ARTICLE

LAST CALL FOR THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE AFTER CARPENTER?

HARVEY GEE†

† The author is an attorney in San Francisco. He previously served as an attorney with the Office of the Federal Public Defender in Las Vegas and Pittsburgh, the Federal Defenders of the Middle District of Georgia, and the Office of the Colorado State Public Defender. LL.M., The George Washington University Law School; J.D., St. Mary's School of Law; B.A., Sonoma State University. The author thanks the Journal of Science & Technology Law editors for their invaluable advice and editorial assistance.

INTRODUCTION

"Modern surveillance technology has the potential to radically increase the ability of law enforcement to detect crime and collect evidence, often with little or no effects on our privacy."[1] "[Facial-recognition] surveillance would permit the government to pervasively track people's movements and associations in ways that threaten core constitutional values."[2]

During this time of Big Data policing and aggressive policing, we need to ask ourselves some important questions about the government's use of surveillance technology. Do we want to live in a world where the government continuously tracks the location of our cell phone or smartphone, and knows about every online click and scroll we make, and when we make it? Do we mind that the Federal Bureau of Investigation and Immigration and Customs Enforcement routinely probes state driver's license databases with facial recognition technology in their investigations?[3] Do we want to allow police departments to secretly use less than perfect and unprecedented facial recognition software in real-time video surveillance footage streaming from stores, buildings, streets, and police body cameras? [4] Whatever happened to the Fourth Amendment's prohibition against unreasonable searches and seizures, and the warrant requirement?[5]

The third-party doctrine allows the government to do all of these things without a warrant based on probable cause. The third-party doctrine "may be the most critiqued aspect of Fourth Amendment jurisprudence,"[6] since being established forty-something years ago by the leading cases: *United States v.*

---

[1] RIC SIMMONS, SMART SURVEILLANCE: HOW TO INTERPRET THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 189 (2019).

[2] Drew Harwell, *ACLU Sues FBI, DOJ over Facial-Recognition Technology, Criticizing 'Unprecedented' Surveillance and Secrecy*, WASH. POST (Oct. 31, 2019, 11:04 AM), https://www.washingtonpost.com/technology/2019/10/31/aclu-sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/ [https://perma.cc/5T8N-7HRN].

[3] *See* Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 3:54 PM), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/NK8N-N47C].

[4] *See* Aaron Mondry, *Criticism Mounts over Detroit Police Department's Facial Recognition Software*, DETROIT CURBED (July 8, 2019, 7:52 PM), https://detroit.curbed.com/2019/7/8/20687045/project-green-light-detroit-facial-recognition-technology [https://perma.cc/DUK6-5SW6] (reporting that Detroit Police Department's use of facial recognition software in real-time video surveillance footage has raised growing civil rights concerns). *But see* Andy Kessler, *Have No Fear of Facial Recognition*, WALL ST. J. (Aug. 4, 2019, 5:51 PM), https://www.wsj.com/articles/have-no-fear-of-facial-recognition-11564955494 ("If it is bound by legal protections, the technology is a boon, not a tool for tyranny.").

[5] U.S. CONST. amend. IV.

[6] SIMMONS, *supra* note 1, at 146.

Miller[7] and *Smith v. Maryland*.[8] When information is "voluntarily" conveyed to a third-party, an individual has no reasonable expectation of privacy in that information, making the Fourth Amendment inapplicable.[9] Consequently, the government can liberally glean the most intimate details about users of technology from communicative content such as text messages, private social media messages, documents and photos stored in the cloud, search engine queries, web browsing history, Google Maps, smart devices in the home, fitness/health trackers, and from government/private third-party platforms.[10]

Professor Ric Simmons characterizes the third-party doctrine as "anachronistic" in this age of surveillance, stating that "[i]t is unreasonable to argue that by using e-mail, searching the Internet, or driving a car, a person assumes the risk that the government will obtain her e-mails, Internet search terms, or the location of her car."[11] In his testimony before Congress about facial recognition technology, Professor Andrew Ferguson explained that we are living in the era of Big Data policing, whereby technology and programs aggregate and analyze information in the short-term and long-term.[12] Ferguson sees the dangers of Big Data policing on privacy because of the possibility of surveillance overreach violating the Fourth Amendment.[13]

Two years ago, in *Carpenter v. United States*,[14] the Supreme Court reframed the third-party doctrine by limiting and departing from a long tradition of

[7] United States v. Miller, 425 U.S. 435, 443 (1976) (holding that respondent had no reasonable expectation of privacy in information voluntarily conveyed to bank).

[8] Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (holding that petitioner had no reasonable expectation of privacy in information voluntarily conveyed to telephone company).

[9] *See* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 84 (2017).

[10] *See* Michael Price & Bill Wolf, *Building on* Carpenter*: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider*, THE CHAMPION, Dec. 2018, at 23-24 (explaining that IP addresses can show individual's "digital travels, personal curiosities, and online associations"); *see generally* GRAY, *supra* note 9, at 88-89 (explaining government requests for access to cellphone location data, user information from search engines, and data from social media websites). Email metadata identifying the sender/recipient, the originating computer, and any attachments is considered noncontent and can be obtained by the government without a warrant. Individuals have a reasonable expectation of privacy in the contents of emails held by service providers. *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (holding individuals have a reasonable expectation of privacy in the contents of emails held by service provider, and therefore a warrant is presumptively required to obtain them).

[11] SIMMONS, *supra* note 1, at 144.

[12] *Facial Recognition Technology: (Part I) Its Impact on our Civil Rights and Liberties: Hearings Before the H. Comm. on Oversight and Reform*, 116th Cong. 27 (2019) (testimony of Prof. Andrew Guthrie Ferguson).

[13] *Id.* at 15-16.

[14] Carpenter v. United States, 138 S. Ct. 2206 (2018).

deference paid to the doctrine.[15] The Court held, for the first time, that cell phone users possess a reasonable expectation of privacy in the cell-site location information (CSLI) history associated with their cell phones.[16] The majority concluded CSLI was not voluntarily exposed, and due to its revealing nature, was not subject to the third-party doctrine.[17] Accessing a person's historical cell-site records - or at least seven days or more of cell site records - is a Fourth Amendment search because it violates the person's "legitimate expectation of privacy in the record of his physical movements."[18] The majority further held that law enforcement agencies generally need a warrant to track suspects' locations using CSLI.[19]

Chief Justice Roberts, writing for the majority, questioned the viability of the third-party doctrine *in dicta* by observing that there is a world of difference between the limited types of personal information found in 1970s era bank records and landline phone records at issue in *Smith*/*Miller*, and the exhaustive chronicle of communicative content, including CSLI, casually collected by wireless carriers today.[20] As to the Court's express statement that the ruling does not affect *Smith/Miller*, Berkeley Law Dean Erwin Chemerinsky observed:

> The Court was careful to say that it was not overruling or changing the doctrine but did not offer a clear explanation as to why it did not apply, other than to make a distinction based on the amount of information that can be learned about a person from stored cellular location information.[21]

This Article argues for the abolishment of the third-party doctrine, an old idea that has recently gained renewed interest in the wake of *United States v. Jones*,[22] *Riley v. California*,[23] and *Carpenter*. Professor Daniel Solove asserts: "*Carpenter* would have been the ideal case to get rid of the third-party Doctrine. Instead the Supreme Court did what it has often done in recent years — tiptoe weakly like a mouse, nibbling around the edges of issues rather than directly resolving them."[24]

---

[15] Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205, 224 (2018) (stating that Carpenter significantly circumvented and narrowed the Third-Party Doctrine).

[16] *Carpenter*, 138 S. Ct. at 2219.

[17] *Id.*

[18] *Id.* at 2217. Chief Justice Roberts was joined by Justices Breyer, Ginsburg, Kagan, and Sotomayor.

[19] *Id.*

[20] *Id.* at 2211, 2219.

[21] Erwin Chemerinsky, *Protecting Electronic Privacy*, 103 JUDICATURE 76, 79 (2019).

[22] United States v. Jones, 565 U.S. 400 (2012).

[23] Riley v. California, 573 U.S. 373 (2014).

[24] Daniel Solove, Carpenter v. United States*, Cell Phone Location Records, and the Third-Party Doctrine*, TEACHPRIVACY (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell phone-location-records-and-the-third-party-doctrine/ [https://perma.cc/X97T-SARK].

This Article is divided into three sections. Part One explains why and how *Miller* and *Smith* were wrongly decided, and then proceeds to explore why the third-party doctrine placed surveillance technology beyond the reach of Fourth Amendment regulation. Part Two analyzes the reasoning of the *Carpenter* majority opinion, and Justice Kennedy's embrace of the third-party doctrine in dissent. Part Three forecasts *Carpenter*'s potential influence in moving Fourth Amendment jurisprudence towards the direction of affording more privacy protections against government surveillance. In particular, this Part discusses how state and federal courts, guided by *Carpenter*'s reasoning about historical cell phone data should conclude that information gathered from "prospective" or "real-time" cellphone data, for any length of time, also requires a warrant supported by probable cause.

Part Three then expands to an analysis of the threats to our civil liberties posed by the government's use of facial recognition surveillance technology. Concerns over this critical issue are growing. The issue of facial recognition was even interjected into the 2020 presidential campaign when Senator Bernie Sanders became the first candidate to call for a nationwide ban on surveillance software for policing.[25] Part Three argues that future courts should follow the judicial trend set by the federal judiciary of updating Fourth Amendment principles for emerging technologies. It also advocates for more government transparency and legislation regulating emerging technology to preserve an ever-eroding Fourth Amendment.

I. FROM *MILLER* AND *SMITH* TO *CARPENTER:* THE ORIGINS AND DEVELOPMENT OF THE THIRD-PARTY DOCTRINE

"[T]he Third-Party Doctrine turns the Fourth Amendment into a historical relic."[26]

To understand the significance of *Carpenter* and its lessons moving forward, we must first go back in time to discuss a 1976 case about a pen registry that gave birth to the third-party doctrine. Respondent in *Miller* was convicted of possessing a raw whiskey distillery.[27] The U.S. Attorney used a subpoena to get copies of checks and other records *required* to be kept by the bank under federal banking laws.[28] The Court ruled that there was no legitimate expectation of

[25] Shirin Ghaffary, *Bernie Sanders Wants to Ban Police Use of Facial Recognition Tech*, VOX.COM (Aug. 19, 2019, 3:30 PM), https://www.vox.com/recode/2019/8/19/20812594/bernie-sanders-ban-facial-recognition-tech-police [https://perma.cc/JXS8-E4GZ].

[26] Daniel Solove, *10 Reasons Why the Fourth Amendment Third-Party Doctrine Should be Overruled in* Carpenter v. US, TEACH PRIVACY (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled/ [https://perma.cc/U38V-V69Q].

[27] United States v. Miller, 425 U.S. 435, 436 (1976).

[28] *Id.*

privacy concerning the information kept in bank records because the transactions were "voluntarily" conveyed to a bank in the ordinary course of business.[29]

In dissent, Justice Brennan challenged the Court's reasoning in finding that the bank records were "voluntarily" provided to the bank, even though it was practically a necessity to use banks for any type of financial commerce.[30] To the contrary, Brennan surmised that bank customers reasonably expect privacy when routinely cashing checks:

> [T]he disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since *it is impossible to participate in the economic life of contemporary society without maintaining a bank account*. In the course of such dealings, a depositor reveals many aspects of his personal affairs opinions, habits and associations. . . . To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, *opens the door to a vast and unlimited range of very real abuses of police power*.[31]

Three years later, the Court stretched its definition of "voluntariness" further in *Smith* by condoning the Baltimore Police Department's warrantless request to the telephone company to physically attach a pen register device to identify and link phone numbers.[32] The police were monitoring the home phone of a robbery suspect who made threatening and obscene phone calls to his victim.[33] At some point, the police learned of the suspect's identity by running his license plate number when he drove by the victim's home.[34]

The *Smith* Court saw no infringement of privacy interests because the "limited capabilities" of pen registers did not reveal the purpose of the call, identities of callers, or call completion.[35] The Court also reasoned petitioner "assumed the risk" in making the calls because telephone users do not expect the dialed numbers to remain secret, when the telephone company records all phone numbers.[36]

The majority's narrow view of privacy was taken to task by the collective thrust of the dissents which expressed a broader view of privacy: individuals do have a legitimate expectation of privacy in the phone numbers dialed from their homes, and that the installation of a pen register was a "search."[37] First, Justice

---

[29] *Id.* at 441-43.

[30] *Id.* at 451 (Brennan, J., dissenting).

[31] *Id.* (emphasis added).

[32] *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).

[33] *Id.* at 737.

[34] *Id.*

[35] *Id.* at 736 n.1, 742-43.

[36] *Id.* at 735-36.

[37] *Id.* at 746-47 (Stewart, J., dissenting).

Stewart strongly disagreed with the majority's finding that phone numbers do not implicate the contents of the call.[38] To him, the surveillance of telephone information is revealing, and such information "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[39]

Second, Justice Marshall took issue with the majority's "assumption of the risk" characterization: "Unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[40]

Taken together, the Court's skewed interpretation of "voluntariness" and "assumption of the risk" set the groundwork for the government's longstanding reliance on the third-party doctrine to get information it would not ordinarily be able to obtain absent a warrant based on probable cause.

In the intervening decades, the government's use of the third-party doctrine to subpoena records from wireless carriers dramatically accelerated as the sales of cell phones and smartphones increased exponentially in the digital age. The two kinds of CSLI central to the litigation were historical CSLI (indirect surveillance) referring to "[r]ecords stored by the wireless service providers that detail the location of a cell phone in the past" and prospective or real-time CSLI (direct surveillance), which are "all cell site information that is generated after the government has received court permission to acquire it."[41]

Under the government's theory, the third-party doctrine allows agents to reach CSLI records or global positioning system (GPS) data because (1) phone service providers, not the phone users, own and maintain the records; (2) individuals do not expect privacy when they knowingly and voluntarily disclose their location information to the service provider; (3) people choose to have cell phones; and (4) CSLI shows only limited routing information, just like pen registers that reveal dialed phone numbers.[42]

The Stored Communications Act (SCA),[43] along with the third-party doctrine, allowed the government to win many courtroom battles over the use of CSLI in criminal prosecutions. The government only has to clear a low threshold to get CLSI records with a court-issued subpoena.[44] The subpoena just has to provide "specific and articulable facts" showing the information contains potentially

[38] *Id.* at 746.

[39] *Id.* at 748.

[40] *Id.* at 750 (Marshall, J., dissenting).

[41] *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

[42] *See* Smith v. Maryland, 442 U.S. 735, 742-45 (1979); *see also* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 240-42 (2017).

[43] Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012).

[44] *Id.* § 2703(d).

"relevant and articulable facts," that is potentially "relevant and material" to a criminal investigation."[45] Professor Friedman asserts the government's easy ability to get third-party information with a subpoena is a license to pry because it does not require a probable cause showing or judicial approval.[46]

Because Congress mostly stayed on the sidelines, the legal protections created were slight. Title of II the 1986 Electronic Communications Privacy Act (ECPA), which was passed to protect the content of communications requiring a warrant based on probable cause, did not go far enough. Specifically, the ECPA does not require probable cause for non-content records such as metadata and historical CSLI from service providers.[47] Title III, the Pen/Trap Statute allows pen registers and trap/trace devices to capture the phone number called and received from target phones.[48]

Given this reality, nationwide divergent views exist regarding the third-party doctrine leading up to *Carpenter*. As the litigation over the government's tactical use of CSLI in their prosecutions ensued, multiple splits resulted on the issue of whether a warrant is required by law enforcement agencies to collect cell phone information.

Several state courts recognize a privacy interest in long-term tracking.[49] However, the Fourth, Fifth, Sixth, and Eleventh Circuits held that no privacy interest exists, and that people voluntarily disclose their location data.[50] A minority of courts focused on privacy and concluded that the third-party doctrine should not apply to historical CSLI because it reveals information about people, the things inside their homes, and other private spaces where an expectation of privacy is at its pinnacle. Massachusetts, New Jersey, Florida and the Northern

[45] *Id.* (suggesting relevancy is a low threshold and gives government a "blank check" for things that it seeks regardless if the target is under suspicion or not).

[46] FRIEDMAN, *supra* note 42, at 241.

[47] 18 U.S.C. § 2703 (2012). Title I is known as the Wiretap Act prohibiting intentional inception, use, disclosure of wire, oral, or electronic communication. *Id.* § 2515.

[48] 18 U.S.C. § 3121-3127 (2012).

[49] *E.g.*, Commonwealth v. Rousseau, 990 N.E.2d 543, 553 (Mass. 2013); People v. Weaver, 990 N.E.2d 1195, 1202 (N.Y. 2009).

[50] United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc) (holding that the government's acquisition of historical CSLI from the defendant's cell phone provider without a warrant did not violate the Fourth Amendment); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (addressing the constitutionality of whether court orders authorized by the Stored Communications Act to compel cell phone service providers to produce historical cell site information of their subscribers, and ruling that orders to obtain historical cell site information for specified cell phones at the points at which the user places and terminated a call are not categorically unconstitutional); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2010), *rev'd*, 138 S. Ct. 2206, 2232 (2018); United States v. Davis, 785 F.3d 498, 510 (11th Cir. 2011) (en banc).

District of California recognized a privacy interest in CSLI, and these courts require the government to get a warrant.[51]

In the interim, the legal academy weighed in. A sampling of the extant literature finds Professor Orin Kerr defending the third-party doctrine: "Without a third-party doctrine, suspects can act opportunistically to effectively hide their criminal enterprises from observation."[52] Kerr insists that the third-party doctrine is a valuable investigative tool, and that a warrant requirement would impede legitimate good faith investigations.[53] Professor Ric Simmons likewise believes the doctrine allows police to get information from informants and others who want to help the police.[54]

Conversely, Professor David Gray asserts the government overreaches when it claims that the third-party doctrine eliminates all reasonable expectation of privacy in information shared with third-parties, thereby threatening the right of

[51] *E.g.*, State v. Earls, 70 A.3d 630, 642, 644 (N.J. 2013) (holding that cell phone users have a reasonable expectation of privacy in their cell phone location information, and that police must obtain a search warrant before accessing that information); Tracey v. State, 152 So.3d 504, 525 (Fla. 2014) (addressing the issue of whether the warrantless use of electronically-generated CSLI to track an individual's movements, in real time both on public roads and into a residence violates a subjective expectation of a privacy in that person's location, and holding that a subjective expectation of privacy of location as signaled by one's cell phone—even on public roads—is a reasonable expectation of privacy that society is now prepared to recognize); *see also In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015) (holding that cell phone users "have an expectation of privacy in the historical CSLI associated with their cell phones, and that such an expectation is one that society is prepared to recognize as [objectively] reasonable"); People v. Gordon, 68 N.Y.S.3d 306, 308, 311 (N.Y. Sup. Ct. 2017) (holding that the government's reliance on New York's pen register statute is inapplicable to cell site simulators and observing, "[b]y its very nature . . . the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping, and requires a separate warrant supported by probable cause rather than [solely a pen register warrant]").

[52] *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 573 (2009).

[53] *Id.* at 601.

[54] *See* SIMMONS, *supra* note 1, at 147. In his recent volume, Simmons proposes a new cost-benefit approach to the Fourth Amendment that accommodates new surveillance technologies and strong privacy protections. He argues that modern surveillance techniques need methods of evaluation and regulation based on a new paradigm that measures the efficiency of the new technology in comparison with the efficiency of existing surveillance techniques. *Id.* at 2. According to Simmons, a fresh perspective of surveillance is necessary because the current Supreme Court analysis is limited to making a determination of whether the surveillance is a "search" under the classic Fourth Amendment doctrine, or arbitrary line drawing about what constitutes a search. *Id.* at 10. Simmons offers his alternative—a cost-benefit theory allowing a precise calculation of the levels of intrusiveness, and a measurement of how much surveillance infringes on personal privacy. *Id.*

the people to be secure against unreasonable searches.[55] Professor Daniel Solove offers solid reasons for why the third-party doctrine should be overruled, including the fact that almost all of our data is in the hands of third-parties; almost everything in a modern home involves a third-party record; the Court erroneously links the third-party doctrine with the assumption of risk doctrine through faulty reasoning; many third parties breach their contractual promises to maintain private information, including health records, to share data with third parties; the third-party doctrine enables the "digital equivalent of general warrant"; and the third-party doctrine threatens First Amendment rights by monitoring our online activities.[56]

With no clear consensus about the applicability of the third-party doctrine, Supreme Court observers eagerly awaited the outcome of *Carpenter* in the October 2017 term, hoping that it would provide much-needed guidance on this divisive issue.[57] *Carpenter* was the third technology case to reach the Court in a decade, and privacy rights advocates had reason to be optimistic.[58] The first two cases, *United States v. Jones*[59] and *Riley v. California*,[60] were among the few substantive Fourth Amendment cases where the government lost, and moreover, these rulings signaled the Court's marked retreat from the third-party doctrine.

In *Jones*,[61] a unanimous Court expressed discomfort with the government's attachment of a GPS tracker on a car over 28 days, which was determined to be

---

[55] *See* GRAY, *supra* note 9, at 87, 249. As to National Security Agency metadata surveillance programs, Professor Christopher Slobogin proposes a regime for accessing third-party records that offers meaningful limitations on law enforcement. *See* Christopher Slobogin, *Cause to Believe What? The Importance of Defining a Search's Object–Or, How the ABA Would Analyze the NSA Metadata Surveillance Program*, 66 OKLA. L. REV. 725, 744 (2014). In particular, he wants to replace the low relevance standard with a probable cause or reasonable suspicion requirement for the government in seeking third-party records. *Id.* Elsewhere Professor Erin Murphy wants a reconstituted third-party doctrine that works on a sliding scale offering more protection for only select disclosures made in confidence. *See* Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1252-53 (2009). Murphy considers a "sliding scale of protections" offering absolute privacy for medical records and lesser protection for banking records and emails, and social networking, stating: "we might even impose a heightened standard for what constitutes 'voluntary' disclosure of information held by third parties. We might . . . require covered third parties (imagine for instance banks and medical professionals) to be informed of the Fourth Amendment right of the defendant to keep this information from government hands absent a warrant and probable cause, before being asked whether they are willing to waive it." *Id.* at 1253.

[56] Solove, *supra* note 26.

[57] Freiwald & Smith, *supra* note 15, at 206.

[58] *Id.* at 216.

[59] United States v. Jones, 565 U.S. 400, 413 (2012).

[60] Riley v. California, 573 U.S. 373, 403 (2014).

[61] *Jones*, 565 U.S. at 404.

a "search." [62] Justice Scalia wrote the majority opinion concluding that the government's installation of a GPS device purposed onto defendant's jeep was a physical trespass, and thus a search under the Fourth Amendment.[63] Justices Ginsburg, Breyer, Alito, and Kagan, in a separate concurrence, expressed overarching concerns about the impact of contemporary surveillance technologies on Fourth Amendment rights.[64] Notably, Justice Alito voiced concern over long-term surveillance and articulated, "[t]he best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of [deprivation of privacy] that a reasonable person would not have anticipated."[65]

Justice Sotomayor wrote a separate concurrence explaining why the Court's Fourth Amendment search and seizure doctrine has become "ill suited to the digital age."[66] Among her key points, she cautioned about the government's ability of monitoring through GPS-enabled smartphones.[67] She expressed 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," and recognized the consequential chilling effect.[68]

Then, in *Riley*, the Court addressed whether an officer's search of a defendant's smart phone incident to an arrest violated the Fourth Amendment and ruled unanimously that police generally must obtain a warrant to search the contents of cell phones.[69] Chief Justice Roberts, writing for the majority, recognized that today's cell phones, which are used pervasively, are essentially powerful minicomputers that function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers" and detailed the privacy interests implicated in data stored in modern cell phones showing internet searches, browsing history, and other

[62] *See id*. at 404–05. Eleven years earlier, in *Kyllo v. United States*, the Court held that the use of a thermal imaging device (not in general public use) aimed at a private home from a public street to detect relative amounts of heat and obtain information about the interior of a home constitutes a "search" under the Fourth Amendment. 533 U.S. 27, 34-35 (2001).

[63] *Jones,* 565 U.S. at 404-05.

[64] *Id.* at 430 (Alito, J., concurring).

[65] *Id.* at 430 (alteration in original).

[66] *Id.* at 417 (Sotomayor, J., concurring).

[67] *Id.* at 415.

[68] *Id.* Sotomayor stated that "the Government's physical intrusion on Jones's Jeep, erodes . . . longstanding protection for privacy expectation inherent in items of property that people possess or control." *Id*. at 414. As for the public's reasonable societal expectation of privacy, Sotomayor doubted that people would be willing to exchange their expectations of privacy for more convenience or find the warrantless disclosures of their tracked public movements to be acceptable. *Id.* at 417–18.

[69] Riley v. California, 573 U.S. 373, 400-01 (2014).

personal information.[70] The Court reasoned that the third-party doctrine did not apply because (1) the defendant did not voluntarily consent to and was unaware of the cell phone company's collection of his or her location information; and (2) cell phone data is "qualitatively different" from ordinary physical records as it reveals much more personal information than older technologies.[71]

II. DEPARTING FROM *SMITH* AND *MILLER*: *CARPENTER* DIGITIZES THE *KATZ* REASONABLE EXPECTATION OF PRIVACY TEST

In *Carpenter v. United States*, Timothy Carpenter was apprehended after another suspect in the case gave police the names and some of the cell phone numbers of fifteen accomplices involved in a series of robberies of nine Radio Shack and T-Mobile stores in Michigan and Ohio in 2010.[72] Relying on the SCA, which requires a showing that the data was "relevant and material" to the ongoing investigations, prosecutors went to a federal magistrate to obtain a subpoena to secure records of Carpenter's CSLI from cell phone providers MetroPCS and Sprint, thereby connecting his whereabouts over a four-month period with the dates, times, and locations of the robberies.[73] The government used 186 pages of Carpenter's CSLI collected over 127 days as evidence placing Carpenter within a half-mile to two miles of four of the scenes of the robberies.[74]

At the outset, the Court interpreted the government's request for CSLI relying on the third-party doctrine as a significant stretch of *Smith/Miller* because such records were never contemplated when the Court created the third-party doctrine.[75] Without offering a clear definition of the scope of the third-party doctrine as applied to emerging technologies, the majority declined to extend it.[76]

---

[70] *Id*. at 393-95.

[71] *Id*. at 395-96.

[72] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[73] *Id*.

[74] *Id*. at 2212-13.

[75] *See id.* at 2216-17; Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018), http://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/7FSJ-ASKQ]; Editorial Board, *Congress Must Reckon with the Fourth Amendment and New Technology*, WASH. POST (June 23, 2018, 2:20 PM), https://www.washingtonpost.com/opinions/congress-must-reckon-with-the-fourth-amendment-and-new-technology/2018/06/23/f95578c0-7653-11e8-9780-b1dd6a09b549_story.html [https://perma.cc/7Y77-MGM7] ("The *Carpenter* decision reflects a broader shift in the way the court interprets the Fourth Amendment, an interpretation that is gradually evolving to accommodate new technological realities.").

[76] *See* Price & Wolf, *supra* note 10, at 21(asserting that "*Carpenter* cracked the armor of the 'third-party doctrine,' signaling that the Fourth Amendment may protect other types of personal information held by third-party service providers like Google, Apple, or Facebook.").

Believing that privacy rights are diminished but not entirely eliminated under the doctrine, the majority emphatically rejected the government's arguments that people lose their privacy rights when using these technologies.[77] Historical CSLI is an "exhaustive chronicle of location information casually collected by wireless carriers today," and the mere powering on of a cell phone should not be construed as an affirmative act of voluntarily surrendering information.[78]

Finding CSLI to be too revealing and precise, Chief Justice Roberts echoed the concerns raised in Justice Sotomayor's dissent in *Jones*, writing "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[79] Acknowledging the "seismic shifts in digital technology" and the ubiquity of cellphones, Chief Justice Roberts raised concerns about the current and future potential for abuse if the government is able to collect a week or more of a person's data without having to show probable cause.[80]

Carpenter's reliance on the main strands of reasoning from *Jones* and *Riley* was especially apparent when Chief Justice Roberts referred to the voluminous amount of information secured by the government and compared the capabilities of the GPS monitoring in *Jones* to the ability to chronicle a person's past movements through the record of cell phone signals and the mapping of a cellphone's location over 127 days.[81] Chief Justice Roberts noted, "[a]s with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them 'his familial, political, professional, religious and sexual associations.'"[82]

Next, Chief Justice Roberts builds on the foundation he laid in *Riley* by intimating there may be limitations to the third-party doctrine in the digital era when extraordinarily comprehensive records detailing a person's life records are collected automatically.[83] But to a dissenting Justice Kennedy, the third-party doctrine is as viable as ever.

---

[77] Kerr, *supra* note 75.

[78] *Carpenter*, 138 S. Ct. at 2219-20.

[79] *Id.* at 2218; *see also* Mark Joseph Stern, *Sotomayor, Fourth Amendment Visionary: How the Supreme Court Vindicated the Justice's Prescient Theory of Digital Privacy*, SLATE (June 24, 2018, 5:56 PM), http://slate.com/news-and-politics/2018/06/in-carpenter-v-united-states-the-supreme-court-vindicates-justice-sonia-sotomayors-theory-of-digital-privacy.html [https://perma.cc/C3WE-BMHP] (discussing Chief Justice Roberts's reliance in *Carpenter* on Sotomayor's concurrence in *Jones* as reflected in his repeated citations to her concurrence).

[80] *Carpenter*, 138 S. Ct. at 2219.

[81] *Id.* at 2217.

[82] *Id*. Scholars have voiced similar concerns. *See* ERIN MURPHY, THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND CONTEMPORARY DEBATE 242, 243, 245-46 (Cynthia Lee ed., 2011) (warning that courts are overlooking the significant threat to liberty posed by technology such as GPS tracking bracelets, biometric scanners, offender and DNA database indexes).

[83] *Carpenter*, 138 S. Ct. at 2209-10.

Kennedy strenuously argued that the third-party doctrine controls CSLI business records, and therefore the government has a legal right to obtain them without a warrant.[84] He criticized the majority for using a category-by-category balancing test instead of strictly applying *Miller* and *Smith:*

> [T]he majority opinion misreads this Court's precedents, old and recent, and transforms *Mille*r and *Smith* into an unprincipled and unworkable doctrine. The Court's newly conceived constitutional standard will cause confusion; will undermine traditional and important law enforcement practices; and will allow the cell phone to become a protected medium that dangerous persons will use to commit serious crimes.[85]

To the dismay of third-party critics, Kennedy made no distinction at all between cell-site records and financial/telephone/business records. To him, cell phone customers like Carpenter simply have no possessory interest in them because CSLI is controlled and owned by the cell phone service provider, not by its customer.[86] He urged that the government has always had a longstanding lawful practice in collecting credit card information, and records for vehicle registration, hotel stays, employment, and utility bills—regardless of their personal and sensitive nature.[87] According to Kennedy, the *Smith*/*Miller* voluntariness requirement is also satisfied, since Americans are aware that they have a lesser expectation of privacy in the digital age, and voluntarily share their location with the public via social media.[88]

Here Kennedy downplays the general public's significant concerns about the government knowing too much. An *amicus* brief filed in *Carpenter* by empirical Fourth Amendment scholars, citing numerous studies reporting that a majority of people do not knowingly convey their locations information to cell phone providers and expect law enforcement to obtain a warrant before gathering information.[89] Public opinion polls also consistently show that Americans strongly support privacy rights.[90]

Further, Kennedy minimized the majority's concerns about invasiveness of CSLI and potential for mass surveillance, by arguing that unlike the pinpoint accuracy of GPS, CSLI imprecisely covers a large geographic area:

> [C]ell-site records . . . disclose a person's location only in a general area. The records at issue here, for example, revealed Carpenter's location within an area covering between around a dozen and several hundred city

[84] *Id.* at 2223 (Kennedy, J., dissenting).

[85] *Id.* at 2230.

[86] *Id.* at 2224.

[87] *Id.* at 2228-29, 2233.

[88] *Id.* at 2232.

[89] *See* Brief of Amici Curiae Empirical Fourth Amendment Scholars in Support of Petitioner at 3-10, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No.16-402).

[90] *See* Public Opinion on Privacy, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/survey [perma.cc/8LZA-4GBE].

> blocks. . . . These records could not reveal where Carpenter lives and works, much less his "familiar, political, professional, religious, and sexual associations."[91]

While Kennedy's assertion is debatable, what is clear is that surveillance technology has evolved considerably at a breakneck speed since *Carpenter* began an almost decade long journey to the high court. The litigation will continue. and as discussed below, law enforcement will increasingly rely on direct surveillance to satisfy its insatiable appetite for CLSI.

III. AFTER *CARPENTER*: ARGUING FOR A WARRANT REQUIREMENT FOR HISTORICAL AND REAL-TIME CLSI, THE THIRD-PARTY DOCTRINE IS NOT APPLICABLE TO REAL-TIME CELL PHONE MONITORING, AND THE THREAT OF FACIAL RECOGNITION SURVEILLANCE TECHNOLOGY

"[T]he third-party rationale no longer controls cases concerning historical CSLI data, and its persuasive authority is significantly undercut regarding real-time CSLI data."[92]

Without question, *Carpenter* reinvigorated *Katz v. United States*[93] by broadly applying its longstanding reasonable expectation of privacy analysis in the digital era.[94] Going forward, it is important to recall the origins and early development of the Fourth Amendment as well, while acknowledging the changing times. As the *Carpenter* majority noted, the Framers of the Constitution never anticipated how much and how fast technology would develop or how much the Fourth Amendment would be broadened to protect our privacy.[95] As evidenced in *Katz* and *Carpenter*, the Fourth Amendment flexes and evolves as technology expands and society moves forward. Just as public telephones were vital in 1967, we are even more reliant on smartphones fifty-years later. This has become the new normal. Mindful of this, Professor Friedman asserts, "Courts need to pay attention to present social conventions and based on these observations, distinguish between what is knowingly exposed to the public and what we want to keep private."[96]

Katz brought protections against unreasonable warrantless searches by the Government, but the opinion's murkiness also led to the growth of aggressive

---

[91] *Carpenter*, 138 S. Ct. at 2232.

[92] State v. Muhammad, 451 P.3d 1060, 1073 (Wash. 2019).

[93] Katz v. United States, 389 U.S. 347, 360-61 (1967).

[94] In *Katz*, the petitioner relied on the privacy of a phone booth when he made illegal gambling wagers not knowing that federal agents covertly attached an electronic listening and recording device onto the outside. *Id.* at 347, 349. The Court held that Fourth Amendment protected the petitioner's oral statements. *Id.*

[95] Relatedly, the Framers also did not predict the evolution of racially divisive modern law enforcement practices or predict the Court's practices or predict the Court's shift to probable cause and exclusionary rule. Carol Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 839 (1994).

[96] *See* FRIEDMAN, *supra* note 42, at 215.

policing. On this point, Professor David Gray says the *Katz* Court made a mistake by crafting a novel definition of "search" instead of basing their definition on the text and history of the Fourth Amendment.[97] Had *Katz* preserved the historical and basic meaning of "search," Gray says this would have prevented the creation of the third-party doctrine.[98]

As a rebuttal, Professor Ric Simmons, a proponent of surveillance technology, defends the third-party doctrine and wants to keep its intake in the wake of *Carpenter*.[99] He believes that the *Carpenter* Court overreacted in being too quick in finding a warrant requirement for access to all public data collection, and mosaic searches.[100]Absent the doctrine, Simmons says, criminals will conceal their illegal activities, maintain secrecy over their interactions with undercover agents, and store incriminating information with third-party companies.[101]

In contrast, Professor Stephen Schulhofer argues for requiring the government to get a warrant based on probable cause, and insists, "Fourth Amendment safeguards should apply whenever citizens convey personal information to a trusted third-party under promise of confidentiality."[102] Schulhofer further insists that the courts should "restore the Fourth Amendment to its intended position as a mechanism for preserving those spaces in the face of unprecedented technological, social, and political pressures."[103] Professor Gray shares a similar view, and adds a warrant requirement could be modeled after the Wiretap Act.[104] Under this regulatory regime, officers would be further required to exhaust other investigatory means before using tracking technologies, and officers must debrief the court afterward.[105]

---

[97] *See* GRAY, *supra* note 9, at 250. On this topic, Professor Jeffrey Bellin says that the *Katz* test is unpredictable, vague, difficult to apply, and often results in inconsistent search determinations. *See* Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV 233, 234-38 (2019). Bellin offers textualism and a clearer definition of "search" as an alternative to the *Katz* test of reasonable expectation of privacy. *Id.* at 239-241. Unfortunately, this is moving backwards and protecting places and property. We can never go back, just like forward progress of technology. Bellin's proposal will lead to courts returning to weakening privacy rights that existed before *Katz*— a world where the Fourth Amendment protected only property.

[98] GRAY, *supra* note 9, at 250.

[99] *See* SIMMONS, *supra* note 1, at 161.

[100] *See id*. at 126.

[101] *Id.* at 147, 161; *see also* Christopher Slobogin*, Policing, Databases, and Surveillance*, 18 CRIMINOLOGY, CRIM. JUST. L. & SOC'Y 70, 72 (2017) (using the example of cloud-based searches by the government, and discussing how a probable cause requirement may "handcuff legitimate government efforts to nab terrorists and criminals").

[102] STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY FIRST CENTURY 134 (2012).

[103] *Id.* at 143.

[104] GRAY, *supra* note 9, at 255.

[105] *Id.*

Using the above dialogue between the Fourth Amendment scholars as a springboard, this section offers three interrelated arguments: (1) a warrant requirement is needed for real-time CLSI; (2) the third-party doctrine is not applicable to real-time cell phone monitoring; and (3) facial recognition surveillance technology needs to be regulated.

A. Arguing for a Warrant Requirement for Real-Time CLSI

Carpenter represented a victory for privacy rights; however, it was too narrow of a ruling. Though a slew of questions remain after *Carpenter*, here I tackle two that the Court purposefully dodged to ensure that the government's investigative efforts are not completely thwarted because of a warrant requirement: (1) how should lower courts interpret the opinion's declaration that its holding is not applicable to real-time CSLI, and (2) how should jurists interpret *Carpenter*'s silence on historical CSLI for less than seven days.[106]

First, historical and real-time CSLI should be treated the same. For all intents and purposes, both types could be treated the same because they help law enforcement pinpoint a phone's location, when it continuously reveals its

[106] Also, *Carpenter*'s holding is not applicable to getting "tower dump" information about all of the phones that connected to a particular tower at a specific time, or national security or "urgent emergency situations." Carpenter v. United States, 138 S. Ct. 2206, 2217, 2220 (2018); Amy Howe, *Opinion Analysis: Court Holds That Police will Generally Need a Warrant for Sustained Cellphone Location Information*, SCOTUSBLOG (June 22, 2018, 6:01 PM), http://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/ [https://perma.cc/88H3-B7LU]; *see also* Jake Laperuque, *The* Carpenter *Decision: A Huge Step Forward for Privacy Rights but Major-Problems Remain*, POGO (June 28, 2018), https://www.pogo.org/analysis/2018/06/carpenter-decision-huge-step-forward-for-privacy-rights-but-major-problems-remain/ [https://perma.cc/YY7A-HQ5N]; Adam Liptak, *In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell phone-privacy.html [https://perma.cc/NSF3-THEV]; Eunice Park, *Protecting the Fourth Amendment After* Carpenter *in the Digital Age: What Gadget Next?* ORANGE COUNTY LAW. MAG., May 2018, at 35 (discussing the applicability of the then-forthcoming ruling in *Carpenter* and anticipating the repercussions for lower courts addressing next Fourth Amendment technology-based challenges such as Stingray and other technologies on the horizon). *Carpenter* also leaves ambiguity as to when the police will need a warrant rather than a subpoena or court order to get such information, and how specific the warrant or subpoena request must be. *See* Ass'n of Certified E-Discovery Specialists, *Judge Facciola Says* Carpenter *Decision May Signal the End of the Third-Party Doctrine*, JD SUPRA (July 5, 2018), https://www.jdsupra.com/legalnews/judge-facciola-says-carpenter-decision-57055/ [https://perma.cc/6QA9-5M5L]; *see also* Chemerinsky, *supra* note 21, at 79 (suggesting that courts adopt the reasoning of Carpenter and extend to all police investigations involving collection of records).

location to a wireless carrier.[107] This runs afoul of *Carpenter*. Legal scholars Susan Freiwald and Stephen Wm. Smith articulate this precise point:

> Real-time monitoring of cell phone location over time is presumptively a search and will require a warrant . . . the Third-Party Doctrine is not implicated here because the provider does not routinely generate or maintain business records containing precise location data like GPS . . . the multifactor analysis of *Carpenter* would seem equally applicable to prospective location data. Such data is hidden continuous, indiscriminate, intrusive, and inexpensive as historical CSLI.[108]

The government gets the same data sooner or later. Prospective CSLI becomes historical CSLI when the data collected is saved onto another database/server/hard drive/flash drive, and once a case goes to trial the prospective CSLI inevitably becomes historical CSLI anyway. A surveillance technology expert highlights this lack of distinction: "if police collect real-time location data on a mass scale and then stockpile it, they can then simply refer back to their own databases, looking up desired location information on internal servers and circumventing the warrant requirement."[109] Accordingly, the lower courts can conclude that the use of real-time CSLI to locate a defendant through his cell phone invades his actual legitimate and reasonable expectation of privacy in his location information, thus a search requiring a warrant.[110]

---

[107] *See* Kristi Winner, *From Historical Cell-Site Location Information to IMSI-Catchers: Why TriggerFish Devices Do Not Trigger Fourth Amendment Protection*, 68 CASE W. RES. L. REV. 243, 248-249 (2017). CSLI is more akin to content than neutral routing information. It shows when a call or text message is sent or received by, when cell phones are used, and the day and time when they connect to the cell tower emitting the strongest signal, including the GPS coordinates of each connected tower. CSLI can be used to approximate the location of the cellphone at particular times when transmissions are made. *See* United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015); *see also* Renée McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414-16 (2007) (describing the science and multiple uses of GPS).

[108] Freiwald & Smith, *supra* note 15, at 227.

[109] *See* Jake Laperruque, *Privacy After* Carpenter*: We Need Warrants for Real-Time Tracking and "Electronic Exhaustion,"* POGO (July 2, 2018), https://www.pogo.org/analysis/2018/07/privacy-after-carpenter-we-need-warrants-for-real-time-tracking-and-electronic-exhaustion/ [https://perma.cc/5EDQ-9L98].

[110] Cal Cumpstone, *Game of Phones: The Fourth Amendment Implications of Real-Time Cellphone Tracking*, 65 CLEV. ST. L. REV. 77, 101 (2016) ("Real-time cell phone tracking violates a person's reasonable expectation of privacy in both his or her physical location within constitutionally protected areas, such as homes, and in the location of the cell phone itself when held in pockets or containers not in open view of the general public."); Matthew DeVoy Jones, *Cell Phones are Orwell's Telescreen: The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information*, 67 CLEV. ST. L. REV. 523, 556 (2019) (arguing that *Carpenter* requires a warrant prior to law enforcement's collection of real-time CLSI).

Second, the *Carpenter* majority likely avoided discussing historical data collected over a time span of a week in part because it would have meant extending the warrant requirement for CSLI less than seven days. A quick review of a three-decades-old Court decision about tracking devices supports this theory. During the height of the war on drugs, in *United States v. Karo*, the Court found the DEA's electronic monitoring of a beeper placed on a can of ether into Karo's house without a warrant constituted an unlawful search.[111] The Court reasoned Karo had a justifiable interest in the privacy of his residence, a location not open to visual surveillance.[112] It concluded that the installation of the beeper did not constitute a "search" or "seizure" per se, but the Fourth Amendment implications began when the beeper was turned on and used as a tracker on private property. Despite this, Karo's conviction was upheld because the arrest warrant, contains enough information not derived from the unlawful use of the beeper, which provided sufficient probable cause.[113]

Curiously, *Karo* is missing entirely from *Carpenter*. It was probably by design because applying *Karo*'s clear rationale to the facts in *Carpenter* compels the conclusion that the government needs a warrant for even a brief real-time surveillance. In *Karo*, the beeper alone, without outside observation, informed the agents when the container was taken into private residences and storage.[114] Similarly, modern cellphones and smartphones when travelling unseen in a user's purses or pockets, pings its whereabouts.[115] Regarding this issue, Freiwald and Smith articulate, "[g]iven that cell phones are routinely used inside the home (even in the shower), as well as other places withdrawn from public view, it is difficult to imagine that *Karo* would allow warrantless monitoring for *any* length of time, day or night."[116] All told, defense attorneys can still make a strong argument that real-time CSLI, of any duration, does not fall under the third-party doctrine because the rationale in *Carpenter* would apply.[117] The jurisprudence for this proposition is growing.

Recent Washington Supreme Court and Massachusetts Supreme Judicial Court rulings offer persuasive and consistent authority for the proposition that *Carpenter's* reasoning equally applies to real-time CSLI, and not limited to any

[111] United States v. Karo, 468 U.S. 705, 708, 714-18 (1984).

[112] *Id.* at 714.

[113] *Id.* at 721.

[114] *Id.* at 714.

[115] *See* Winner, *supra* note 107, at 247-49.

[116] Freiwald & Smith, *supra* note 15, at 228; *see also* Cumpstone, *supra* note 110, at 94 ("Cell-site location data and GPS data, both the tools of real-time cell phone location tracking, would allow law enforcement agents to extend its tracking into private residences where the expectation of privacy is unassailable.").

[117] *See* DeVoy Jones, *supra* note 110, at 557 (arguing "[a]ny case regarding real-time cell phone location information should simply refuse to extend the third-party doctrine to real-time cell phone location information, since the rationale in *Carpenter* would apply").

amount of data.[118] In the Pacific Northwest, in *State v. Muhammad* the police lost track of Muhammad's car, and pinged his cell phone to locate it.[119] The Washington Supreme Court held that a cell phone ping is a search under the Fourth Amendment and the Washington state constitution requires a warrant absent exigent circumstances.[120] The court found that *Carpenter*'s reasoning applied to real-time CSLI by comparing historical CSLI to GPS monitoring.[121]

After considering the government's great ability to monitor and track, the court found a reasonable expectation of privacy in public movement.[122] The court then rejected the mosaic theory advanced by the government to claim that the cell phone ping, offering only limited information, was not a search, and that *Carpenter* was inapplicable to real-time CSLI. [123] To the court, the mosaic theory was unworkable in practice because it required jurists to make piecemeal judgments calls on acts by law enforcement and potential intrusions of a reasonable expectation of privacy.[124]

The court thereby concluded, "a cell phone user has a reasonable expectation of privacy in real-time CSLI, and the collection of location data implicates the Fourth Amendment."[125] The court held that *Carpenter* precluded warrantless access to any amount of cell phone location data irrespective of how minimal and no matter whether it was historical or prospective. As an end note, the Court referred to *Carpenter* to declare, "the third-party rationale no longer controls cases concerning historical CSLI data, and its persuasive authority is significantly undercut regarding real-time CSLI data."[126]

Back east, the Massachusetts Supreme Judicial Court interpreted its state constitution in *Commonwealth v. Almonor*.[127] There, the police asked a cellphone company to "ping" homicide suspect Almonor's target phone to discover its real-time location.[128] When the police found the phone's general location on a particular street, Almonor was found with a weapon, and a bulletproof vest in a house in the vicinity of the GPS ping.[129] The court held that the police must get a warrant to track cell phones in historical or real-time.[130]

---

[118] Commonwealth v. Almonor, 120 N.E.3d 1183, 1194 (Mass. 2019); State v. Muhammad, 451 P.3d 1060, 1070-72 (Wash. 2019).

[119] *Muhammad*, 451 P.3d at 1067.

[120] *Id.* at 1066, 1074-75.

[121] *Id.* at 1071-72.

[122] *Id.* at 1072-73.

[123] *Id.*

[124] *Id.*

[125] *Id.* at 1072.

[126] *Id.* at 1073.

[127] Commonwealth v. Almonor, 120 N.E.3d 1183, 1187 (Mass. 2019).

[128] *Id.*

[129] *Id.*

[130] *Id.* at 1188.

Using *Carpenter*'s analytical framework, and including *Karo*, the court reasoned that the intrusive nature of police action caused an individual's cell phone to transmit its real-time location raises distinct privacy concerns, because "[i]n today's digital age, the real-time location of an individual's cell phone is a proxy for the real-time location of the individual."[131] However, in the end analysis, the Court declined to suppress any of the incriminating evidence because the court found that the warrantless search was supported by probable cause and exigent circumstances existed.[132]

Demonstrating the opinion's wide scope, there was a related discussion of Stingray surveillance technology, another pressing issue punted by *Carpenter*.[133] In a footnote, the Massachusetts Supreme Court extended its analyses to address the surveillance techniques by the government, including the warrantless use of Stingrays which bypasses the third-party doctrine altogether:

> We recognize that the government's ability to compel a cell phone to reveal its location is not limited to the pinging that occurred in this case. . . . Nor do we doubt that as technology continues to advance, the *government will develop new ways to compel an individual's cell phone to reveal its location*. The privacy concerns raised by pinging a cell phone apply equally to any circumstance where the cell phone's location information is generated as a direct result of the *government's manipulation of an individual's cell phone*." [134]

Stingrays which have garnered increasing attention, are the military grade cell-site simulators used by federal and local law enforcement in the past decade to electronically track individuals suspected of criminal activity, or to conduct mass surveillance on groups of unsuspecting people or particular areas.[135] Stingrays directly capture texts, numbers of outgoing calls, emails, serial numbers, identification, GPS location, actual content of conversation, and other raw and detailed information from unsuspecting phones and track the location of targets and non-targets in apartments, cars, buses, and on streets through

[131] *Id.* at 1194.

[132] *Id.* at 1188.

[133] *Id.* at 1193 n.13 (addressing law enforcement's use of cell site simulators).

[134] *Id.* (emphasis added).

[135] *See* Alicia Lu, *What is StingRay, The Creepy Device Chicago Police "Used to Spy" on Eric Garner Protesters?,* BUSTLE (Dec. 9, 2014), http://www.bustle.com/articles/53050-what-is-stingray-the -creepy-device-chicago-police-used-to-spy-on-eric-garner-protesters [https://perma.cc/273R-STLT].

mapping software.[136] They can even make the tracked device send texts and make calls.[137]

Although there are legitimate uses of Stingrays in tracking down dangerous fugitives, Stingrays are more commonly used as a tracking device for locating stolen cell phones, or scanning from the skies over amusement parks and along the border. Absent any specified protocol about their Stingray use or judicial oversight, law enforcement may freely rely on Stingrays to target particular individual protesters or collect phone numbers en masse in high-crime areas.[138]

Upon challenge, the government's reluctance, and sometimes outright refusal, to provide information about the capabilities of Stingray technology to the courts evoke great skepticism about their legitimacy and efficiency. This outlook heightens even more whenever the FBI has required state prosecutors to dismiss charges in civil and criminal cases to avoid revealing information about the use and full capabilities of Stingray technology.[139]

---

[136] *See, e.g.*, FRIEDMAN, *supra* note 42, at 30; Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register Are Less Than a Wire Tap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 145-46 (2013); Austin McCullough, Note, *StingRay Searches and the Fourth Amendment Implications of Modern Cellular Surveillance*, 53 AM. CRIM. L. REV. ONLINE 41, 41 (2016); Marian Hetherly, *Judge Rules Surveillance Info Collected by Police Stingrays Can Remain Confidential*, WBFO (Apr. 12, 2018), http://news.wbfo.org/post/judge-rules-surveillance-info-collected-police-stingrays-can-remain-confidential [https://perma.cc/X6P3-6A8Q]. The collateral consequences resulting from their use, includes the disruption of cell service to phones in the form of service outages, blocked and dropped calls, and causing a connected cellphone's battery to drain and die. *See* Brian Barrett, *The Baltimore PD's Race Bias Extends to High-Tech Spying, Too,* WIRED (Aug. 16, 2016, 8:01 AM), http://www.wired.com/2016/08/baltimore-pds-race-bias-extends-high-tech-spying [https://perma.cc/P3NL-GSYP]; Colin Daileda, *The Police Technology Intensifying Racial Discrimination*, MASHABLE (Oct. 3, 2016), https://mashable.com/2016/10/03/police-technology-surveillance-racial-bias/ [https://perma.cc/R65W-VG8B].

[137] Andrew Hemmer, *Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches*, 91 CHI.-KENT L. REV. 295, 295-96 (2016) (describing the tracking abilities of Stingrays and how they can "hijack" a phone to perform calls and texts disguised as the targeted phones.

[138] *See* Kate Klonick, *Stingrays: Not Just for Feds! How Local Law Enforcement Uses an Invasive, Unreliable Surveillance Tool*, SLATE (Nov. 10, 2014, 9:52 AM), https://slate.com/technology/2014/11/stingrays-imsi-catchers-how-local-law-enforcement-uses-an-invasive-surveillance-tool.html [https://perma.cc/8APH-G76E]; *see also* Andrew Guthrie Ferguson, *The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis*, 57 AM. U. L. REV. 1587, 1590-92 (2008) (analyzing and critiquing reviewing courts consideration of an area as a "high crime area" as an evaluation factor determining reasonableness of Fourth Amendment stops).

[139] Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FED. SOC'Y REV. 29, 32 (2016) (reporting on speculation by commentators that state and federal charges have been reduced or dismissed by federal prosecutors

Not surprisingly, there is significant rebuke against the secret use of Stingray tracking by civil rights advocacy groups, public defenders, and jurists. Four years ago in *State v. Andrews*, the Maryland Court of Special Appeals ruled on the issue of whether a cell phone may be transformed into a real-time tracking device by the government without a warrant, and held that the Baltimore Police Department's use of Hailstorm, an upgraded version of the Stingray, required a valid search warrant based on probable cause.[140] The appellate court distinguished *Smith v. Maryland* and concluded that (1) unlike the defendant in *Smith*, Andrews, just by carrying and using a cell phone, did not "assume the risk" that the information obtained through the use of the Hailstorm device would be shared by the service provider and that (2) the third-party doctrine did not apply since he never voluntarily transmitted his location data to a third-party.

A year later, in *Jones v. United States*, the D.C. Court of Appeals ruled that the D.C. police's use of Stingray technology violated Jones's Fourth Amendment rights.[141] The majority determined that it was unconstitutional for the government to use a Stingray to find Jones before first obtaining a warrant based on probable cause.[142] Jones assaulted and robbed two women, and stole a cellphone from one of the women. The D.C. Metro Police anticipated that Jones would use the stolen cellphone, and without first getting a warrant, relied on a Stingray to track down the phone's location. The police were led to a parked car where they found and arrested Jones.[143] The appellate court found the use of a cell-site simulator as a locating device invades the "person's actual, legitimate, and reasonable expectation of privacy in his or her location information and is a search."[144]

After *Carpenter*, the Florida District Court of Appeals in *State v. Sylvestre* rejected the government's argument that an order for historical CSLI permitted the use of a Stingray in tracking down a robbery suspect's cell phone location and concluded that a warrant was necessary under *Carpenter*.[145] The appellate court observed: "With a cell-site simulator, the government does more than obtain data held by a third-party. The government surreptitiously intercepts a

in lieu of having to give confidential information about Stingrays to the court); Mike Maharrey, *Federal Programs are Funding Local Stingray Spying,* TENTH AMEND. CTR. (Aug. 26, 2017), https://tenthamendmentcenter.com/2017/08/26/federal-programs-are-funding-local-stingray-spying/ [https://perma.cc/AR3C-K3NF].

[140] State v. Andrews, 134 A.3d 324, 327 (2016).

[141] Jones v. United States, 168 A.3d 703, 716-17 (D.C. 2017).

[142] *Id.* at 707. The court ruled on the issue of whether the use of a cell-site simulator was a search even though the trial court declined to do so, and focused instead on the issues of standing, exigent circumstances, and inevitable discovery. *Id.* at 710.

[143] *Id.* at 708-09.

[144] *Id.* at 714-15.

[145] State v. Sylvestre, 254 So. 3d 986, 992 (Fla. Dist. Ct. App. 2018).

signal that the user intended to send to a carrier's cell-site tower or independently pings a cell phone to determine its location."[146]

The warrantless use of Stingrays is part of what Professor Friedman calls "policing without permission."[147] Against this kind of police state, Professor Friedman proposes regulation of policing as a partial remedy: "We need policies—transparent rules adopted with public input—to deal with the use of force, with implicit racial bias, with police adoption of new technologies."[148] Likewise, Professor Gray urges Congress and state legislatures to pass meaningful legislation limiting the government's ability to deploy overly broad searches and seizures.[149]

Fortuitously, several state legislatures have already passed legislation regulating the use of Stingrays and calling for transparency of Stingray policies. These kinds of activity directly or indirectly influenced the Justice Department's 2015 decision requiring federal investigators to obtain a search warrant from a judge to use the device.[150] Outside the beltway, Arizona, California, Colorado, Florida, Illinois, Indiana, Maine, Maryland, Minnesota, Missouri, Montana, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin have passed laws that protect citizens' cell phone data and require police to get a warrant to use a Stingray.[151] The Oregon Senate is considering a proposed law

[146] *Id.* at 991 (citing Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018)).

[147] FRIEDMAN, *supra* note 42, at 16.

[148] *Id.* at 326.

[149] *See* GRAY, *supra* note 9, at 17-18.

[150] *See* Robert Snell, *Feds Use Anti-Terror Tool to Hunt Undocumented Immigrants Amid Trump's Crackdown*, DETROIT NEWS (May 18, 2018, 10:49 PM), https://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/ [https://perma.cc/QA4M-YYPB]. Congress must also update and create privacy laws to address law enforcement's use of these advanced surveillance techniques. *See* Cox, *supra* note 139, at 35 (calling for Congress to draft legislation creating a new statutory right in privacy and limiting government's access to this data); *see also Congress Must Reckon with the Fourth Amendment and New Technology*, *supra* note 75 (opining that after *Carpenter*, Congress should step in to craft rules that clarify standards to accommodate new technology).

[151] *See, e.g.*, Cox, *supra* note 139, at 31 (discussing the reaction by various state legislatures to the use of Stingrays and remarking that "at least twelve states have passed laws mandating that law enforcement use of a cell-site simulator must be based upon a court issued search warrant based upon a finding of probable cause"); Katherine M. Sullivan, *Is Your Smartphone Conversation Private? The Stingray Device's Impact on Privacy in States*, 67 CATH. U. L. REV. 388, 390, 407-08 (2018) (arguing for more state legislation to protect privacy of citizens); Klonick, *supra* note 138; Mike Maharrey, *Arizona Bill Would Prohibit Warrantless Stingray Spying, Hinder Federal Surveillance Program*, TENTH AMEND. CTR. (Feb. 7, 2017), https://blog.tenthamendmentcenter.com/2017/02/arizona-bill-would-prohibit-warrantless-stingray-spying-hinder-federal-surveillance-program/ [https://perma.cc/PLG4-GY3B]; Mike Maharrey, *Florida Committee Passes Bill to Ban Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMEND. CTR. (Feb. 11, 2018), https://blog.tenthamendmentcenter.com/2019/02/florida-committee-passes-bill-to-ban-warrantless-stingray-spying-

that would block the warrantless use of Stingrays in order to protect privacy rights.[152] The Texas legislature is also considering a warrant requirement for Stingrays except in emergency situations.[153] New York and approximately 17 other localities are developing similar legislation.[154]

B. The Third-Party Doctrine is Not Applicable to Real-Time Cell phone Monitoring

Even before *Carpenter*, the Fourth and Eleventh Circuits were already declining to apply the third-party doctrine in surveillance cases. Those opinions were consistent with the design of the Fourth Amendment as a counterweight to the authority of government agents armed with general warrants and writs of assistance to conduct broad and indiscriminate searches with impunity.[155] Embracing the principles set forth in *Carpenter*, state and federal courts can now follow the trail already paved by the Fourth and Eleventh Circuits in explicitly determining that the third-party doctrine should not apply to the use of historical

help-hinder-federal-surveillance-2/ [https://perma.cc/CD47-JUSJ]; Mike Maharrey, *Missouri Committee Passes Bill to Ban Warrantless Stingray Spying; Help Hinder Federal Surveillance*, TENTH AMEND. CTR. (Feb. 21, 2018), https://blog.tenthamendmentcenter.com/2018/02/missouri-committee-passes-bill-to-ban-warrantless-stingray-spying-hinder-federal-surveillance/ [https://perma.cc/D4ZV-K9WJ]; Snell, *supra* note 150 (offering that States can adopt laws requiring judicial authorization before local law enforcement is allowed to use Stingrays and limiting on how long they can retain the data and reserve their use only in cases implicating violence or harm to human life).

[152] Mike Maharrey, *Oregon Bill Would Ban Warrantless Stingray Spying, Help Hinder Federal Surveillance*, TENTH AMEND. CTR. (Jan. 17, 2019), https://blog.tenthamendmentcenter.com/2019/01/oregon-bill-would-ban-warrantless-stingray-spying-help-hinder-federal-surveillance/ [https://perma.cc/KU74-P6DH].

[153] Anna M. Tinsley, *Texas Lawmakers' Bills Would Limit Cellphone Trackers*, FORT WORTH STAR-TELEGRAM (Apr. 18, 2015, 3:58 PM), https://www.star-telegram.com/news/politics-government/article18868620.html [https://perma.cc/2YC7-G54K].

[154] Andy Martino, *Black Lives Matter Activists are Convinced the NYPD Hacked Their Phones*, THE OUTLINE (Apr. 7, 2017, 1:30 PM), https://theoutline.com/post/1360/black-lives-matter-police-surveillance-the-cops-hacked-their-phones [https://perma.cc/2RLR-PU8Z]. But some localities have pushed back against such transparency laws. *See* Michael Maharrey, *California Committee Kills Bill to Help End Unchecked Police Surveillance* (Aug. 22, 2018), https://blog.tenthamendmentcenter.com/2018/08/california-committee-kills-bill-to-help-end-unchecked-police-surveillance/ [https://perma.cc/CFM5-U4XV]. For example, a California Assembly committee held up a bill in appropriations that would have increased oversight and transparency of law enforcement surveillance technology, preventing the bill from moving forward. *Id.*

[155] GRAY, *supra* note 9, at 70-71; *see also* David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 99-100 (2018) (explaining that the historical goal of the Fourth Amendment "was to provide for the general security of the nation and society as a whole against threats posed by grants of unfettered discretion to government agents to conduct searches and seizures").

CSLI.[156] Informed by the analyses of real-time CSLI in subsection A, and by analogy, lower courts could determine that the third-party doctrine does not apply to real-time CSLI either. These two lengthy rulings are especially instructive because they go into more depth about the third-party doctrine's inadequate fit with emerging technology than *Carpenter*.[157]

Diving in, an en banc Fourth Circuit in *United States v. Graham* found the third-party doctrine inapplicable to the facts, and held that the government's warrantless procurement of CSLI for 221 days in an investigation of robberies violated the Fourth Amendment.[158] Yet the court allowed the government to use the CSLI under the "good faith" exception to the exclusionary rule.[159]

Although I disagree with the result in *Graham*, I agree with the court's reasoning that the third-party doctrine of *Miller* and *Smith* is inapplicable because cell phone users do not voluntarily convey their CSLI to their service providers Sprint/Nextel.[160] The Fourth Circuit explained that cell phone users do not assume any risk of disclosure to law enforcement by using their devices because the data created by the user, including location-identifying information and messages and calls received but not answered, do not involve any affirmative act by the user.[161] The court further declared:

> [S]ociety recognizes an individual's privacy interest in her movements over an extended time period . . . . The fact that a provider captures this information in its account records, without the subscriber's involvement, does not extinguish the subscriber's reasonable expectation of privacy. *Applying the third-party doctrine in this context would simply permit the government to convert an individual's cell phone into a tracking device by examining the massive bank of location information retained by her service providers and to do so without probable cause*.[162]

A complimentary view was conveyed by Judge Martin's insightful dissent challenging the reach of the third-party doctrine in *United States v. Davis*.[163] Martin disagreed with the en banc Eleventh Circuit's holding that government collection of a third-party telephone company's business records pursuant to the SCA, which produced 67 days of historical cell cite information for the plaintiff's cell phone, did not constitute a search and did not violate the Fourth

---

[156] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[157] United States v. Graham, 796 F.3d 332, 359-60 (4th Cir. 2015).

[158] *Id.* at 338, 353.

[159] *Id.* at 361-63.

[160] *Id.* at 354-55.

[161] *Id.*

[162] *Id.* at 357 (emphasis added).

[163] United States v. Davis, 785 F.3d 498, 533 (11th Cir. 2015) (en banc), *abrogated by* Carpenter v. United States, 138 S. Ct. 2206 (2018).

Amendment.[164] Martin argued that the government was required to obtain a warrant under the Fourth Amendment.[165] He cautioned about the dangers of an expansive application of the third-party doctrine, which would allow the government warrantless access of cell phone users' locations at any given time, along with individuals' email recipients, browser histories, shopping records, and online personals.[166]

The thrust of Martin's dissent comes when he distinguished Davis's facts from *Smith v. Maryland*. He stated cell phone users, unlike phone numbers a person dials from a home phone connected to a landline, do not affirmatively enter their location when making a call.[167] Martin added that the *Miller/Smith* rule is limited, and the government cannot access all information that any third-party obtains.[168] Martin especially criticized the panel majority's "blunt application" of the third-party doctrine as enabling the government to gain an immense amount of information while infringing upon privacy rights.[169] Martin reasoned that since a majority of adults do not expect their cell phones tracked by the government, Davis did not intend to disclose his location to the government. Thus, he had a reasonable and subjective expectation that his physical movement would be private.[170]

Now with the blessing of the *Carpenter* rationale, future courts should feel confident, if not emboldened, to conclude the third-party doctrine as inapplicable, and in following the majority of federal courts having considered the issue of whether there is a reasonable expectation of privacy in real-time CSLI. These courts concluded CSLI information may only be obtained pursuant to a warrant supported by probable cause because it effectively converts the cell phone into a tracking device.[171] As one scholar opined:

---

[164] *Id.* at 500. According to majority: (1) the CSLI was non-content evidence; (2) Davis did not own the information held by the third-party telephone company; and (3) Davis had not subjective or objective reasonable expectation of privacy in the CSLI. *Id.* at 511. Embracing the third-party doctrine, the court stressed that CSLI differs from GPS tracing because it does not pinpoint the user's location, it only identifies nearby cell towers that are routing the user's call. *Id.* at 515-16. The majority stated that even if there was a search, "any intrusion on Davis's alleged privacy expectation, arising out of MetroPCS's production of its own records pursuant to a § 2703(d) order, was minimal . . . [because] there was no overhearing or recording of any *conversations* . . . [and] there is no GPS real-time tracking or precise movements of a person or vehicles." *Id.* at 517.

[165] *Id.* at 533 (Martin, J., dissenting).

[166] *Id.*

[167] *Id.* at 534.

[168] *Id.* at 535.

[169] *Id.*

[170] *Id.* at 539.

[171] *See, e.g.*, United States v. Espudo, 954 F. Supp. 2d 1029, 1035-36 (S.D. Cal. 2013) (reasonable expectation of privacy in prospective cell phone location information, concluding real-time cell phone data not business records under the Stored Communications Act); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified

> If law enforcement were to follow *Carpenter*, it would understand that because the third-party doctrine was not extended to historical CSLI, it would not extend to any similar information, such as real-time cell phone location information, that would allow the government to obtain private and detailed information with minimal effort.[172]

On the flipside, Professor Simmons argues against a probable cause requirement for modern policing based on his belief that it would place severe limitations on law enforcement's use of low-cost, effective, Big Data tools.[173] But Simmons's concerns are exaggerated. Judging by the continual erosion of the Fourth Amendment in judicial rulings giving great deference to the government in traffic stops, searches and seizures, and surveillance cases, coupled with the great lengths that the government will go in surreptitiously acquiring information in their investigations, a probable cause requirement is not asking for much.

To be sure, there are reasons for not trusting the government to honor the Fourth Amendment when using surveillance technology to snoop. Look at the track record. From the 1960s to the present day, modern policing went from reactive policing to proactive monitoring with technology.[174] Since 1992, the Drug Enforcement Agency has heavily relied on technology in drug cases (pen registry, electronic beepers, and wire taps) during the "War on Drugs" and in 2013, eighty-eight percent of the Department of Justice's wiretap warrants were filed under seal in drug cases (cell-site records location data from wireless carriers).[175] The U.S. District Court for the District of Columbia released information showing an impressive sevenfold surge in law enforcement requests under seal to track Americans without warrants through cell phone locations and internet activity in the past three years.[176] Also, the public learned last year about

---

Wireless Tel., 849 F. Supp. 2d 526, 539-43 (D. Md. 2011) (reasonable expectation of privacy in location and movements revealed by cell phone data); *In re* Application of the U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No. ESN, Misc. No. 06-0186, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006) (same: probable cause required for cell phone tracking data warrant); *In re* Application of the U.S. for an Order Authorizing the Use of an Pen Register and a Trap and Trace Device, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (same); *see also In re* Application of the U.S. for Historical Cell Cite Data, 724 F.3d 600, 615 (5th Cir. 2013)(expressly limiting its holding to historical data).

[172] DeVoy Jones, *supra* note 110, at 548.

[173] *See* SIMMONS, *supra* note 1, at 131.

[174] *See* JAMES FORMAN, JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 20, 25 (2017).

[175] *See* Andy Greenberg, *Want to See Domestic Spying's Future? Follow the Drug War*, WIRED (Apr. 10, 2015, 7:00 AM), https://www.wired.com/2015/04/want-see-domestic-spyings-future-follow-drug-war/ [https://perma.cc/L8AN-G6TM].

[176] *See* Spencer S. Hsu, *In District, Warrantless Tracking Requests Surge in Past 3 Years*, WASH. POST, July 19, 2017, at B1. To add to this, law enforcement pen registry and trap and

the National Security Agency's illegal collection of communication information from domestic phone calls and text messages.[177] A month later, it was revealed that the FBI searched unsuspecting Americans' emails without warrants or individualized grounds for suspicion.[178]

Further, third-party doctrine cheerleaders seem to conveniently forget about the government's huge advantage of having the "good faith" exception to the exclusionary rule at its disposal. When the government fails to convince a court that there was no search in phone tracking cases, it will nevertheless often succeed in arguing that the CSLI were not subject to suppression because the government acted in good-faith reliance on court orders issued under the SCA.[179] This argument has been so successful that the good faith exception has barred almost all defendants from suppressing CSLI evidence in surveillance cases.[180] It is this same exception that prevented Carpenter from being granted any relief on remand—the Sixth Circuit ordered that Carpenter must serve out his 116-year prison sentence despite having his Fourth Amendment right violated because the agents acted reasonably and in good faith relying on the SCA.[181]

---

trace requests to conduct electronic surveillance and track metadata information about telephone, email, and social media, have increased exponentially in Washington and Northern Virginia, two of the most active federal courts. *See also* Spencer S. Hsu & Rachel Weiner, *U.S. Courts: Electronic Surveillance Up 500 Percent in D.C.-Area Since 2011, Almost All Sealed Cases*, WASH. POST (Oct. 24, 2016), https://www.washingtonpost.com/local/public-safety/us-courts-electronic-surveillance-up-500-percent-in-dc-area-since-2011-almost-all-sealed-cases/2016/10/22/48693ffa-8f10-11e6-9c52-0b10449e33c4_story.html [https://perma.cc/Y8L6-QBSM] (explaining that unlike traditional wiretaps to listen to land-line phone calls requiring probable cause, these requests only require the government to persuade a judge that the information sought is relevant to an investigation); Naomi Gilens, *New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance*, ACLU (Sept. 27, 2012, 1:32 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/new-justice-department-documents-show-huge-increase [https://perma.cc/2VBA-2AMC].

[177] *See* Charlie Savage, *N.S.A. Collected Call Data It was Not Authorized to*, N.Y. TIMES, June 27, 2019, at A17. The NSA monitors Americans by acquiring data from phone calls and text messages, and analyzes patterns of movement with other intersecting mobile device users. *See* Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801facstory.html [https://perma.cc/D8R9-QL72].

[178] *See* Charlie Savage, *Judge Says F.B.I Tactics Violated Right of Privacy*, N.Y. TIMES, Oct. 9, 2019, at A16.

[179] *See* 18 U.S.C. § 2703 (2018).

[180] *See* Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting* Carpenter*?*, LAWFARE (Oct. 18, 2018, 8:57 AM), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter [https://perma.cc/A3YV-PWWJ].

[181] United States v. Carpenter, 926 F.3d 313, 318 (6th Cir. 2019).

A more recent example is *United States v. Elmore*, where the Ninth Circuit held that police lacked probable cause to obtain CSLI data showing the defendant to be in the vicinity of a shooting death.[182] Although the affidavit for warrant offered scant inferences about the defendant and did not support a reasonable inference that defendant's CSLI contained evidence of a crime, the majority panel nevertheless concluded that the good faith exception to the exclusionary rule applied.[183] This finding raised the ire of dissenting Judge McKeown who opined that the warrant affidavit "so thoroughly lacked probable cause that was objectively unreasonable for the officer to have relied on it" and that "[w]eak inferences from vague facts do not amount to probable cause as to specific individuals."[184]

Although the legislative process is agonizingly slow, law makers can follow California's Electronic Communications Privacy Act (CalECPA) as an example until national laws are enacted regulating the government's use of real-time surveillance technology.[185] CalECPA went into effect in 2016, and requires government entities in California to obtain a warrant based on probable cause before they can obtain a person's electronic communication information from a person's service provider or electronic device. CalECPA goes further than the ECPA by broadly requiring warrants for content metadata, location data, and electronic device data.[186] Unlike ECPA, CalECPA requires the government to furnish notice to the target of the investigation, and provides a suppression remedy for evidence gathered in violation of its terms.[187] Unlike the SCA, CalECPA protects information stored on electronic devices.[188] Significantly, CalECPA does not distinguish on the basis of historical as opposed to prospective or real-time data.[189]

C. The Threat of Facial Recognition Surveillance Technology and the Need for Regulation

Facial recognition and facial surveillance technology are the latest threats to associational privacy and personal security.[190] These two distinct kinds of technology are not governed by any legislation, and it remains an open question

[182] United States v. Elmore, 917 F.3d 1068, 1075 (9th Cir. 2019).

[183] *Id.* at 1075-78.

[184] *Id.* at 1079 (McKeown, J., dissenting).

[185] CAL. PENAL CODE § 1546 (West Supp. 2020).

[186] *See* Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, 33 BERKELEY TECH. L.J. 131, 162-64, 174 (2018).

[187] *Id.* at 135.

[188] *Id.* at 147-48.

[189] *Id.* at 174.

[190] *See* Ferguson, *supra* note 12, at 3-4; Taylor Book, *Recognizing Your Privacy Rights: Facial Recognition Technology and Third-Party Doctrine*, MICH. TECH. L. REV. (Apr. 25, 2019), http://mttlr.org/2019/04/recognizing-your-privacy-rights-facial-recognition-technology-and-third-party-doctrine/ [https://perma.cc/DUB5-JDTF].

as to whether the use of such technology by law enforcement constitutes a search for the purposes of the Fourth Amendment.[191]

To begin with, the parallels between Stingrays and facial recognition technology are striking. A few years ago, the Baltimore Police Department used Stingrays and facial recognition technology in tandem during the Freddie Gray riots and during peaceful Black Lives Matter demonstrations calling for police accountability.[192] Similar to the secrecy over Stingrays, law enforcement agencies are keeping hush about their use of facial recognition software. The New York City Police Department shrouds their use of real-time facial recognition surveillance in secrecy, and the American Civil Liberties Union has sued the Justice Department, the DEA, and the FBI for records detailing their use of facial recognition software.[193]

As an investigative tool, facial recognition systems use computer algorithms to compare data on other face images previously collected and stored in driver's license database, government identifications records, police bookings of all arrestees (including people who are arrested but never charged or who are found innocent), and social media accounts.[194] The third-party doctrine gives the FBI, the central source for face recognition identification for federal, state, and local law enforcement agencies, access to over 641 million photos, including

[191] There is hope that courts will find facial recognition technology must respect the right to privacy. In one case, the Ninth Circuit ruled that Facebook users in Illinois can move forward in suing Facebook over facial recognition technology. Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019). This was the first federal circuit decision to directly address privacy concerns about facial recognition technology. The case concerned Facebook users in Illinois who accused Facebook of violating the State's Biometric Information Privacy Act, designed to safeguard their privacy. *See* 740 ILL. COMP. STAT 14/1 (2008). In 2010, Facebook launched a feature called "tag suggestions" that analyzes the details of people's faces in hundreds of millions of daily uploaded photos. Facebook argued that users could show no concrete harm, but the Ninth Circuit determined intangible injuries can still be concrete, and cited to recent Fourth Amendment jurisprudence including *Carpenter* and the Court's views on "enhanced technological intrusions on the right to privacy." *Patel*, 932 F.3d at 1273.

[192] *See* Klonick, *supra* note 138.

[193] Ángel Díaz, *New York City Police Department Surveillance Technology*, BRENNAN CTR. FOR JUST. (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology [https://perma.cc/5W9D-8NYB] (reporting on New York Policy Department's efforts to shroud their use of real-time facial recognition surveillance in secrecy); Harwell, *supra* note 2 (reporting on American Civil Liberties Union lawsuit against the Justice Department, the DEA, and the FBI for records detailing their use of facial recognition software).

[194] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A. CRIM. JUST. MAG. (Spring 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/WQZ7-SZUK].

"volunteered" driver's license and passports and mandatory mug shots.[195] The FBI facial recognition database contains 25 million state and federal mug shots with associated criminal fingerprints.[196]

The FBI has faced intense backlash. It began two years ago when the US Government Accountability Office (GAO) analyzed the FBI's use of facial recognition technology and found it to be lacking in accountability, accuracy and oversight, and made recommendations of how to address the problem.[197] The FBI's inaction irritated the House Oversight Committee during the second of three hearings last summer, when lawmakers in Washington intensified their calls for a temporary ban on the federal government's use of facial recognition technology.[198] More specifically, the late Elijah Cummings, former Oversight Committee Chairman, criticized the FBI for failing to implement changes previously recommended by the GAO addressing privacy and accuracy concerns about the technology.[199] After the hearing, Democratic and Republican oversight members expressed support for a full moratorium on facial recognition technology until civil rights and liberties concerns are addressed satisfactorily.[200]

In one of the largest studies of facial recognition technology, the National Institute of Standards and Technology's negative performance review of facial recognition adds fuel to the fire.[201] The results of the study show that the majority of commercial facial-recognition systems exhibit bias.[202] Agency researchers accessed "more than 18 million photos of about 8.5 million people from mug shots, visa applications and border-crossing databases . . . [and] tested 189 facial-recognition algorithms from 99 developers."[203] The following were among the disconcerting findings involving race: the systems tested falsely

[195] *See* Frank Konkel, *The FBI is Trying Amazon's Facial-Recognition Software*, NEXTGOV (Jan. 3, 2019), https://www.nextgov.com/emerging-tech/2019/01/fbi-trying-amazons-facial-recognition-software/153888/ [https://perma.cc/RKG4-RAMX**]**.

[196] *Id*.

[197] *See* Mary Harris, *Amazon Encourages Police to Use Untested Facial Recognition Technology*, SLATE (May 24, 2019, 3:06 PM), https://slate.com/news-and-politics/2019/05/facial-recognition-police-officers-hillsboro-oregon-amazon.html [https://perma.cc/72H6-XEYC**]**.

[198] Emily Birnbaum, *FBI Database Strokes Worries Over Facial Recognition Tech*, THE HILL (June 4, 2019, 8:04 PM), https://thehill.com/policy/technology/446991-fbi-database-stokes-worries-over-facial-recognition-tech [https://perma.cc/Y7M8-N9JV].

[199] *Id*.

[200] *Id*.

[201] *See* Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/5XYN-5F5U].

[202] *Id.*

[203] *Id.*

identified African Americans and Asian faces 10 times to 100 times more than Caucasian faces; and Native Americans represented the highest error rates. [204]

In the third hearing before the oversight committee at the beginning of 2020, lawmakers expressed continued concern of abuses of facial recognition technology by the government, and this time they agreed to pass bipartisan legislation designed to examine the government's use of facial recognition programs and evaluate whether they infringe upon the First and Fourth Amendments.[205]

Incredibly, the controversy over the facial recognition in D.C. has done little to dissuade local police from scanning surveillance footage from third-party platforms to identify faces, and data mine stored images containing revealing metadata from third-party platforms, including Facebook, Google, Instagram, Twitter, and YouTube, to identify persons.[206] The Department of Homeland Security, under the auspices of national security, has even proposed a new rule requiring all travelers, including U.S. citizens, to be photographed upon entry and/or departure.[207] False positive matches could result in real and harmful consequences including missed flights, interrogations, and false accusations and arrests.[208]

All the while, Americans are becoming more aware of facial recognition technology. A Pew Research Center report shows Americans have mixed sentiments about facial recognition.[209] More than half of Americans surveyed trust law enforcement to put facial recognition software to good use, yet the survey showed that whites expressed more support than African Americans and Hispanics.[210]

More telling are Georgetown Center on Privacy and Technology's extensive reports concluding that facial recognition technology is fraught with issues and concerns over: (1) the endless sources of images, such as the internet, through

---

[204] *Id*.

[205] Sabrina Eaton, *Facial Surveillance Alarms Congress; Republicans and Democrats Pledge Action*, CLEVELAND.COM (Jan. 15, 2020), https://www.cleveland.com/open/2020/01/facial-surveillance-alarms-congress-republicans-and-democrats-pledge-action.html [https://perma.cc/KD7T-37XS].

[206] *See* Ferguson, *supra* note 12, at 15-16.

[207] Dan King, *The Trump Administration's Dangerous Facial Surveillance Scheme*, AM. CONSERVATIVE (Dec. 11, 2019, 1:02 PM), https://www.theamericanconservative.com/articles/the-trump-administrations-dangerous-facial-surveillance-scheme/ [https://perma.cc/XX8E-RWYW].

[208] Singer & Metz, *supra* note 201.

[209] Dalvin Brown, *Pew Survey: Americans Trust Police More Than Tech Giants to Use Facial Recognition*, USA TODAY (Sept. 5, 2019, 10:00 AM), https://www.usatoday.com/story/tech/2019/09/05/facial-recognition-americans-dont-trust-tech-firms-says-report/2210864001/ **[**https://perma.cc/7YYM-P3CM**].**

[210] *Id.*

which police utilize face recognition algorithms to start investigation leads;[211] (2) law enforcement agencies' failures to verify facial recognition systems for accuracy;[212] (3) a majority of face recognition systems are not audited for misuse;[213] (4) the disproportionate misidentification of African Americans, women, and senior citizens by police systems' facial recognition technologies;[214] and (5) the potential chilling effect on our First Amendment rights to free speech and peaceful assembly at public gatherings.[215]

The Center concluded its analysis by recommending a moratorium on the use of face recognition.[216] The Center further recommended state legislatures pass commonsense legislation and policy to comprehensively regulate facial recognition technology, including requiring reasonable suspicion of criminal conduct prior to a face recognition search.[217]

Facial surveillance technology is equally problematic because facial surveillance casts such a wide net. Street surveillance cameras and police worn body cameras indiscriminately cross-compare all faces from various distances, varied angles, and different lighting against a search list.[218] Officers can use real-time facial recognition software linked to video surveillance cameras and biometric databases to check a person for active warrants, assess his risk level, and monitor prior locations at particular times through citywide surveillance images.[219] As with CSLI and Stingrays, this real-time tracking of individual's movement over an extended period of time could reveal intimate details about the individual's personal life.[220]

Notably, private technology companies enable law enforcement with their surveillance efforts. The FBI and the police routinely use Amazon's

---

[211] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. CTR. ON PRIVACY & TECH. 1, 9 (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/AAB7-A2Q3].

[212] *Id.*

[213] *Id.*

[214] Clare Garvie & Laura M. Moy, *America Under Watch-Face Surveillance in the United States*, GEO. CTR. ON PRIVACY & TECH. (May 16, 2019), https://www.americaunder-watch.com/ [https://perma.cc/UES5-DJTY]; Jake Laperrugue, *Facial Recognition Surveil-lance Face: New Calls for Legal Limits*, PROJECT ON GOV'T OVERSIGHT (Mar. 13, 2019), https://www.pogo.org/analysis/2019/03/facial-recognition-surveillance-faces-new-calls-for-legal-limits/ [https://perma.cc/GP6T-YA66]; Singer & Metz, *supra* note 201.

[215] Garvie & Moy, *supra* note 214.

[216] Clare Garvie*, Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. CTR. ON PRIVACY & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/AA7R-29EN].

[217] Garvie et al., *supra* note 211.

[218] Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELECTRONIC FRONTIER FOUND., 1, 6-7 (May 2019), https://www.eff.org/wp/law-enforcement-use-face-recognition [https://perma.cc/3QLY-KXRG].

[219] *Id.* at 1, 4.

[220] *See* Ferguson, *supra* note 12, at 15-16; Hamann & Smith, *supra* note 194.

"Rekognition," a facial matching software program that tracks and identifies people as they walk down the street living their life at schools, airports, malls, stadiums, or attending political rallies.[221] Rekognition has been widely panned for its inaccuracy, and especially disproportionate misidentification of racial minorities. Astonishingly, forty percent of the false matches by Rekognition used by the police involved persons of color.[222] The program even mistakenly identified 28 Congressman as known criminals.[223]

More dubious is Clearview AI's new groundbreaking facial recognition app Smartcheckr used by the FBI, the Department of Homeland Security, and over 600 law enforcement agencies.[224] Akin to a Google search, in just seconds, the app allows a sensitive photo of a person to be uploaded to match public photos of that person, and to offer links to where those photos appeared.[225] Astonishingly, Smartcheckr has a database of more than three billion images scraped from Facebook, YouTube and millions of other websites. Smartcheckr also allows users the option of wearing "augmented–reality glasses" to take photos of a person walking down the street, and then learn of their home address, listen in on their conversations, and get other confidential information.[226]

There is more. Police can also upload photos and videos taken from a bystander's phone. Additional unease is found in Clearview AI's ability to store all uploaded content, and manipulate results.[227] Although law enforcement agencies attest to the Smartcheckr's effectiveness, this relatively new app has yet to be independently checked for accuracy by the National Institute of Standards and Technology, or anyone else. Like Stingrays, such technology will likely encourage copycat competing devices.

Against this backdrop, Professors Ferguson and Friedman in a *New York Times* editorial advocated for a ban on facial surveillance, and tight regulation allowing police to only use facial recognition technology to identify a criminal suspect caught on camera. These legal scholars also want equal treatment of all

[221] Book, *supra* note 190; Laperrugue, *supra* note 214; Konkel, *supra* note 195; Dean DeChiaro, *Bipartisan Thumbs-Down to Facial Recognition Technology*, ROLL CALL (May 29, 2019, 5:00 AM), https://www.rollcall.com/news/policy/bipartisan-thumbs-down-to-facial-recognition-technology [https://perma.cc/2NEQ-CXDF].

[222] Queenie Wong, *Why Facial Recognition's Racial Bias Problem is So Hard to Crack*, CNET (Mar. 27, 2019, 5:00 AM), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/ [https://perma.cc/X73R-753C].

[223] Sean Hollister, *Amazon Facial Recognition Mistakenly Confused 28 Congressman with Known Criminals*, CNET (July 26, 2018, 12:45 PM), https://www.cnet.com/news/amazon-facial-recognition-thinks-28-congressmen-look-like-known-criminals-at-default-settings [https://perma.cc/QKM8-GZNT]; Eaton, *supra* note 205.

[224] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/35T7-BN2H].

[225] *Id*.

[226] *Id*.

[227] *Id*.

races and genders, a warrant requirement, and suggests that search technology should not be limited to criminal databases.[228]

Surely Ferguson and Friedman contribute to the facial recognition conversation, yet they only scratch the surface of a discussion about the interplay between race and facial matching software. This issue deserves broader discussion. Aware of the subordination effects of facial recognition, a coalition of more than 42 racial justice and civil rights groups demanded tech companies stop selling the technology to government because such technology exacerbates historical and existing biases harming already over policed communities.[229] The Electronic Frontier Foundation claim facial recognition technology contributes to:

[O]ver-policing in Black and Latinx neighborhoods. If such systems are included into street lights or other forms of surveillance cameras, these communities may be unfairly targeted simply because they appeared in another database or were subject to discriminatory policing in the past.[230]

Especially troubling is the manner in which Big Data analyzes collected data and targets persons employing "person-based predictive targeting" and "place-based predictive targeting."[231] This data-driven approach identifies criminal patterns in specific geographic locations and deploys resources to those areas.[232] Writing separately in his volume, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, Professor Ferguson cautions these technical advancements comes with a cost since they are prone to distorting reasonable suspicion, "[i]ndividuals who live in high-crime areas or who have repeated contacts with police may increasingly be linked with others would have been targeted for increased police attention."[233]

The issue is not that clear-cut. Professor Simmons counters that under the Fourteenth Amendment, race can be used as a factor for reasonable suspicion or probable cause, and he approves of properly designed algorithms that explicitly use race if "there would be empirical statistical proof that in the given context, race did help determine whether or not an individual was guilty of a crime." [234] Simmons maintains that mechanical predictive algorithms are more effective

---

[228] Barry Friedman & Andrew Guthrie Ferguson, *Here's a Way Forward on Facial Recognition*, N.Y. TIMES (Oct. 31, 2019), https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html [https://perma.cc/5UM9-KZHX].

[229] Jon Schuppe, *Axon's Police Body Cams Could Be Getting an AI Upgrade. Civil Rights Groups are Worried*., NBC NEWS (Apr. 26, 2018, 11:30 AM), https://www.nbcnews.com/news/us-news/axon-s-police-body-cams-could-be-getting-ai-upgrade-n869071 [https://perma.cc/H748-WEWC].

[230] Lynch, *supra* note 218.

[231] *See* ANDREW FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 34, 62 (2017).

[232] *Id*.

[233] *Id*. at 57.

[234] *See* SIMMONS, *supra* note 1, at 48.

than the current system that counts on implicated implicit biases held by police officer and judges.[235] However, as Simmons himself concedes, these predictive algorithms using race would not survive Equal Protection Clause challenges, not to mention public outcries of racial profiling.[236]

Moving forward, there are reasons to be optimistic about efforts to curtail the government's use of facial recognition technology. Bill S.847, the Commercial Facial Recognition Privacy Act of 2019 was introduced in the Senate to prohibit the commercial use of facial recognition technology to identify and track consumers without consent.[237] That bill placed limitations on the third-party sharing of collected face print data, and required entities to meet certain minimum data security standards.[238] On the west coast, California has passed the California Consumer Privacy Act (CCPA), the most expansive state privacy law in the United States.[239] CCPA includes biometric information (facial recognition) within the definition of personal information.[240] Since then at least six state legislatures have introduced privacy laws similar to the CCPA.[241]

Finally, California lawmakers also temporarily banned facial recognition software from police body cameras with the Body Camera Accountability Act.[242] San Francisco is the first American city to ban city use of facial recognition surveillance technology,[243] and Alameda, Berkeley, Oakland, Santa Clara County, Nashville, Seattle, Somerville, and Davis have also since adopted

[235] *Id*. at 63.

[236] *Id*. at 48.

[237] *See* Jeffrey D. Neuburger, *Bipartisan Facial Recognition Privacy Bill Introduced in Congress*, NAT'L L. REV. (Mar. 26, 2019), https://www.natlawreview.com/article/bipartisan-facial-recognition-privacy-bill-introduced-congress [https://perma.cc/G7ZK-ELTF].

[238] *Id*.

[239] *See* Joseph J. Lazzarotti & Jason C. Gavejian, *State Law Developments in Consumer Privacy*, NAT'L L. REV. (Mar. 15, 2019), https://www.natlawreview.com/article/state-law-developments-consumer-privacy [https://perma.cc/KUY4-7WED].

[240] *See* Danielle Ochs, *The Latest on California's Approach to Biometrics in the Workplace*, NAT'L L. REV. (Oct. 10, 2019), https://www.natlawreview.com/article/latest-california-s-approach-to-biometrics-workplace [https://perma.cc/4MM5-F6A5].

[241] *See* Lazzarotti & Gavejian, *supra* note239.

[242] *See* Rachel Metz, *California Lawmakers Ban Facial-Recognition Software from Policy Body Cams*, CNN (Sept. 13, 2019, 8:04 AM), https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html [https://perma.cc/7LVG-WR6K]. While body cameras may initially seem like worthwhile safety and security devices, Professor Friedman urges that they are merely Band-Aids for a larger probe. More consideration reveals that body cameras are pointed at the public, and can be turned on/off at the discretion of police, and acts as a tool for police monitoring of the public. *See* FRIEDMAN, *supra* note 42, at 312-13.

[243] Dave Lee, *San Francisco is the First US City to Ban Facial Recognition*, BBC (May 15, 2019), https://www.bbc.com/news/technology-48276660 [https://perma.cc/6YFC-R43P].

strong laws governing the police acquisition and use of surveillance technologies.[244]

CONCLUSION

By tracing the development of the third-party doctrine, this Article has illustrated the problems inherent in the third-party doctrine when it was originated and as it is regularly (mis)applied in today's digital world. Simply put, the government's theoretical framework about the doctrine is wrong. A person does not "assume the risk" that his CLSI information would be shared. Similarly, a cell phone or smartphone user is not "voluntarily" transmitting his location data to a third-party. The third-party doctrine which was always anathema to the Fourth Amendment, has outlived its usefulness. There is no need to amend or modify it—it just needs to be completely abolished.

Following *Carpenter*, courts should require a warrant based on probable cause from the government before gathering real-time CSLI information and data, and using Stingrays and facial recognition surveillance technology. As an emerging body of Fourth Amendment law concerning digital privacy slowly develops in the face of hyper-fast technological advancement, the onus rests on law makers, judges, and the people, to take action in safeguarding ourselves from government overreach that threatens our privacy and civil liberties. This is the America we live in.

[244] *See*, *e.g.*, Robyn Greene, *How Cities Are Reining in Out-of-Control Policing Tech*, SLATE (May 14, 2018, 1:58 PM), https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html [perma.cc/SP6Q-UK3P]; Peter Hegarty, *East Bay City Becomes Latest to Ban Use of Facial Recognition Technology*, MERCURY NEWS (Dec. 18, 2019, 6:18 AM), https://www.mercurynews.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology/ [https://perma.cc/M5JE-SLEF]; DJ Pangburn, *Berkeley Mayor: We Passed the "Strongest" Police Surveillance Law*, FAST COMPANY (Apr. 24, 2018), https://www.fastcompany.com/40558647/berkeley-mayor-we-passed-the-strongest-police-surveillance-law [https://perma.cc/ZTU6-29RK]; Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, S.F. CHRON. (July 17, 2019, 8:33 AM), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php [https://perma.cc/982Q-DV67]; Levi Sumagaysay, *Berkeley Bans Facial Recognition*, MERCURY NEWS (Oct. 16, 2019, 11:27 AM), https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/ [https://perma.cc/X5B5-535N].