

COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

No. SJC-11482

COMMONWEALTH,

Appellant,

v.

SHABAZZ AUGUSTINE,

Defendant-Appellee.

BRIEF OF MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE
LAWYERS AS AMICUS CURIAE IN SUPPORT OF APPELLEE

Elizabeth A. Lunt
(BBO #307700)
ZALKIND, DUNCAN & BERNSTEIN
65A Atlantic Avenue
Boston, MA 02110
(617) 742-6020
President,
Massachusetts Association of
Criminal Defense Lawyers

Alex G. Philipson
(BBO #637528)
PHILIPSON LEGAL
97 Montvale Road
Newton Centre, MA 02459
(617) 671-9015
Co-Chair, Amicus Curiae
Committee,
Massachusetts Association of
Criminal Defense Lawyers

Louis W. Tompros
(BBO #657791)
Kevin S. Prussia
(BBO #666813)
Thaila K. Sundaresan
(BBO #683616)
Matthew J. Tokson
(Pro Hac Vice)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

*Attorneys for
Massachusetts Association
of Criminal Defense
Lawyers*

TABLE OF CONTENTS

| | |
|---|----|
| TABLE OF AUTHORITIES..... | IV |
| STATEMENT OF INTEREST..... | 1 |
| SUMMARY OF ARGUMENT..... | 2 |
| ARGUMENT | 4 |
| I. THIS COURT SHOULD REJECT THE THIRD-PARTY DOCTRINE AS INAPPLICABLE TO MODERN TECHNOLOGIES AND HOLD THAT MONITORING OF CELL PHONE LOCATION DATA IS A SEARCH UNDER ARTICLE 14..... | 4 |
| A. ARTICLE 14 OF THE MASSACHUSETTS DECLARATION OF RIGHTS IS BROADER IN SCOPE THAN THE FOURTH AMENDMENT, AND ACCORDINGLY, MASSACHUSETTS NEED NOT FOLLOW THE THIRD-PARTY DOCTRINE..... | 4 |
| B. THIS COURT HAS PREVIOUSLY DECLINED TO FOLLOW THE THIRD-PARTY DOCTRINE..... | 6 |
| C. SEVERAL STATES HAVE ALREADY REJECTED THE THIRD-PARTY DOCTRINE, AND HAVE NOT SUFFERED ANY NOTICEABLE INCREASE IN CRIME..... | 10 |
| D. SMITH V. MARYLAND OFFERS A VERY POOR ANALOGY TO THE INSTANT CASE..... | 12 |
| 1. The third-party doctrine was developed in cases such as <i>Smith</i> that involved vastly different technologies than that addressed in the instant case..... | 13 |
| 2. The U.S. Supreme Court has backed away from the third-party doctrine and has called its viability into question..... | 17 |

| | | |
|------------|--|----|
| 3. | The differences between this case and <i>Smith</i> outweigh any similarities..... | 21 |
| E. | IF EXTENDED TO MODERN TECHNOLOGY, THE THIRD-PARTY DOCTRINE WOULD ELIMINATE CITIZENS' RIGHTS TO PRIVACY IN NEARLY ALL OF THEIR PERSONAL INFORMATION..... | 30 |
| CONCLUSION | | 42 |

TABLE OF AUTHORITIES

| | Page(s) |
|--|----------------|
| FEDERAL CASES | |
| <u>Bond v. United States,</u> 529 U.S. 334 (2000) | 18, 19 |
| <u>City of Ontario v. Quon,</u> 130 S.Ct. 2619 (2010) | 20, 31 |
| <u>Ferguson v. City of Charleston,</u> 532 U.S. 67 (2001) | 19, 20, 29 |
| <u>Harris v. United States,</u> 331 U.S. 145 (1947) | 5 |
| <u>Hoffa v. United States,</u> 385 U.S. 293 (1966) | 13, 27, 31 |
| <u>In re Application for Pen Register and Trap/Trace Device,</u> 396 F. Supp. 2d 747 (S.D. Tex. 2005) | 26 |
| <u>In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register,</u> 402 F. Supp. 2d 597 (D. Md. 2005) | 25, 26 |
| <u>In re Application of the U.S. for Historical Cell Site Data,</u> 747 F. Supp. 2d 827 (S.D. Tex. Oct. 29, 2010) ... | 25 |
| <u>In re Application of the U.S. for Historical Cell Site Data,</u> No. 11-20884, 2013 WL 3914484 (5th Cir. July 30, 2013) | 32 |
| <u>Katz v. United States,</u> 389 U.S. 347 (1967) | 10, 15, 16, 37 |
| <u>Rehberg v. Paulk,</u> 611 F.3d 828 (11th Cir. 2010) | 38 |
| <u>Smith v. Maryland,</u> 442 U.S. 735 (1979) | passim |

| | |
|---|---------------|
| <u>United States v. Benford</u> , No. 2:09 CR 86, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010) | 25, 32 |
| <u>United States v. Jones</u> , 132 S. Ct. 945 (2012) | 22 |
| <u>United States v. Karo</u> , 468 U.S. 705 (1984) | 17 |
| <u>United States v. Knotts</u> , 460 U.S. 276 (1983) | 17 |
| <u>United States v. Maynard</u> , 615 F. 3d 544 (D.C. Cir. 2010) | 21 |
| <u>United States v. Miller</u> , 425 U.S. 435 (1976) | 14, 19 |
| <u>United States v. White</u> , 401 U.S. 745 (1971) | 6, 13, 27, 40 |

STATE CASES

| | |
|--|-----------------|
| <u>Commonwealth v. Blood</u> , 400 Mass. 61 (1987) | 5, 6, 7, 37, 40 |
| <u>Commonwealth v. Buccella</u> , 434 Mass. 473 (2001) | 8, 9 |
| <u>Commonwealth v. Connolly</u> , 454 Mass. 808 (2009) | 9 |
| <u>Commonwealth v. Cote</u> , 407 Mass. 827 (1990) | 7, 8 |
| <u>Commonwealth v. Cundruff</u> , 382 Mass. 137 (1980) | 5 |
| <u>Commonwealth v. Feodoroff</u> , 43 Mass. App. Ct. 725 (1997) | 8, 9 |
| <u>Commonwealth v. Gonsalves</u> , 429 Mass. 658 (1999) | 5 |

| | |
|--|--------|
| <u>Commonwealth v. Lyons,</u> 409 Mass. 16 (1990) | 5 |
| <u>Commonwealth v. Rousseau,</u> 465 Mass. 372 (2013) | 9 |
| <u>Commonwealth v. Stoute,</u> 422 Mass. 782 (1996) | 5 |
| <u>Commonwealth v. Upton,</u> 394 Mass. 363 (1985) | 5, 6 |
| <u>People v. DeLaire,</u> 610 N.E.2d 1277 (Ill. App. Ct. 1993) | 11 |
| <u>People v. Jackson,</u> 452 N.E.2d 85 (Ill. App. Ct. 1983) | 10 |
| <u>People v. Larkin,</u> 239 Cal. Rptr. 760 (Ct. App. 1987) | 11 |
| <u>People v. Oates,</u> 698 P.2d 811 (Colo. 1985) | 10 |
| <u>People v. Weaver,</u> 12 N.Y.3d 433 (2009) | 21, 22 |
| <u>Shaktman v. State,</u> 553 So. 2d 148 (Fla. 1989) | 11 |
| <u>State v. Mollica,</u> 554 A.2d 1315 (N.J. 1989) | 11 |
| <u>State v. Nelson,</u> 941 P.2d 441 (Mont. 1997) | 11 |
| <u>State v. Rothman,</u> 779 P.2d 1 (Haw. 1989) | 11 |
| <u>Winfield v. Div. of Pari-Mutuel Wagering,</u> 477 So. 2d 544 (Fla. 1985) | 10 |

CONSTITUTIONAL PROVISIONS

| | |
|--|--------|
| United States Constitution, Amendment IV..... | passim |
| Massachusetts Declaration of Rights, Article 14..... | |
| | passim |

FEDERAL STATUTES

| | |
|---|----|
| Communications Act of 1934, Chapter 652, § 605, 48 Stat. 1064, 1104 (codified as amended at 47 U.S.C. § 605 (2006)) | 37 |
|---|----|

REGULATIONS

| | |
|--|----|
| Senate Select Comm. On Governmental Operations, Book III: Supplemental Detailed Staff Reports on Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755 (1976) | 38 |
|--|----|

OTHER AUTHORITIES

| | |
|--|--------|
| Federal Bureau of Investigation, Uniform Crime Report, Crime in the United States by State (2011-12), available at http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.- 2012/tables/4tabledatadecoverviewpdf | 11, 12 |
| Adam Gabbatt, <u>NSA Analysts 'Wilfully Violated' Surveillance Systems, Agency Admits</u> , The Guardian (Aug. 24, 2013), available at http://www.theguardian.com/world/2013/aug/24/nsa-analysts-abused-surveillance-systems | 39 |
| Curt Gentry, J. Edgar Hoover: The Man And The Secrets 372 (1991) | 38 |
| Darlene Storm, <u>How Long Does Your Mobile Phone Provider Store Data for Law Enforcement Access?</u> , Computerworld (Sept. 28, 2011), available at http://blogs.computerworld.com/19016/how_long_does_your_mobile_phone_provider_store_data_for_law_enforcement_access | 23, 24 |

| | |
|---|--------|
| Ellen Nakashima, <u>Some Web Firms Say They Track Behavior Without Explicit Consent</u> , Wash. Post, Aug. 12, 2008 | 34 |
| Erick Schonfeld, <u>Gmail Nudges Past AOL Email in the U.S. To Take No. 3 Spot</u> , TECHCRUNCH (Aug. 14, 2009), available at http://www.techcrunch.com/2009/08/14/gmail-nudges-pastaol-email-in-the-us-to-take-no-3-spot | 33 |
| Gerald G. Ashdown, <u>The Fourth Amendment and the "Legitimate Expectation of Privacy,"</u> 34 Vand. L. Rev. 1289 (1981) | 29 |
| Herbert P. Wilkins, <u>The Massachusetts Constitution-The Last Thirty Years</u> , 44 Suffolk U.L.Rev. 331 (2011) | 6 |
| James Beck et al., <u>The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location-Part II</u> , 49 Crim. Law. Bull. 8 (Summer 2013) | 23 |
| James X. Dempsey, <u>Digital Search & Seizure: Updating Privacy Protections To Keep Pace with Technology</u> , in <u>Seventh Annual Institute on Privacy Law: Evolving Laws and Practices in a Security-Driven World</u> (PLI Patents, Copyrights, Trademarks & Literary Prop., Course Handbook Series No. 8966, 2006) | 33 |
| Jen Manso, <u>Cell-Site Location Data and the Right to Privacy</u> , 27 Syracuse Sci. & Tech. L. Rep. 1 (2012) | 25 |
| John Palfrey, <u>The Public and the Private at the United States Border with Cyberspace</u> , 78 Miss. L. J. 241 (2008) | 35 |
| Julia Angwin and Jennifer Valentino-Devries, <u>Apple, Google Collect User Data</u> , Wall Street Journal (Apr. 22, 2011), available at http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html | 26, 36 |

| | |
|--|------------|
| Keir Thomas, <u>Choosing Cloud Backup for PCs</u> , PC World (Mar. 31, 2011), available at http://www.pcworld.com/article/223354/choosing_cloud_backup_for_pcs.html . | 35 |
| Michael Fitzgerald, <u>Cloud Computing: So You Don't Have To Stand Still</u> , N.Y. Times, May 25, 2008 | 35 |
| Noam Cohn, <u>It's Tracking Your Every Move and You May Not Even Know</u> , N.Y. Times (Mar. 26, 2011), available at http://www.nytimes.com/2011/03/26/business/medi a/26privacy.html . | 27 |
| Orin S. Kerr, <u>Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law</u> , 54 Hastings L.J. 805 (2003) | 34 |
| Paul Ohm, <u>The Rise and Fall of Invasive ISP Surveillance</u> , 2009 U. Ill. L. Rev. 1417 | 34 |
| Recent Development, <u>Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators</u> , 18 Harv. J. Law & Tech. 307 (2004) | 24 |
| Stephen E. Henderson, <u>Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search</u> , 55 Cath. U.L.Rev. 373 (2006) | 10, 11 |
| Susan Friewald, <u>Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact</u> , 70 Md. L. Rev. 681 (2011) | 24, 26, 36 |
| Susan W. Brenner & Leo L. Clarke, <u>Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data</u> , 14 J.L. & Pol'y 211 (2006) | 32 |

| | |
|---|----|
| Suzanne Choney, <u>How Long Do Wireless Carriers Keep Your Data?</u> , NBC News (Sept. 29, 2011), available at http://www.nbcnews.com/technology/how-long-do- wireless-carriers-keep-your-data-120367 | 35 |
| Thomas Claburn, <u>What Google Search Reveals About Us</u> , Info. Week, Mar. 13, 2006 | 34 |
| Wayne R. La Fave, 1 Search and Seizure, a Treatise on the Fourth Amendment § 2.7(c) (5th ed. 2012) | 29 |
| Zachary Roth, <u>Penn. AG Subpoenas Twitter: A Move To Silence Critics?</u> , Talking Points Memo (May 20, 2010, 9:09 AM), available at http://tpmmuckraker.talkingpointsmemo.com/2010/ 05/penn_ag_subpoenas_twitter_a_move_to_silence_ critic.php?ref=fpblg | 39 |

The Massachusetts Association of Defense Criminal Lawyers respectfully submits this brief pursuant to the Court's solicitation of amicus briefs issued on September 3, 2013.

STATEMENT OF INTEREST

The Massachusetts Association of Criminal Defense Lawyers (MACDL), as *amicus curiae*, submits this brief in support of defendant-appellee Shabazz Augustine. MACDL is an incorporated association of more than 1,000 experienced trial and appellate lawyers who are members of the Massachusetts Bar and who devote a substantial part of their practices to criminal defense.

MACDL is dedicated to protecting the rights of the citizens of the Commonwealth guaranteed by the Massachusetts Declaration of Rights and the United States Constitution. MACDL seeks to improve the criminal justice system by supporting policies and procedures to ensure fairness and justice in criminal matters. MACDL devotes much of its energy to identifying, and attempting to avoid or correct, problems in the criminal justice system. It files

amicus curiae briefs in cases raising questions of importance to the administration of justice.

SUMMARY OF ARGUMENT

The "third-party doctrine" provides that the Fourth Amendment does not apply to records or other information disclosed to a third party and then obtained by the Government from that party. The U.S. Supreme Court developed this controversial doctrine in a series of cases in the 1960s and 1970s dealing with government informants and telephone call logs. The Commonwealth now asks this Court to extend these decades-old cases to the modern technology of Cell Site Location Information (CSLI), allowing the Commonwealth to warrantlessly monitor everywhere its citizens go while carrying a cell phone. This radical reduction of the privacy of Massachusetts' citizens is wholly unjustified.

This Court should reject the third-party doctrine and hold that Massachusetts citizens have an objectively reasonable expectation of privacy in CSLI under Article 14 of the Declaration of Rights of the Massachusetts Constitution. This Court has previously

declined to follow the third-party doctrine in cases where doing so would threaten personal privacy or subject citizens to an unjustifiable risk of widespread surveillance and government abuse. Other states have rejected the doctrine outright, and there is no evidence that the absence of the doctrine has impeded law enforcement in any of those states, many of which rank among the lowest-crime states in the nation. And the U.S. Supreme Court case on which the Government relies has been called into question by subsequent U.S. Supreme Court cases. Further, it dealt with a far less invasive and revealing type of information, in a vastly different technological context, and--unlike this case--it involved a defendant who actively and directly sent the information at issue to a third party.

Moreover, the third-party doctrine is itself inherently flawed. It rests on the unsound premise that once a person shares her information with any other party, even for a limited and confidential purpose, her information is exposed for all of the public to see. It also relies upon the questionable assumption that a person in the modern world can

reasonably choose to forego services and technologies such as banks and telephones. These premises were wrong in the 1970s and are even more obviously wrong today. Further, the extension of the third-party doctrine to modern information technologies would eliminate citizens' reasonable expectations of privacy in nearly all of their personal electronic information, exposing their associations, their movements, their intimate communications and thoughts, to Government scrutiny. This massive expansion in warrantless government surveillance would chill citizens' exercise of vital First Amendment freedoms and drastically expand the potential for government abuses of surveillance power.

ARGUMENT

- I. THIS COURT SHOULD REJECT THE THIRD-PARTY DOCTRINE AS INAPPLICABLE TO MODERN TECHNOLOGIES AND HOLD THAT MONITORING OF CELL PHONE LOCATION DATA IS A SEARCH UNDER ARTICLE 14
 - A. ARTICLE 14 OF THE MASSACHUSETTS DECLARATION OF RIGHTS IS BROADER IN SCOPE THAN THE FOURTH AMENDMENT, AND ACCORDINGLY, MASSACHUSETTS NEED NOT FOLLOW THE THIRD-PARTY DOCTRINE

This Court need not embrace federal decisions that limit the rights of Massachusetts citizens under

the Commonwealth's Constitution. Indeed, the Court has consistently recognized that Article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment are not mirror provisions. See, e.g., Commonwealth v. Stoute, 422 Mass. 782, 789 (1996); Commonwealth v. Lyons, 409 Mass. 16, 18 (1990). This is in part premised on the fact that the Massachusetts Constitution preceded and is independent of the Constitution of the United States. Commonwealth v. Upton, 394 Mass. 363, 367 (1985). Portions of the United States Constitution are in fact based on provisions of the Massachusetts Constitution, and this has been thought to be particularly true of the relationship between the Fourth Amendment and Article 14. See Harris v. United States, 331 U.S. 145, 158 (1947) (Frankfurter, J., dissenting); Commonwealth v. Cundriff, 382 Mass. 137, 144 n. 11 (1980).

On numerous occasions, this Court has interpreted Article 14 to provide greater protections than the Fourth Amendment in the area of searches and seizures. See, e.g., Commonwealth v. Gonsalves, 429 Mass. 658, 663 (1999) (Article 14 provides greater protections during vehicle stops); Stoute, 422 Mass. at 789

(Article 14 provides greater protections in determining when a person is "seized"); Commonwealth v. Blood, 400 Mass. 61, 67-74 (1987) (Article 14 provides greater protections against surreptitiously recorded conversations in another person's home); Upton, 394 Mass. at 373 (Article 14 provides greater protections in the determination of probable cause).

Over the last several decades, this Court has "resisted urgings to relax the requirements of art. 14 to conform to the Supreme Court's revisions of Fourth Amendment law." Herbert P. Wilkins, The Massachusetts Constitution, The Last Thirty Years, 44 Suffolk U.L.Rev. 331, 337 (2011).

B. THIS COURT HAS PREVIOUSLY DECLINED TO FOLLOW THE THIRD-PARTY DOCTRINE

The Court's commitment to upholding constitutional safeguards under Article 14 is consistent with its decisions that have declined to follow the third-party doctrine. In Commonwealth v. Blood, 400 Mass. 61 (1987), this Court decided that the search and seizure provision of Article 14 did not allow the police to record conversations between a third party who had consented to the surveillance and a suspect who did not know he was being recorded. Id.

at 74. In resolving this issue, the Blood decision rejected the U.S. Supreme Court's ruling in United States v. White, 401 U.S. 745 (1971), and found that the warrantless electronic recording violated the defendant's rights under the Massachusetts Constitution. Blood, 400 Mass. at 68. The Court explained that "because the peculiar virtues of these [electronic] techniques are ones which threaten the privacy of our most cherished possessions . . . these techniques are peculiarly intrusive upon that sense of personal security which art. 14 commands us to protect." Id. at 70. As such, the Court held that the fact that the third party had consented to the surveillance did not obviate the need for a warrant.

In Commonwealth v. Cote, 407 Mass. 827 (1990), this Court indicated that it might diverge from the federal third-party doctrine. There, a district attorney used a grand jury subpoena to obtain the defendant's telephone messages, which had been conveyed to an answering service. Id. at 829. The Court held that the defendant lacked a protected privacy interest in the messages because "both the defendant and any caller were well aware of the

involvement of a third party," id. at 834, as any caller leaving a message with an answering service would necessarily understand that his message could not possibly be deemed private. Importantly, however, the Court was careful to point out that Article 14 may afford more substantive protection to individuals than under the federal constitution. Id. at 834-35. Accordingly, the Court explained that "[o]ur conclusion that the defendant does not enjoy a reasonable expectation of privacy under the Fourth Amendment does not compel a similar conclusion regarding the reasonableness of the defendant's expectation of privacy under art. 14." Id. at 834 (emphasis added). As seen in both Blood and Cote, this Court has found the third-party doctrine applicable only where the defendant is aware that the information he conveys will not be private.

The Commonwealth incorrectly argues in a footnote that Massachusetts does not recognize an "expectation of privacy in information voluntarily turned over to third parties." See Comm. Brief, at 35 n.7. This Court has never so held. Each of the cases cited recognized that "analysis of an expectation of privacy

following entrustment to a third party might be different under art. 14" than under the Fourth Amendment. Commonwealth v. Buccella, 434 Mass. 473, 484 n.9 (2001); Cote, 407 Mass. at 834-35; Commonwealth v. Feodoroff, 43 Mass. App. Ct. 725, 729-730 (1997). The Commonwealth's reliance on these cases is misplaced for other reasons as well. Feodoroff is an Appeals Court decision and therefore not binding on this Court. And in Buccella, the Court's finding that the student had no expectation of privacy in his written schoolwork was premised on the fact that the search was conducted on school grounds, where "school officials are not required to obtain a search warrant." Id. at 486. Fourth Amendment requirements are significantly relaxed in a school setting, where school officials do not even need to meet the standard of probable cause, but instead, must only show that their actions are reasonable. Id. Thus, Buccella is inapplicable to the case at hand.

Consistent with the Court's broad interpretation of rights protected under Article 14, this Court has found that extended electronic surveillance violates an individual's reasonable expectation of privacy. In

Commonwealth v. Connolly, 454 Mass. 808 (2009), this Court held that installing a GPS on a defendant's vehicle in the absence of a warrant constituted a seizure in violation of Article 14. And most recently in Commonwealth v. Rousseau, 465 Mass. 372 (2013), a case in which the police used a GPS device to monitor a truck for 31 days, this Court held that under Article 14, "a person may reasonably expect not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements, without judicial oversight and a showing of probable cause." Id. at 382.

C. SEVERAL STATES HAVE ALREADY REJECTED THE
THIRD-PARTY DOCTRINE, AND HAVE NOT SUFFERED
ANY NOTICEABLE INCREASE IN CRIME

In light of the significant privacy concerns raised through third party disclosure, more states have begun to question the validity of the third-party doctrine. Nearly a dozen states have abandoned it altogether. See Stephen E. Henderson, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search, 55 Cath. U.L.Rev. 373, 395 (2006) (listing California,

Colorado, Florida, Hawaii, Idaho, Illinois, Montana, New Jersey, and Pennsylvania as having rejected the federal third-party doctrine). Of these states, the majority have adopted the reasonable expectation of privacy standard set forth in Katz, but have diverged from the federal doctrine and recognized privacy interests in the areas of electronic tracking, see, e.g., People v. Oates, 698 P.2d 811 (Colo. 1985), bank records, see, e.g., Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544 (Fla. 1985), People v. Jackson, 452 N.E.2d 85 (Ill. App. Ct. 1983), telephone numbers dialed, see, e.g., People v. Larkin, 239 Cal. Rptr. 760 (Ct. App. 1987), Shaktman v. State, 553 So. 2d 148 (Fla. 1989), People v. DeLaire, 610 N.E.2d 1277 (Ill. App. Ct. 1993), State v. Mollica, 554 A.2d 1315 (N.J. 1989), State v. Rothman, 779 P.2d 1 (Haw. 1989), and medical records, see, e.g., State v. Nelson, 941 P.2d 441 (Mont. 1997), among other areas.¹

There is no evidence to suggest that rejection of the third-party doctrine has impeded law enforcement

¹ An additional ten states have given reason to suggest they might reject the doctrine, and still another eleven states have deviated from the Fourth Amendment on substantive issues. Henderson, 55 Cath. U.L.Rev. at 395.

in any of these states. In fact, many of the states that have rejected the doctrine rank among the lowest in terms of crime rate. See The Federal Bureau of Investigation, Uniform Crime Report, Crime in the United States by State (2011-12), available at [http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-](http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/tables/4tabledatadecoverviewpdf)

[2012/tables/4tabledatadecoverviewpdf](http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/tables/4tabledatadecoverviewpdf); Idaho (ranked 9th lowest in the country for violent crime); Hawaii (11th lowest for violent crime); California (10th lowest for forcible rape); Pennsylvania (12th lowest for property crime); Montana (8th lowest for robbery); Colorado (19th lowest for robbery); New Jersey (13th lowest for aggravated assault); New Jersey (4th lowest for forcible rape). Indeed, several of the states placed within the top half of states with the lowest crime. See Id.

D. **SMITH V. MARYLAND OFFERS A VERY POOR ANALOGY TO THE INSTANT CASE**

The Commonwealth's assertion that it should be allowed to warrantlessly track the locations of citizens who carry cell phones hinges on its characterization of the 1979 case Smith v. Maryland, 442 U.S. 735 (1979), as directly analogous to the

instant case. On the basis of that analogy, the Commonwealth argues, this Court should extend the third-party doctrine to cover CSLI location data, thus allowing the Commonwealth to warrantlessly monitor everywhere its citizens have traveled or will travel while carrying a cell phone. See Comm. Br. at 35-41.

But this radical diminution of Massachusetts' citizens' privacy is not supported by Smith. Even a basic understanding of Smith and its context reveals that the differences between the situation addressed in Smith and the collection of CSLI here are so substantial as to outweigh the similarities.

1. The third-party doctrine was developed in cases such as *Smith* that involved vastly different technologies than that addressed in the instant case

The third-party doctrine, which reached its outermost limit in Smith, has its origins in a series of cases upholding the warrantless use of undercover agents to obtain information from criminals gullible enough to disclose the details of their crimes in casual conversation. Each of these early-era cases involved the voluntary communication of information to a human third party.

For instance, Hoffa v. United States, 385 U.S. 293 (1966), involved statements made by Jimmy Hoffa to his co-conspirator in the presence of a witness, who (unbeknownst to Hoffa) was a government informant. The U.S. Supreme Court held that the government informant did not violate Hoffa's Fourth Amendment rights by deceiving Hoffa as to his intentions so that he could overhear incriminating information. Id. at 302. The Court ruled that Hoffa had assumed the risk that the persons to whom he disclosed his crime might someday testify against him. See also United States v. White, 401 U.S. 745 (1971) (government informants do not violate the Fourth Amendment by wearing "a wire"--i.e. a sound recording device--when obtaining information from a talkative criminal, because there is no constitutional difference between testifying to a conversation and recording it as evidence).

The U.S. Supreme Court greatly extended the scope of the third-party doctrine in United States v. Miller, 425 U.S. 435 (1976), which held that a defendant had no reasonable expectation of privacy in his bank records. The records consisted of checks, financial statements, and deposit slips that were

voluntarily conveyed to the banks and "exposed to their employees in the ordinary course of business." Id. at 442. Although Miller extended the third-party doctrine in the sense that it involved paper records and not oral communications, the information in the bank records was not meaningfully different from the information conveyed to a government informant during a face-to-face conversation. Id. at 443.

The Court expanded the third-party doctrine again in 1979's Smith v. Maryland, 442 U.S. 735 (1979). In Smith, the U.S. Supreme Court held that a defendant had no reasonable expectation of privacy in the telephone numbers he dialed, which are conveyed to the telephone company in the ordinary course of business. Id. at 745-46.

The U.S. Supreme Court reached this conclusion by purporting to apply the two-part test established in Katz v. United States, 389 U.S. 347 (1967): the Fourth Amendment applies whenever an individual has (1) an actual, subjective expectation of privacy, and (2) the expectation is one that society recognizes as objectively reasonable. See id. at 361 (Harlan, J., concurring). Defendant Smith, the U.S. Supreme Court

reasoned, had no subjective expectation of privacy in the phone numbers he dialed, because he was very likely aware that the telephone company recorded the numbers of his long-distance phone calls. Smith, 442 U.S. at 742. Those numbers appeared on his monthly bills, and the telephone company offered to check for overbilling and to identify callers making "annoying or obscene calls"--all of which made it obvious that the telephone company could and did record dialed phone numbers. Id. at 742-43.

Nor, the U.S. Supreme Court concluded, did Smith have an objectively reasonable expectation of privacy in the numbers he dialed. Mere numbers dialed did not reveal the contents of Smith's private communications, only to whom the calls were placed. Id. at 741. Thus, Smith's situation was distinguishable from that in Katz, see id., because recording of the numbers dialed did not compromise the "vital role" that telephone conversations "ha[ve] come to play in private communication." Katz, 389 U.S. at 352. In addition, Smith voluntarily conveyed the phone numbers to a third party. Smith, 442 U.S. at 743-44. By doing so, he assumed the risk that the third party

would turn the numbers over to the government. Id. at 744. Further, it was immaterial that telephone call routing was mostly automated by the 1970s, such that no human being was likely to ever see Smith's dialed numbers. The automatic call-routing equipment was "merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." Id. Had Smith placed his calls through an operator, that operator could have testified against him under the Court's previous third-party doctrine cases. The Court was "not inclined to hold that a different constitutional result is required because the telephone company has decided to automate." Id. at 745. For these reasons, the U.S. Supreme Court concluded, the Government's tracking of the telephone numbers that Smith dialed was not a Fourth Amendment search, and therefore did not require a warrant.

2. The U.S. Supreme Court has backed away from the third-party doctrine and has called its viability into question

The U.S. Supreme Court has never applied the third-party doctrine of Smith to modern technology

that reveals location information.² In fact, over the last several decades, the U.S. Supreme Court has backed away from the third-party doctrine, particularly in cases involving revealing and intimate personal information.

For example, in Bond v. United States, 529 U.S. 334, 336 (2000), the defendant sought to suppress evidence obtained when his carry-on luggage was searched by a border agent. The agent squeezed the defendant's soft luggage and felt a "brick-like"

² The U.S. Supreme Court held in 1983 that the police could use a combination of "visual surveillance" and a beeper device (placed inside a drum of chemicals used to make methamphetamine) to monitor a car on public roads. United States v. Knotts, 460 U.S. 276, 284-85 (1983). The majority held that the warrantless use of the device was not a violation of the Fourth Amendment because the police could have obtained the same information by "following [the defendant] at a distance throughout his journey," id. at 285, which would not have required a warrant. The "scientific enhancement" of the beeper did not raise any unique constitutional issues, because it merely aided visual surveillance. Id.

Knotts is nearly as old as Smith, and it involved a technology that relied upon contemporaneous human surveillance and recorded no data. It did not purport to address technologies capable of monitoring and storing all of a person's location data indefinitely. Moreover, even in the context of beeper devices, Knotts was sharply limited by United States v. Karo, 468 U.S. 705 (1984), which held that the police could not warrantlessly monitor a beeper once the drum containing it entered a private residence.

object, which was revealed to be drugs. Id. The government argued that the defendant could not have a reasonable expectation of privacy in luggage in an overhead compartment on a bus because "matters open to public observation are not protected by the Fourth Amendment." Id. at 337. The U.S. Supreme Court rejected this argument, finding that although bus passengers expect that their bags may be handled, they do not expect that "other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner." Id. at 338-39. Therefore, notwithstanding that Bond's carry-on luggage "was not part of his person," id. at 337, and was open to the public, the Court did not apply the third-party doctrine. The Court noted concern that carry-on luggage is generally used to transport "personal items that, for whatever reason, [individuals] prefer to keep close at hand." Id. at 338. Accordingly, the Court determined that the defendant's expectation of privacy in the contents of his bag was reasonable.

In another case involving the dissemination of sensitive information, Ferguson v. City of Charleston, 532 U.S. 67, 70-73 (2001), the U.S. Supreme Court

struck down a hospital policy that tested the urine samples of pregnant patients for drug use. Although the patients voluntarily shared the urine samples and the resulting test data with third party medical professionals, the Court found that they retained a reasonable expectation of privacy in the results of the tests. Id. at 78 ("the reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."). This holding is directly contrary to that of the earlier third-party doctrine cases like Miller, where disclosure of bank information to bank personnel was sufficient to eliminate a reasonable expectation of privacy in that information, even though bank information is virtually never shared with non-bank personnel without the customer's consent. See Miller, 425 U.S. at 442 (finding no Fourth Amendment protection for bank information "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"). The reasoning of Ferguson

thus calls into question the continued viability of the third-party doctrine.³

3. The differences between this case and *Smith* outweigh any similarities

The differences between the situation addressed in *Smith* and the collection of CSLI here are, in any event, numerous and substantial.

First, location tracking is far more invasive than the collection of phone numbers dialed. The collection of data that can reveal everywhere a person goes for as long as he or she owns or has owned a cell phone is incredibly intrusive and reveals personal and even intimate details about that person's life. Data that reveals a person's location will disclose "trips

³ In addition, the U.S. Supreme Court's increasing concern with the dissemination of personal information in the digital age was vividly illustrated in *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010). The case involved electronic text communications of a government employee, which were stored by the text service provider. *Id.* at 2626. The Court stated that "Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." *Id.* at 2629 (emphasis added). It also specifically addressed cell phone use, noting that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy." *Id.* at 2630.

the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." People v. Weaver, 12 N.Y.3d 433, 441-442 (2009). And such information is profoundly revealing when aggregated. "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups -- and not just one such fact about a person, but all such facts." United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (emphasis added). Location data thus yields "a highly detailed profile, not simply of where we go, but by easy inference, of our associations--political, religious, amicable and amorous, to name only a few--and of the pattern of our professional and avocational pursuits." Weaver, 12 N.Y. 3d at 442. Even in the absence of actual monitoring, citizens' rights and freedoms will be

diminished, in large part because "[a]wareness that the Government may be watching [everywhere they go] chills associational and expressive freedoms." United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). In short, location tracking would essentially allow the police to record and monitor a huge portion of one's life and one's daily actions, without any constitutional barrier to abuse or overreach. As revealing as telephone numbers might sometimes be, they do not approach the level of invasiveness of potentially limitless location monitoring.

Second, the Court in Smith concluded that telephone users likely knew that their dialed telephone numbers were routinely recorded by the telephone company because "they see a list of their long-distance (toll) calls on their monthly bills" and because most phone-books instructed their readers that their telephone company could identify callers who make annoying or obscene phone calls. Smith, 442 U.S. at 742. There is nothing remotely analogous in the CSLI context. Cell phone users do not receive (nor are they offered) a monthly tracking report of

everywhere they traveled over the past month. Indeed, cell phone companies do not disclose their CSLI data retention policies to their customers at all—not even buried in the back pages of user agreements or privacy policies. See, e.g., Darlene Storm, How Long Does Your Mobile Phone Provider Store Data for Law Enforcement Access?, Computerworld (Sept. 28, 2011), available at http://blogs.computerworld.com/19016/how_long_does_your_mobile_phone_provider_store_data_for_law_enforcement_access.

Third, cell phones users do not directly convey their location information to cell phone companies. When a user dials a telephone number, she is actively transmitting that information to a telephone company. By contrast, a cell phone user only reveals her location to a cell phone company because the company can track her by tracing her wireless signal in relation to nearby cell towers. See, e.g., James Beck et al., The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location—Part II, 49 Crim. Law. Bull. Art. 8 (Summer 2013).

In addition, unlike in Smith (and nearly every other case applying the third-party doctrine) where the disclosing party engaged in an affirmative act resulting in disclosure (e.g., dialing a phone number, writing a check, or speaking), cell tower information can be disclosed without any action by the disclosing party. Cell phones periodically (about every seven seconds) transmit a "registration" signal containing the phone's unique electronic serial number that is received by every cell tower within range of the phone. Id. Thus a cell phone user reveals her location automatically and constantly, whether or not she actively uses her phone.

The Commonwealth argues that Defendant Augustine has not yet proven that registration data was turned over to the Commonwealth in this particular case.⁴ See

⁴ The Commonwealth also quotes two articles that express uncertainty as to whether cellular companies routinely store registration data. One, a nine-year old news item, states that it is "unclear . . . whether cell service providers maintain records of these registrations." Recent Development, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 Harv. J. Law & Tech. 307, 309 (2004). This may have been true in 2004, but in the years since, the Government has repeatedly sought and obtained registration data from cell service providers. See, e.g., Susan Friewald, Cell Phone Location Data and the Fourth Amendment: A

Comm. Br. at 37-38. This fact dispute is irrelevant to the legal question at hand. Regardless of the specific information used in this case, registration data is routinely collected and used by law enforcement. See, e.g., In re Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 829 (S.D. Tex. Oct. 29, 2010) ("[T]he Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *1 (N.D. Ind. Mar. 26, 2010) (describing the information sought as data "identifying which cell tower communicated with the cell phone while it was turned on"); In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 402 F. Supp. 2d 597, 598, 600

Question of Law, Not Fact, 70 Md. L. Rev. 681, 705 (2011). The other source cited by the Government, Jen Manso, Cell-Site Location Data and the Right to Privacy, 27 Syracuse Sci. & Tech. L. Rep. 1, 4 (2012), quotes a criminal law practice guide that states "If registration data were also collected by the provider and made available, such records would track the user on a minute by minute basis, compiling a continuous log of [a person's] life, awake and asleep." This arguably suggests that registration data is not always collected by cell phone providers, but it sheds very little light on the issue.

n.6 (D. Md. 2005) (Government sought CSLI data identifying "the physical location of the person in possession of the cell phone whenever the phone was on").⁵ Registration data allows law enforcement to constantly track the locations of cell phone users for as long as they use a cell phone. See, e.g., In re Application, 402 F. Supp. 2d at 598. The fact that cell phone users do not directly send their location data to cell phone companies and that cell phones automatically transmit their user's location data further distinguishes CSLI from Smith.

Fourth, the Smith case involved a technology that, for decades, relied upon third party human beings who obtained the information that the Government was seeking. A telephone user would give

⁵ See also, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 748 (S.D. Tex. 2005) (the Government sought cell site data revealing "the user's physical location while the phone is turned on"); see also Friewald, 70 Md. L. Rev. at 705 (discussing other cases involving registration data); Julia Angwin and Jennifer Valentino-Devries, Apple, Google Collect User Data, Wall Street Journal (Apr. 22, 2011), available at <http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html> (location data is automatically and constantly transmitted by cell phones to third party companies like Apple and Google).

contact information to a human operator, who would then connect the call for the subscriber. See Smith, 442 U.S. at 744. These human operators could have simply testified to the information conveyed to them by a user, under the Court's government informant precedents. See, e.g., Hoffa, 385 U.S. at 303; White, 401 U.S. at 751-53. Thus the Court was "not inclined to hold that a different constitutional result is required because the telephone company has decided to automate." Smith, 442 U.S. at 745.

Here, there has never been a human employee involved in the collection or tracking of cell phone users' location data. Although the circuits of a cell phone company's data servers may hold this data, and although aggregated collections of anonymous data may be scanned by marketing software programs,⁶ the data is functionally private and seen by no one. Indeed, a cell phone company whose employees monitored and recorded everywhere its customers went each day, scrutinizing the details of each customer's life as

⁶ See Noam Cohn, It's Tracking Your Every Move and You May Not Even Know, N.Y. Times (Mar. 26, 2011), available at <http://www.nytimes.com/2011/03/26/business/media/26privacy.html>.

they are revealed over time, would likely soon find itself without any customers (and bankrupted by all of the overtime it would have to pay its employees). The U.S. Supreme Court did not sanction in Smith and has never sanctioned what the Commonwealth asks for here: warrantless access for government officials to a whole category of revealing personal information that historically has never been seen by human beings.

For all of these reasons, the 1979 case Smith offers a very poor analogy to the CSLI case that the Court confronts today. The Commonwealth asks the Court to extend this precedent, which involved dialed telephone numbers on land-line telephones, to encompass location data with the potential to reveal virtually all of the details of citizens' personal lives and to chill citizens' associative and expressive freedoms. In doing so, it has understated how enormous this expansion of Smith would be and how little support Smith offers for this radical reduction in citizens' privacy.

E. IF EXTENDED TO MODERN TECHNOLOGY, THE THIRD-PARTY DOCTRINE WOULD ELIMINATE CITIZENS' RIGHTS TO PRIVACY IN NEARLY ALL OF THEIR PERSONAL INFORMATION

The third-party doctrine is based on a profound misunderstanding of the concept of privacy. Its core premise is that once a citizen discloses information to any other party, then the citizen irrevocably loses her reasonable expectation of privacy in that information and the Government can obtain it without a warrant. But "[p]rivacy is not an all or nothing phenomenon," and people do not think of information that they disclose to others for a specific, limited purpose as exposed to the public (or to the Government). Gerald G. Ashdown, The Fourth Amendment and the "Legitimate Expectation of Privacy," 34 Vand. L. Rev. 1289, 1315 (1981).

Rather, in disclosing financial information to a bank, or telephone numbers to a telephone company, a customer has a reasonable expectation that his information will be used for the bank or company's limited purposes and will not be disclosed to any other party without the customer's permission. See, e.g., Wayne R. La Fave, 1 Search and Seizure, a Treatise on the Fourth Amendment § 2.7(c) (5th ed.

2012). Neither the customer nor society at large considers such information to be exposed to the public; and thus the cases extending the third-party doctrine to bank or telephone records were "dead wrong" about privacy. Id.; see also Ferguson, 532 U.S. at 78 (finding that hospital patients had a reasonable expectation of privacy in test results because the results are typically used for hospital purposes only and not disclosed to any other party without the patients' permission).

Smith and Miller are likewise incorrect in their conclusion that bank and telephone users somehow "assume[] the risk," Smith, 442 U.S. at 744, that their banks or telephone companies will provide their personal information to the police. First, unlike the government informants at issue in the early third-party doctrine cases, neither the bank nor the telephone company chose to disclose their customer's information to the police. Rather, in Miller, the Government subpoenaed the bank records, leaving the bank little choice but to turn them over; and in Smith, the Government directed the telephone company to install a device (called a "pen register") to

record Smith's dialed telephone numbers. Thus the Government actively sought the defendants' information, which would have remained unexposed but for the Government's action. Such action is surely a "search," at least under Article 14.

Second, Smith and Miller did not involve a defendant who decided to take a risk by telling a third party about the details of his crimes, therefore exposing himself to the chance of disclosure, as in Hoffa. The defendants in Smith and Miller simply used services that are employed by virtually every modern citizen and that have become integral to modern life. See, e.g., Ashdown, supra, at 1314. They had no meaningful choice to not use the banking system or to not communicate with others via telephone. Indeed, it borders on the absurd to suggest that a person has meaningfully chosen to expose their revealing personal information to the Government just because they use a service that has become part of the fabric of modern society, such as a telephone, cell phone, or bank service. See, e.g., Quon, 130 S.Ct. at 2630 ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential

means or necessary instruments for self-expression, even self-identification."). And it is hardly reasonable to expect citizens to forego certain occupations, avoid travel, bury their money in the back yard, or cut off communication with their loved ones in order to prevent the Government from monitoring their personal information. See, e.g. Ashdown, *supra*, at 1314-15; Wayne R. La Fave, 1 *Search and Seizure, a Treatise on the Fourth Amendment* § 2.7(c) (5th ed. 2012); Susan W. Brenner & Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data, 14 J.L. & Pol'y 211, 244 (2006).

Thus the third-party doctrine has, ever since Miller and Smith, threatened citizens' privacy in their personal information. But the greatest danger posed by the third-party doctrine is that courts may extend it beyond land-line telephones and bank receipts to modern information technologies. See, e.g., In re: Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. July 30, 2013) (Government agents may collect CSLI data that allows them to track a user's location even when the

user's phone is "in an idle state" without any constitutional limitation); Benford, 2010 WL 1266507, at *3 (same). If courts determine that information shared with third party equipment (such as computers and servers) is no longer entitled to constitutional protection, then there will be virtually no limit to the personal information that the Government can obtain without a warrant or probable cause.

The variety and amount of personal electronic data has increased exponentially since the 1970s, when the U.S. Supreme Court's last expansions of the third-party doctrine occurred. Today, a huge portion of the information that people produce as they live their lives is stored in electronic form, and nearly all of that data is shared with and stored by third party equipment at some point. For example, emails sent and received via web-based email services like Gmail, Yahoo, Hotmail, or numerous others (which account for over 200 million email accounts in the United States), or through any service that stores emails on a remote server, are retained by the service provider until the user deletes them and often even after deletion. See, e.g., James X. Dempsey, Digital Search & Seizure:

Updating Privacy Protections To Keep Pace with Technology, in Seventh Annual Institute on Privacy Law: Evolving Laws and Practices in a Security-Driven World, at 505, 523 (PLI Patents, Copyrights, Trademarks & Literary Prop., Course Handbook Series No. 8966, 2006). Emails are also scanned by these services to detect spam and viruses, for advertising purposes, and for indexing and search purposes. See, e.g., Erick Schonfeld, Gmail Nudges Past AOL Email in the U.S. To Take No. 3 Spot, TECHCRUNCH (Aug. 14, 2009), available at <http://techcrunch.com/2009/08/14/gmail-nudges-pastaol-email-in-the-us-to-take-no-3-spot/>.⁷ If the third-party doctrine is expanded to cover modern information technologies, then the Government will be able to obtain and read all of these emails, which are exposed to third party equipment and stored on third party servers, without any constitutional limitation.

Likewise, the address of every website that a person visits is likely to be recorded by the

⁷ See also, e.g., Orin S. Kerr, Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805, 812-16 (2003).

computers of internet service providers or affiliated groups of websites, for advertising, marketing, and network maintenance purposes. See, e.g., Paul Ohm, The Rise and Fall of Invasive ISP Surveillance, 2009 U. Ill. L. Rev. 1417, 1424-25, 1432-38; Ellen Nakashima, Some Web Firms Say They Track Behavior Without Explicit Consent, Wash. Post, Aug. 12, 2008. The search terms that a user types into a search engine (such as Google) are processed and stored by third party computers. See, e.g., Thomas Claburn, What Google Search Reveals About Us, Info. Week, Mar. 13, 2006, at 45.⁸ And even word processing documents may be stored on third party computers, especially if they are created or stored on "cloud computing" software such as Google Docs or if a user's computer automatically backs up its hard drive offsite using any one of several available back-up services. See, e.g., Michael Fitzgerald, Cloud Computing: So You

⁸ See also, e.g., John Palfrey, The Public and the Private at the United States Border with Cyberspace, 78 Miss. L. J. 241, 267 (2008).

Don't Have To Stand Still, N.Y. Times, May 25, 2008,
at Bu4.⁹

Finally, of course, cell phone companies and software providers often record and store information generated by cell tower transmissions and GPS monitoring. See, e.g., Suzanne Choney, How Long Do Wireless Carriers Keep Your Data?, NBC News (Sept. 29, 2011), available at <http://www.nbcnews.com/technology/how-long-do-wireless-carriers-keep-your-data-120367>.¹⁰ If courts expand the third-party doctrine to cover modern information technologies, then all of this information and more will be available to the Government without constitutional limits.

Thus, nearly every bit of information about a person's life, from their bank records and the people whom they call on the telephone, to the addresses and

⁹ See also, e.g., Keir Thomas, Choosing Cloud Backup for PCs, PC World (Mar. 31, 2011), available at http://www.pcworld.com/article/223354/choosing_cloud_backup_for_pcs.html.

¹⁰ See also, e.g., Friewald, 70 Md. L. Rev. 681; Julia Angwin and Jennifer Valentino-Devries, Apple, Google Collect User Data, Wall Street Journal (Apr. 22, 2011), available at <http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html>.

contents of their emails, every website they visit, every web search they perform, the contents of their personal letters and documents created using a word processor, to every place they travel inside and outside of the home, may be subject to warrantless government intrusion if courts expand the third-party doctrine to cover modern information technologies. The possibility of such pervasive monitoring would surely "chill[] associational and expressive freedoms," Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring), and would run counter to the fundamental principles of Article 14. See, e.g., Blood, 400 Mass. at 73.

The Commonwealth does not offer a reason why the third-party doctrine should be expanded to eliminate Massachusetts' citizens reasonable expectations of privacy in their electronic personal data exposed to third party equipment, beyond its argument (addressed above) that Smith is analogous and applicable to these modern technologies. Comm. Br. at 35. Nor does the Commonwealth argue that government agents given the power to warrantlessly collect revealing personal information about any citizen can simply avoid abusing

that power. Indeed, such an argument would be untenable, given the checkered history of government surveillance programs.

For example, prior to 1967's Katz v. United States, 389 U.S. 347 (1967), there were no constitutional limitations on the Government's ability to wiretap telephone calls or use small microphones to secretly record conversations.¹¹ During this period, Government agents recorded a staggering number of personal conversations, including conversations between attorneys and their clients and the conversations of sitting U.S. Supreme Court justices. See, e.g., Curt Gentry, J. Edgar Hoover: The Man And The Secrets 372, 630 (1991). The Government used the information it captured to pervasively monitor left-wing and right-wing political groups, to intimidate or discredit certain Congressmen, and to attempt to discredit Martin Luther King and induce him to commit suicide. See, e.g., id. at 119, 137, 564, 571-76, 588. Intelligence agencies set up programs expressly

¹¹ There was a statute limiting the interception of communications data, but it proved ineffectual. See Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1104 (codified as amended at 47 U.S.C. § 605 (2006)).

designed to "influence political choices and social values" in a misguided attempt to thwart a perceived domestic communist threat. See Senate Select Comm. on Governmental Operations, Book III: Supplemental Detailed Staff Reports on Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755, at 4 (1976).

Although surveillance abuses are rarely disclosed until decades later, there have already been reports of abuses of Internet surveillance technologies by government officials for political ends. See, e.g., Rehberg v. Paulk, 611 F.3d 828, 835 (11th Cir. 2010) (after Rehberg criticized the managers of a local hospital, district attorneys who were political allies of the managers obtained Rehberg's personal emails and turned them over to the managers for use against him); Zachary Roth, Penn. AG Subpoenas Twitter: A Move To Silence Critics?, Talking Points Memo (May 20, 2010, 9:09 AM), available at http://tpmmuckraker.talkingpointsmemo.com/2010/05/penn_ag_subpoenas_twitter_a_move_to_silence_critic.php?ref=fpblg (A state attorney general running for governor

subpoenaed the account information of bloggers and Twitter users who criticized him).

Likewise, in the foreign surveillance sphere (which is not at issue here), a whole host of surveillance abuses and violations is just now coming to light. See, e.g., Adam Gabbatt, NSA Analysts 'Wilfully Violated' Surveillance Systems, Agency Admits, The Guardian (Aug. 24, 2013), available at <http://www.theguardian.com/world/2013/aug/24/nsa-analysts-abused-surveillance-systems> (reporting, among other abuses, that "various agents had used the NSA's controversial data monitoring capabilities to spy on love interests"). Court approval of massive, warrantless domestic surveillance of Massachusetts citizens would likely lead to a significant expansion of surveillance abuses in the State.

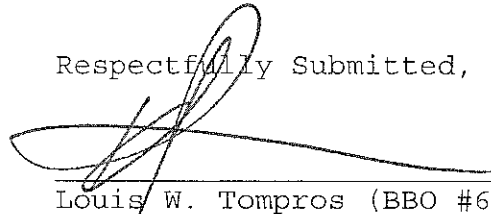
Massachusetts should not repeat the mistakes of Miller and Smith when determining the scope of Article 14. Instead, the Court should follow the path it set out in Blood, 400 Mass. at 73, where it rejected the third-party doctrine reasoning of White, 401 U.S. at 752-53, and held that warrantless recording of conversations by government informants violated

Article 14. Even more than White, Miller and Smith are based on faulty conceptions of privacy and "underestimate[] the risk" of government abuses and widespread warrantless surveillance. Blood, 400 Mass. at 73.

CONCLUSION

For the foregoing reasons, this Court should reject the third-party doctrine as inapplicable to modern technologies and hold that a person has an objectively reasonable expectation of privacy in CSLI under Article 14 of the Massachusetts Constitution.

Respectfully Submitted,



Louis W. Tompros (BBO #657791)
Kevin S. Prussia (BBO #666813)
Thaila K. Sundaresan (BBO #683616)
Matthew J. Tokson (Pro Hac Vice)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

Elizabeth A. Lunt (BBO #307700)
ZALKIND, DUNCAN & BERNSTEIN
65A Atlantic Avenue
Boston, MA 02110
(617) 742-6020
lunt@zalkindlaw.com
President,
Massachusetts Association of Criminal
Defense Lawyers

Alex G. Philipson (BBO #637528)
PHILIPSON LEGAL
97 Montvale Road
Newton Centre, MA 02459
(617) 671-9015
ap@philipsonlegal.com
Co-Chair, Amicus Curiae Committee,
Massachusetts Association of Criminal
Defense Lawyers

September 30, 2013

ADDENDUM

United States Constitution, Amendment IV

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

Massachusetts Declaration of Rights, Article 14

Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

47 U.S.C. § 605. Unauthorized publication or use of communications

(a) Practices prohibited

Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over

which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.

(b) Exceptions

The provisions of subsection (a) of this section shall not apply to the interception or receipt by any individual, or the assisting (including the manufacture or sale) of such interception or receipt, of any satellite cable programming for private viewing if--

(1) the programming involved is not encrypted; and

(2) (A) a marketing system is not established under which--

(i) an agent or agents have been lawfully designated for the purpose of authorizing private viewing by individuals, and

(ii) such authorization is available to the individual involved from the appropriate agent or agents; or

(B) a marketing system described in subparagraph (A) is established and the individuals receiving such programming has obtained authorization for private viewing under that system.

(c) Scrambling of Public Broadcasting Service programming

No person shall encrypt or continue to encrypt satellite delivered programs included in the National Program Service of the Public Broadcasting Service and intended for public viewing by retransmission by television broadcast stations; except that as long as at least one unencrypted satellite transmission of any program subject to this subsection is provided, this subsection shall not prohibit additional encrypted satellite transmissions of the same program.

(d) Definitions

For purposes of this section--

(1) the term "satellite cable programming" means video programming which is transmitted via satellite and which is primarily intended for the direct receipt by cable operators for their retransmission to cable subscribers;

(2) the term "agent", with respect to any person, includes an employee of such person;

(3) the term "encrypt", when used with respect to satellite cable programming, means to transmit such programming in a form whereby the aural and visual characteristics (or both) are modified or altered for the purpose of preventing the unauthorized receipt of such programming by persons without authorized equipment which is designed to eliminate the effects of such modification or alteration;

(4) the term "private viewing" means the viewing for private use in an individual's dwelling unit by means of equipment, owned or operated by such individual, capable of receiving satellite cable programming directly from a satellite;

(5) the term "private financial gain" shall not include the gain resulting to any individual for the private use in such individual's dwelling unit of any programming for which the individual has not obtained authorization for that use; and

(6) the term "any person aggrieved" shall include any person with proprietary rights in the intercepted communication by wire or radio, including wholesale or retail distributors of satellite cable programming, and, in the case of a violation of paragraph (4) of subsection (e) of this section, shall also include any person engaged in the lawful manufacture, distribution, or sale of equipment necessary to authorize or receive satellite cable programming.

(e) Penalties; civil actions; remedies; attorney's fees and costs; computation of damages; regulation by State and local authorities

(1) Any person who willfully violates subsection (a) of this section shall be fined not more than \$2,000 or imprisoned for not more than 6 months, or both.

(2) Any person who violates subsection (a) of this section willfully and for purposes of direct or indirect commercial advantage or private financial gain shall be fined not more than \$50,000 or imprisoned for not more than 2 years, or both, for the first such conviction and shall be fined not more than \$100,000 or imprisoned for not more than 5 years, or both, for any subsequent conviction.

(3) (A) Any person aggrieved by any violation of subsection (a) of this section or paragraph (4) of this subsection may bring a civil action in a United States district court or in any other court of competent jurisdiction.

(B) The court--

(i) may grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain violations of subsection (a) of this section;

(ii) may award damages as described in subparagraph (C); and

(iii) shall direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails.

(C) (i) Damages awarded by any court under this section shall be computed, at the election of the aggrieved party, in accordance with either of the following subclauses;

(I) the party aggrieved may recover the actual damages suffered by him as a result of the violation and any profits of the violator that are attributable to the violation which are not taken into account in computing the actual damages; in determining the violator's profits, the party aggrieved shall be required to prove only the violator's gross revenue, and the violator shall be required to prove his deductible expenses and the elements of profit attributable to factors other than the violation; or

(II) the party aggrieved may recover an award of statutory damages for each violation of subsection (a) of this section involved in the action in a sum of not less than \$1,000 or more than \$10,000, as the court considers just, and for each violation of paragraph (4) of this subsection involved in the action an aggrieved party may recover statutory damages in a sum not less than \$10,000, or more than \$100,000, as the court considers just.

(ii) In any case in which the court finds that the violation was committed willfully and for purposes of direct or indirect commercial advantage or private financial gain, the court in its discretion may increase the award of damages, whether actual or statutory, by an amount of not more than \$100,000 for each violation of subsection (a) of this section.

(iii) In any case where the court finds that the violator was not aware and had no reason to believe that his acts constituted a violation of this section,

the court in its discretion may reduce the award of damages to a sum of not less than \$250.

(4) Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than \$500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

(5) The penalties under this subsection shall be in addition to those prescribed under any other provision of this subchapter.

(6) Nothing in this subsection shall prevent any State, or political subdivision thereof, from enacting or enforcing any laws with respect to the importation, sale, manufacture, or distribution of equipment by any person with the intent of its use to assist in the interception or receipt of radio communications prohibited by subsection (a) of this section.

(f) Rights, obligations, and liabilities under other laws unaffected

Nothing in this section shall affect any right, obligation, or liability under Title 17, any rule, regulation, or order thereunder, or any other applicable Federal, State, or local law.

(g) Universal encryption standard

The Commission shall initiate an inquiry concerning the need for a universal encryption standard that permits decryption of satellite cable programming intended for private viewing. In conducting such inquiry, the Commission shall take into account--

(1) consumer costs and benefits of any such standard, including consumer investment in equipment in operation;

(2) incorporation of technological enhancements, including advanced television formats;

(3) whether any such standard would effectively prevent present and future unauthorized decryption of satellite cable programming;

(4) the costs and benefits of any such standard on other authorized users of encrypted satellite cable programming, including cable systems and satellite master antenna television systems;

(5) the effect of any such standard on competition in the manufacture of decryption equipment; and

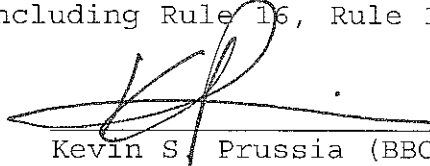
(6) the impact of the time delay associated with the Commission procedures necessary for establishment of such standards.

(h) Rulemaking for encryption standard

If the Commission finds, based on the information gathered from the inquiry required by subsection (g) of this section, that a universal encryption standard is necessary and in the public interest, the Commission shall initiate a rulemaking to establish such a standard.

CERTIFICATE OF COMPLIANCE

I hereby certify that, to the best of my knowledge, this brief complies with the Massachusetts Rules of Appellate Procedure that pertain to the filing of briefs, including Rule 16, Rule 18, and Rule 20.

A handwritten signature in black ink, appearing to read 'K. Prussia', is written over a horizontal line.

Kevin S. Prussia (BBO #666813)

WILMER CUTLER PICKERING

HALE AND DORR LLP

60 State Street

Boston, MA 02109

(617) 526-6000

Dated: September 30, 2013

CERTIFICATE OF SERVICE

I, Kevin Prussia, hereby certify that on September 30, 2013, I caused two true and correct copies of the above document to be served on counsel of record for each other party by mailing the document by first-class mail, postage pre-paid, to the following individuals:

Cailin M. Campbell
Office of the District Attorney/Suffolk
One Bulfinch Place
Third Floor
Boston, MA 02114
(617) 619-4082

Matthew R. Segal
Jessie J. Rossman
American Civil Liberties Union Foundation of
Massachusetts
211 Congress Street
Boston, MA 02110
(617) 482-3170