable observer to conclude that the future is with us today. Goodman began investigating Internet criminal behavior in the mid-90s as a member of the Los Angeles Police Department. During the ensuing 20 years, he has made researching and investigating Internet crimes his principal activity and, indeed, his passion. That passion resonates in his TED talk as it does on each of the nearly 500 pages *Future Crimes* contains.

The book, though, is much more than a compendium of successful and unsuccessful scams. Intertwined with specific examples of large and small things gone wrong is a discussion of the vulnerabilities lurking in all of the undeniable benefits the Internet has produced and will continue to produce in our personal and industrial lives. Revelations over the past few years, and congressional action in response to those revelations, have alerted us to the extent of governmental surveillance of Internet activities. Goodman's focus is chiefly on private profiteering, now and anticipated, as we

1. Marc Goodman, *Future Crimes,* (Anchor Books 2016), at 240-41; *Anthony Curcio,* Wikipedia.com, https://en.wikipedia.org/wiki/Anthony_Curcio (last visited Oct. 18, 2016).
2. *Id.* at 215-20.

move forward into the "Internet of things," the name attached to the growing Internet connectivity of private and industrial objects from thermostats to machines that control our nation's electrical grid. Indeed, his short introduction to the book ends with a warning that "if you proceed in reading the pages that follow, you will never look at your car, smart phone or vacuum cleaner the same way again."[3]

He is probably correct, for his narrative suggests that all of us are engaged in a routine of daily self-revelation that would have been absolutely unthinkable when Warren and Brandeis wrote their famous article on loss of privacy more than 125 years ago.[4] Begin with our cell phones. Cell phones are constantly with us and we at least generally know that they can track our activities. Less apparent is how easily they can be hacked. The ease of surreptitious entry was illustrated dramatically by revelations that staff of Rupert Murdoch's *News of the World* had impeded the investigation of a missing teenage girl by hacking into her cell phone and likewise had hacked into the phones of numerous celebrities, members of the royal family and relatives of British soldiers killed in Iraq and Afghanistan.[5]

But hacking is not the only problem. For example, a readily available "app" called Mobile Spy allows one individual to monitor, in real time, all of the telephone conversations, photographs, texts, chats and other activities being carried out on cell phones belonging to someone else.[6] Moreover, various applications we purchase and install on our phones are constantly recording and transmitting large quantities of personal data unrelated to the application's primary functions.[7]

Cell phones are not the only pathway to vast quantities of personal information. For example, Goodman describes an incident in which officials in an affluent Pennsylvania school district provided 2,300 high school students with MacBook laptops. One day, one of the recipients was summoned to the principal's office where he was informed that school officials were aware that he was dealing drugs. After denying the allegations, the student was shown a photograph taken in his own bedroom that purported to reveal his possession of contraband pills. It turned out that the photograph had been taken by the laptop's camera, which school officials had retained the ability to control remotely on all of the distributed computers. The contraband turned out to be candy and the incident produced an uproar that ultimately involved lawsuits and criminal investigations into the behavior of district officials.[8] But, Goodman tells us, that camera is always there and the software to operate it remotely is out there too.

To be sure, the school district's outrageous behavior is an outlier. Nevertheless, we have voluntarily and involuntarily allowed others to capture a great deal of information about us as we go about our daily lives. On the voluntary side, the terms of service to which we agree when we install or use a new application on our cell phones, laptops, automobiles, or anything else that is connected to the Internet often give the vendor the right to compile, track and distribute to others a vast array of information about the circumstances under which we are using the application and the information the application gathers. In addition, those terms frequently give the vendor a worldwide and perpetual right to use, reproduce and display any document, photograph, or video stored on the cloud or in any other location the vendor maintains. Those terms of service typically are dense and extensive, so few purchasers read them.[9]

The involuntary part can be just as invasive. For example, Goodman recounts an incident in which a father learned that his teenage daughter was pregnant when she began receiving mailed flyers from Target, the large retailer, advertising baby products. She received those flyers because Target had created an algorithm that aggregated a customer's entire purchase history with demographic statistics Target purchased from data brokers. By using that algorithm, Target was able to analyze purchases of products by female customers to create a "pregnancy prediction score" so that it could begin sending women ads for baby products before the child was born.[10] In the same vein, several large national retail stores now track the amount of time customers spend in various locations within the store and use that information for marketing purposes.[11]

Tracking is one thing. Manipulation is something else, but it, too, occurs. In 2014, Facebook participated in an experiment in which it provided 700,000 users with "happy" or "sad" news on a controlled basis. Researchers then watched the recipients' Facebook postings and concluded and that those who received the negative news tended to have more negative postings and that more upbeat postings emanated from those who received the happy news. The results were published by the National Academy of Sciences but none of the subjects of the experiment, who included children between the ages of 13 and 18, had been told that they were participating in a study or that the news they were receiving was being culled for study purposes.[12]

Most of that is perfectly legal, even if highly disquieting. But the Internet also hosts a rich array of the clearly illegal. Much of the illegal part is in the hands of organized crime and resides in a vast component of the Internet most of us have never encountered or even heard of. Known as the "Deep Web," that component is 500 times larger than the surface web that we encounter daily. According to Goodman, our routine Google searches look at only .03 percent of the information contained on the Internet and do not access the Deep Web at all.

On the Deep Web one can find all manner of unsavory things — narcotics, weapons, pirated movies, fake identity documents, software and even assassins.[13] One variety of the software is something called "ransomware," which is used to encrypt all of the data stored on the victim's computer so that the data is no longer accessible. The victim is then notified that the data will be destroyed unless he or she pays a fee to have the encryption removed.[14] Among many others, the Tewksbury, Massachusetts Police Department was a victim

3. *Id.* at 5.
4. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
5. Goodman, *supra* note 1, at 131-32.
6. *Id.* at 141-43.
7. *Id.* at 137-39.
8. *Id.* at 303-04.
9. *Id.* at 69-73.
10. *Id.* at 91-92.
11. Goodman, *supra* note 1, at 145-46.
12. *Id.* at 409-10.
13. *Id.* at 253-64.
14. *Id.* at 278-80.

of a ransomware attack in April, 2015.[15] Purchases and sales on the Deep Web take place using alternative currencies like Bitcoin. Purchasers and sellers are often rated for their reliability and the quality of their products, just as if they were conducting transactions on eBay or another channel for legitimate commerce.

Much Internet criminal activity builds on personal information we have provided to others voluntarily for use in legitimate transactions. Thieves then steal that information by hacking insecure data storage systems, gathering the personal data we have provided, and then using that data to invade our bank and credit card accounts. One of the largest thefts of that sort occurred in 2007 when thieves penetrated a database maintained by TJX, the parent company of T.J. Maxx and Marshalls stores in the United States. In that episode, the thieves obtained credit card information provided by at least 45 million and perhaps as many as 94 million individuals.[16] Sometimes, though, personal information is handed over to criminals accidentally. In 2014, for example, Experian, one of the country's largest data brokers, mistakenly sold a huge volume of personal data to an organized Vietnamese crime group specializing in identity theft.[17]

Goodman foresees a deepening problem as we proceed more deeply into the "Internet of things." For instance, thermostats, automobiles, and even light bulbs are now hooked up to the Internet either directly or through a Bluetooth connection to other devices, and, as such, are vulnerable to hacking. As a result, those Internet connections can yield information about when we are home, when we are away, and where we are when we are away, thereby providing criminals with information and opportunities limited only by their creativity. He suggests that those opportunities will increase with gathering speed in the coming years as the proliferation of "smart" devices reaches into more and more of our personal space.[18]

In Goodman's view, there is no magic bullet to stop the opportunities for criminal behavior that the Internet affords. Nevertheless, he does propose a series of risk-reducing steps all of us can take, but they all require a heightened consciousness of risk, coupled with collaborative action. More deeply, his approaches require individual and collective judgments about the proper balance between the benefits the Internet provides and the intrusion with which those benefits are accompanied.[19]

This is an alarming but important book, though its length may deter some from proceeding to the end. Goodman could have made the same important points without some unnecessary repetition. Despite the alarms the book contains, Goodman is not an alarmist. Other thoughtful observers like Evgeny Morozov[20] and Sir Martin Rees[21] have been raising similar concerns, albeit in different contexts, for years. But the Internet has become and will remain a fundamental component of our social order. Its benefits and accompanying vulnerabilities will proliferate with increasing speed as we move forward. Both have the capacity to control us unless we take conscious and collaborative steps to control them. This book makes that necessity clear.

James F. McHugh

15. Hiawatha Bray, "When Hackers Cripple Data, Police Departments Pay Ransom," Boston Globe, April 6, 2016 (https://www.bostonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcoin-ransom-hackers/PkcE1GBTOfU52p31F9FM5L/story.html) (last visited Oct. 18, 2016).
16. Goodman, *supra* note 1, at 22.
17. *Id.* at 111-12.
18. *Id.* at 281-330.
19. *Id.* at 451-93.
20. *See* Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs 2011).
21. *See* Sir Martin Rees, *Our Final Hour* (2003).

100 Years of Massachusetts Law Review — Available. Searchable. Online.

Massachusetts Bar Association members can now search every past issue of the *Massachusetts Law Review* online through a partnership with HeinOnline.

The *Massachusetts Law Review* is the longest continually published law review in the nation. Now, MBA members can view every issue, starting with the *Massachusetts Law Quarterly* (the original name of the *Massachusetts Law Review*) Vol. 1, No. 1, from November 1915, through the most recent *Massachusetts Law Review,* Vol. 98, No. 3. Using the HeinOnline search function, users can type in a search term (e.g., "eminent domain") to find all of the *Massachusetts Law Review* articles over the past 100 years, where that term has appeared.

Previously, the MBA website included only the most recent issues of *Massachusetts Law Review*, and older issues had to be looked up on microfiche. There was also no way to search past issues by keyword.

Log in under the "Publications" tab on www.MassBar.org for easy access to the law review's articles, case comments and book reviews, using an online, searchable database. This service is provided to MBA members as a free member benefit.

The *Massachusetts Law Review* archive on HeinOnline also works seamlessly with the MBA's recently introduced Fastcase benefit. In many cases, citations to Massachusetts appellate court opinions that appear in the law review articles will hyperlink directly to the opinion itself.

MASSBAR ASSOCIATION
THE PREEMINENT VOICE OF THE LEGAL PROFESSION

www.MassBar.org • 617.338.0500

Massachusetts Bar Institute
20 West St.
Boston, MA 02111-1204