Digital Data Privacy One Year After Carpenter

By **Jonathan Cedarbaum, Nina Cahill and Sam McHale** (June 20, 2019)

Jonathan Cedarbaum

Nina Cahill

Sam McHale

A year ago, the U.S. Supreme Court issued its decision in Carpenter v. United States, holding that police acquisition of a defendant's historical cell-site location information, or CSLI, from his cellphone provider constituted a search for purposes of the Fourth Amendment.[1] In doing so, the court upended some established Fourth Amendment doctrines and raised more questions than it answered about the constitutional limits on government acquisitions of digital data.[2]

Over the past year, lower federal courts and state courts have begun to grapple with Carpenter's implications — not only for CSLI collection but also for other forms of location monitoring and digital surveillance. Despite attempts by criminal defendants to extend Carpenter to internet protocol data, internet transaction history, cell-tower dumps, pole cameras and similar surveillance cameras, and even financial records held by banks, courts have applied Carpenter almost exclusively in situations involving historical or real-time CSLI.

Carpenter characterized CSLI as having the ability to provide a "detailed, encyclopedic, and effortlessly compiled" record of "a person's physical presence" over long periods.[3] Courts have so far rejected attempts to extend Carpenter principally on the ground that other surveillance techniques rarely allow the acquirer to learn about tracked individuals' activities as extensively as CSLI acquisition does and thus raise less serious privacy concerns.

The few notable exceptions involve data that would allow the government to intrude upon the intimacies of people's lives by tracking their physical location over extended periods — as Carpenter found CSLI does. Thus, courts have found that certain uses of GPS devices, pole cameras and internet of things devices rise to the level of being Fourth Amendment searches.

Unanswered Questions About CSLI After Carpenter

Carpenter held that "accessing seven days of CSLI constitutes a Fourth Amendment search."[4] The court characterized its decision as "narrow," suggested it was not disturbing the third-party doctrine but simply refusing to extend it, and disclaimed addressing any issues other than those presented by the facts before it.[5] The court even resisted Justice Anthony Kennedy's urging to decide whether there is any limited period for which law enforcement may obtain historical CSLI free from Fourth Amendment scrutiny.[6] The court thus declined to express a view about collection of real-time CSLI or cell-tower dumps and did not address orders authorizing prospective CSLI collection.[7]

Both lower federal courts and state courts hearing suppression motions based on Carpenter have largely followed the Supreme Court's lead in reading Carpenter narrowly and applying its reasoning only in factually similar situations.

Real-Time or Prospective CSLI

Although Carpenter addressed an order seeking historical CSLI, courts have applied its principles in considering orders seeking real-time CSLI, in which police are actively tracking a suspect in the moment — often to execute a warrant on a person whose location is unknown, or to respond to an emergency situation,[8] and in considering orders authorizing prospective collection of CSLI to track a suspect's movements over a given period going forward.[9]

Quantity of CSLI Necessary to Trigger Fourth Amendment Scrutiny

While Carpenter established that seven days of CSLI is sufficient to trigger the Fourth Amendment, courts have rejected invitations to establish a bright-line rule for the inverse proposition, that is, that fewer than seven days of CSLI would not rise to the level of being a Fourth Amendment search.

In United States v. Gaskin, for example, the government responded to the defendant's objection to its warrantless collection of seven days of his historical CSLI by arguing that it sought to introduce only one day's worth of data. Although the district court ultimately resolved the defendant's challenge under the good faith exception, it expressed considerable skepticism about the government's argument that Carpenter's warrant requirement should apply only to requests for CSLI of one week or more. "Carpenter did not draw any particular bright line," the court observed, "by which a request for data covering a period shorter than seven days would not need a warrant."[10]

The Texas Court of Criminal Appeals addressed a similar question in an opinion holding that law enforcement's use of real-time CSLI to track a defendant's cellphone for three hours did not constitute a search.[11] The court reasoned that the question of whether the government conducted a search turned not on the content of cell-site location records, but on "whether the government searched or seized enough information that it violated a legitimate expectation of privacy."[12] The court concluded that the defendant lacked a legitimate expectation of privacy in three hours of information revealing his physical location under either the Fourth Amendment or the Texas Constitution.[13] The defendant has filed a petition for a writ of certiorari to the U.S. Supreme Court.[14]

Cell-Site Simulators and Cell-Tower Dumps

Courts have also held that Carpenter does not forbid the warrantless use of cell-site simulators (sometimes called stingrays) or cell-tower dumps. Cell-site simulators are devices that mimic cell towers by sending out signals causing phones in the area to transmit their locations and identifying information.[15]

As the district court in United States v. Woodson explained, whereas CSLI allows agents to use a known telephone number to compile a record of a suspect's location over an extended period, the signaling information revealed when using a cell-site simulator is typically obtained by first physically tracking a suspect's location so that agents can then use a device to obtain his previously unknown telephone number.[16]

This distinction was enough for a district judge in the U.S. District Court for the Eastern District of Missouri to declare that the manner in which the stingray was used "simply does not give rise to the same privacy and Fourth Amendment concerns articulated in Carpenter."[17] Tower dumps provide the government with records identifying information for all devices that have pinged a cell tower during a given time period.[18]

The U.S. Court of Appeals for the Seventh Circuit stated that Carpenter declined to rule that such dumps "were searches requiring warrants" and thus "did not invalidate" them.[19] The Seventh Circuit reasoned that, unlike the more extensive data available from CSLI, a single tower dump can identify only phones near one location and at one time.[20]

Carpenter's Applicability to Other Surveillance Techniques

Carpenter stated that it did not "call into question conventional surveillance techniques and tools," but instead held only that a warrant is required in the "rare case" in which a suspect has a reasonable expectation of privacy in records held by a third party.[21] Nevertheless, litigants have attempted to extend Carpenter's rationale to other surveillance tools. Courts have generally rebuffed such attempts, with a few notable exceptions where the data sought would allow the government to construct a detailed record of a person's physical movements. Thus, courts have found that certain uses of GPS devices, pole cameras and IoT devices to rise to the level of Fourth Amendment searches.

GPS Devices

Carpenter reaffirmed the court's holding in United States v. Jones that people have a reasonable expectation of privacy in their physical movements over extended periods.[22] Thus, courts have applied Carpenter to require a warrant for particularly intrusive forms of GPS surveillance.

In United States v. Diggs, for example, an officer was given log-in credentials from a car dealership to access the GPS tracking system for a car driven by a robbery suspect. The system recorded time-stamped entries detailing the car's approximate street address each time the car was turned on, every five minutes while it was being driven, and each time it was parked. Without a warrant, the officer downloaded a month's worth of the information, from which it was possible to extract information down to the level of specific latitude and longitude waypoints. The district court held that such GPS data "fits squarely within the scope of the reasonable expectation of privacy" because — like the CSLI at issue in Carpenter — it provides a "precise, comprehensive record" of the defendant's "public movements," enabling police to "travel back in time to retrace" the defendant's whereabouts.[23]

Pole Cameras

Although Carpenter expressly declined to disturb the use of "conventional surveillance techniques and tools, such as security cameras," lower courts are divided over what constitutes "conventional surveillance."[24] Courts and police often refer to security cameras as pole cameras because they are often affixed to the tops of telephone or utility poles. Property managers use them to deter and record wrongdoing in commercial spaces such as malls and parking lots, but police also install their own pole cameras to investigate criminal activity and monitor potential suspects.

At a minimum, these cameras record video, but they otherwise vary widely in technological capability: some record audio; some can be remotely controlled to tilt, pan, and zoom; and some digitize and archive video on remote servers.[25] Thus far, at least seven district courts have confronted claims seeking to exclude evidence from pole cameras. Six of those courts have denied the defendant's motion to suppress, distinguishing the "conventional surveillance" that can be done with pole cameras from the newer and more intrusive technologies at issue in Carpenter and Jones.[26]

In United States v. Tuggle, for example, the FBI installed three pole cameras on public property in the area around a suspect's home, providing a view of his driveway, the front of the residence, and the street.[27] FBI agents could remotely zoom, pan, and tilt the cameras, which had "rudimentary" lighting technology to assist the camera's operation at night.[28] The cameras allowed the FBI to view the video in real time, and the video feed was archived on a server over the course of an 18-month investigation.[29]

The Tuggle district court held that since pole cameras are "limited to a fixed location and capture only activities in camera view" and use technology that has "been around for decades," their use does not constitute a search — at least, as in Tuggle, when they are used to monitor the outside of a home that is visible to any neighbor or passerby.[30]

One district court, however, has found that the technological power of newer security cameras moves them outside the bounds of "conventional surveillance." In United States v. Moore-Bush, a federal district judge in Massachusetts extended Carpenter to cover eight months of video from a pole camera that continuously recorded, digitized, and archived footage in factually similar ways to the surveillance in Tuggle.

Noting that other courts had approved the use of pole cameras by classifying them as mere "security cameras," the judge reasoned that the pole camera used in the case before him was not a typical security camera "by any stretch of the imagination."[31] It was installed to investigate suspects, not to monitor a heavily trafficked area or commercial establishment; and it was not put in plain view and not accompanied by a warning sign to deter wrongdoers, but was hidden out of sight and used to track a suspect's travels.[32]

The court held that, while not every use of a pole camera constitutes a search, the government's use of the camera in Moore-Bush did because it allowed the government to piece together "intimate details of a suspect's life" by providing continuously recorded video for eight months, focusing on the driveway and front of the suspect's home, allowing officers to zoom in close enough to read license plate numbers, and creating a digitally searchable log.[33] The government has appealed the district court's ruling to the U.S. Court of Appeals for the First Circuit.

Internet of Things Devices

Another potential avenue for extending Carpenter is in the frequent collection and storage of data from IoT devices, such as smart meters that collect information on electricity usage. The Seventh Circuit confronted such a case in Naperville Smart Meter Awareness v. City of Naperville and held that collecting such data every 15 minutes qualifies as a search because it "reveals details about the home that would be otherwise unavailable to government officials."[34]

The court held that the third-party doctrine was not implicated because the government itself — in the form of a public utility — collected the information as part of offering electricity. But the Seventh Circuit suggested that the third-party doctrine would not apply even if a separate entity were to collect the data because "a choice to share data imposed by fiat is no choice at all."[35]

A home occupant, the court opined, no more "assumes the risk" of near constant monitoring by choosing to have electricity than a cellphone user "assumes the risk" of turning over a "comprehensive dossier of physical movements" by choosing to use a cellphone.[36] The court found the search to be reasonable because the collection was not done for purposes of criminal law enforcement and because the utility did not share the data with third

parties.[37] But the case represents the first in what will likely be many challenges over the use of data derived from the ever-increasing number of IoT devices.

Carpenter's Impact on Related Fourth Amendment Issues

So far, lower federal courts and state courts have mostly agreed that Carpenter did little to alter traditional applications of the third-party doctrine, Fourth Amendment standing doctrine or defendants' entitlement to discovery.

The Third-Party Doctrine

In its foundational third-party doctrine cases, the Supreme Court held that a person has no reasonable expectation of privacy in the person's financial records held by his or her bank[38] or in records of dialed phone numbers conveyed to the person's phone company.[39] Carpenter emphasized that its holding did "not disturb the application of" the third-party doctrine in these cases but merely declined to "extend" the doctrine to collection of CSLI.[40]

In doing so, the court stressed the "unique nature of cellphone location information"[41] and its capacity to provide an "intimate window into a person's life,"[42] leaving open the possibility that the third-party doctrine may in time yield to the rapid evolution of other technologies. Defendants have relied on Carpenter to challenge the third-party doctrine's application to internet protocol address data and subscriber information as well as to financial records, but so far without reported success.

Courts have denied motions to suppress banking records and records of financial transactions, holding that the CSLI in Carpenter is easily distinguished from such records.[43] One court, for example, emphasized that records of financial transactions do not include comprehensive records of a person's whereabouts, as in Carpenter.[44] The court took the view that people voluntarily expose their information when they choose to make financial transactions.[45] As a result, those who use banking services or even online platforms like eBay Inc. "assume[] the risk that the company would reveal to police the purchases" or transactions that are made.[46]

So too with IP address data, which may identify the general location of user's accessing of the internet. At least 12 district court cases have considered challenges to the collection of IP addresses and, thus far, none has held such collection amounted to a search. These trial courts — and the U.S. Court of Appeals for the Fifth Circuit as well — have concluded that this data fits "comfortably" within the third-party doctrine and as less revealing than CSLI.[47]

Courts have viewed such data as "voluntarily submitted" to a third-party provider and as having "no bearing on any person's day-to-day movement."[48] Courts have reasoned that IP addresses do not follow people around and do not even identify a specific user — they reveal only the location of internet access.[49] Thus, courts have generally held that IP address data generated by a user's accessing of a website or subscribing to a service is distinguishable from the CSLI at issue in Carpenter.

Courts have been similarly unwilling to re-evaluate applications of the third-party doctrine to other digital data in light of Carpenter.[50] The Colorado Supreme Court, for example, recently held that police use of a defendant's cellphone passcode to execute a search warrant did not violate the Fourth Amendment, even though the defendant gave the passcode to a police officer only for the limited purpose of allowing the officer to call the

defendant's girlfriend to retrieve his vehicle. [51]

The court rejected the defendant's argument that the third-party doctrine applied differently to cellphones in light of Carpenter, reasoning that the defendant did not retain a reasonable expectation of privacy in the phone's contents after revealing his passcode to a third-party — even though the passcode was revealed on the assumption that it would be used only for a limited purpose.[52]

Standing and Discovery

Defendants have also been unsuccessful in using Carpenter to extend the bounds of the Fourth Amendment's standing requirements or their entitlement to seek discovery from the government. Several courts have held that Carpenter did not affect the Fourth Amendment's standing requirements and so a defendant still may normally object to unreasonable searches only of his own person or property.[53]

Thus, when one defendant sought to exclude CSLI obtained from a compatriot's phone, the court held that the defendant had no reasonable expectation of privacy in CSLI collected from a phone over which he lacked "ownership, possession, control, use, and exclusion of others."[54] Nor, another court has held, did Carpenter alter the rules governing discovery, despite one defendant's attempt to argue that Carpenter entitled him to discovery to determine whether the government had been monitoring his CSLI.[55]

State Constitutions

Not all state high courts interpret state constitutional equivalents to the Fourth Amendment in parallel with the U.S. Supreme Court's interpretations of the Fourth Amendment. Defendants in state criminal prosecutions may look to state constitutions to raise issues akin to those addressed by the U.S. high court in Carpenter.

In a series of decisions in the past year, the Massachusetts Supreme Judicial Court has interpreted the Massachusetts Constitution to provide protections that in some ways exceed those provided under Carpenter. Under the state constitution, a defendant may challenge the warrantless tracking of his cellphone, even if he is not the person who regularly uses that phone;[56] police requests for service providers to "ping" a phone to ascertain its real-time location constitutes a search[57] and mandating GPS monitoring as a probation condition constitutes a search,[58] but later review of a database of location information gathered from such GPS monitoring does not.[59]

Conclusions

Thus far, courts have taken Chief Justice John Roberts at his word that Carpenter's holding is narrow. The few areas in which Carpenter has been extended involve surveillance techniques that allow the government to gain a picture of a suspect's life by compiling extensive physical location information — especially where, as in Carpenter itself — that information was not voluntarily shared or disclosed in a meaningful way. While Carpenter might not (yet) have caused the sea change that some expected, more challenges are sure to come as the varieties of digital data collected continue to expand and the technologies used to collect and analyze that data become more sophisticated.

Jonathan Cedarbaum is a partner and Nina Cahill and Sam McHale are summer associates

at WilmerHale.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[2] See generally Orin S. Kerr, Implementing Carpenter, in The Digital Fourth Amendment (forthcoming) (manuscript at 1); Susan Freiwald & Stephen William Smith, The Carpenter Chronicle: A Near-Perfect Surveillance, 132 Harv. L. Rev. 205, 206 (2018).

[3] Carpenter, 138 S. Ct. at 2216, 2220.

[4] Id. at 2217 n.3.

[5] Id. at 2220.

[6] See id. at 2217 n.3.

[7] Id. at 2220.

[8] See, e.g., United States v. Saemisch, 371 F.Supp.3d 37, 42 (D. Mass. 2019).

[9] See Chavez, 2019 WL 1003357, at *4-6 (stating that eventually historical and real-time CSLI will be treated similarly since they both implicate privacy concerns in similar ways); cf. United States v. Gibson, 2019 WL 2265370, No. 3:18-cr-033, at *3 (N.D. Ind. May 28, 2019) (assuming that probable cause standard must be met for government to obtain order for real-time CSLI over 30-day period, just as a court would for historical CSLI).

[10] See United States v. Gaskin, 2018 WL 4926331, No. 1:17-CR-00370, at *2 (N.D. Ga. Sep. 7, 2018) (report and recommendation of magistrate judge), adopted in full by United States v. Gaskin, 2018 WL 4921985, No. 1:17-CR-370, at *1 (N.D. Ga. Oct. 10, 2018).

[11] Sims v. State, 569 S.W.3d 634 (2019), petition for cert. filed (U.S. Apr. 16, 2019) (No. 18-1327).

[12] Id. at 646 (emphasis added).

[13] Id. The court further noted that although Carpenter supported the proposition that longer-term surveillance might infringe on a person's legitimate expectation of privacy if the location records reveal the privacies of his life, "this is not that case." Id.

[14] Petition for Writ of Certiorari, Sims v. Texas, No. 18-1327 (U.S. Apr. 16, 2019).

[15] United States v. Woodson, 2018 WL 7150388, No. 4:16CR541, at *5 (E.D. Mo. Nov. 21, 2018).

[16] Id. at *9. Accord Andres v. State, 254 So.3d 283 (Fla. 2018) (holding Carpenter inapplicable to police use of stingray device to locate defendant for purpose of executing a warrant).

[17] Woodson, 2018 WL 7150388 at *9.

[18] See United States v. Adkinson, 916 F.3d 605, 608 (7th Cir. 2019), petition for cert. filed (U.S. May 15, 2019) (describing tower dumps).

[19] Id. at 611.

[20] See id. But see United States v. Pendergrass, 2018 WL 7283631, No. 1:17-cr-315 at *13 (N.D. Ga. Sep. 11, 2018) (assuming "solely for the sake of argument" that Carpenter applies to tower dumps).

[21] Carpenter, 138 S. Ct. at 2220, 2222.

[22] Id. at 2217 (citing United States v. Jones, 565 U.S. 400 (2012)).

[23] United States v. Diggs, 2019 WL 2088419, No. 18-CR-185-1, at *2-3 (N.D. Ill. May 13, 2019).

[24] Carpenter, 138 S. Ct. at 2220.

[25] See United States v. Moore-Bush, 2019 WL 2341182, No. 3:18-30001 at *5 (D. Mass June 3, 2019).

[26] See United States v. Gbenedio, 2019 WL 2177943, No. 1:17-cr-430 (N.D. Ga. Mar. 29, 2019); United States v. Kay, 2018 WL 3995902, No. 17-cr-16 (E.D. Wis. Aug. 21, 2018); United States v. Kelly, 2019 WL 2137370, No. 17-cr-175 (E.D. Wis. May 16, 2019); United States v. Kubasiak, 2018 WL 6164346, No. 18-CR-120 (E.D. Wis. Aug. 23, 2018); United States v. Moore-Bush, 2019 WL 2341182, No. 3:18-30001 (D. Mass June 3, 2019); United States v. Tirado, 2018 WL 3995901, No. 16-cr-168 (E.D. Wis. Aug. 21, 2018); United States v. Tuggle, 2018 WL 3631881, No. 16-cr-20070 (C.D. Ill. July 31, 2018).

[27] United States v. Tuggle, 2018 WL 3631881, at *1.

[28] Id.

[29] Id.

[30] Id. at *2-3.

[31] United States v. Moore-Bush, 2019 WL 2341182, at *5-6.

[32] Id.

[33] Id. at *5-6, 8.

[34] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018).

[35] Id. at 527-28.

[36] Id.

[37] Id. at 527-29.

[38] United States v. Miller, 425 U.S. 435, 443 (1976).

[39] Smith v. Maryland, 442 U.S. 735, 745 (1979).

[40] Carpenter, 138 S. Ct. at 2220.

[41] Id. at 2209.

[42] Id. at 2217.

[43] See, e.g., United States v. Moiseev, 364 F.Supp.3d 23, 25 (D. Mass. 2019) (stating that the "novel circumstance" presented in Carpenter is "easily distinguished" from the records obtained from a bank via a grand jury subpoena); see also Zanders v. State, 118 N.E.3d 736 (Ind. 2019) (reasoning that Carpenter did not revoke the third-party doctrine's application to phone records); People v. Anderson, 420 P.3d 825 (Cal. 2018) (noting that Carpenter did not disturb the application of Smith v. Maryland to cellphone records of numbers dialed).

[44] United States v. Schaefer, 2019 WL 267711, No. 3:17-cr-00400, at *5 (D. Or. Jan. 17, 2019) (noting Carpenter's holding is narrow, location data is not at issue in transactional records, and users voluntary expose their information to vendors when they agree to do business on an internet platform).

[45] Id.

[46] Id.

[47] United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018). See also Brown v. Sprint Corporate Security Specialist, 2019 WL 418100, No. 17-CV-2561 (E.D.N.Y. Jan. 31, 2019); United States v. Felton, 367 F.Supp.3d 569 (W.D. La. 2019); United States v. Germain, 2019 WL 1970779, No. 2:18-cr-00026 (D. Vt. May 3, 2019); United States v. Gregory, 2018 WL 6427871, No. 8:18cr139 (D. Neb. Dec. 7, 2018); United States v. McCutchin, 2019 WL 1075544, No. CR-17-01517-001 (D. Ariz. Mar. 7, 2019); United States v. Monroe, 350 F.Supp.3d 43 (D.R.I. 2018); United States v. Popa, 369 F.Supp.3d 833 (N.D. Ohio 2019); United States v. Rosenow, 2018 WL 6064949, No. 17CR3430 (S.D. Cal. Nov. 11, 2018); United States v. Street, 363 F.Supp.3d 1212 (D.N.M. 2018); United States v. Therrien, 2019 WL 1147479, No. 2:18-cr-00085 (D. Vt. Mar. 13, 2019); United States v. Tolbert, 2019 WL 2006464, No. 14-3761 (D.N.M. May 7, 2019); United States v. Jenkins, 2019 WL 1568154, No. 1:18-cr-00181 (N.D. Ga. Apr. 11, 2019).

[48] United States v. Therrien, 2019 WL 1147479, at *2 (D. Vt. Mar. 13, 2019) (quoting Contreras, 905 F.3d at 857); see also Brown v. Sprint Corporate Security Specialist, 2019 WL 418100, at *4 (E.D.N.Y. Jan. 31, 2019) (applying the same reasoning to cellphone subscriber and billing information along with call detail records); United States v. Tolbert, 2019 WL 2006464, No. 14-3761, at *3 (D.N.M. May 7, 2019) (applying same reasoning to subscriber information associated with an IP address, including the name of the subscriber, date of subscription, method of payment, phone number associated with the subscription, and IP connection logs).

[49] See United States v. Jenkins, 2019 WL 1568154, at *4 (N.D. Ga. Apr. 11, 2019).

[50] People v. Diaz, 122 N.E.3d 61 (N.Y. 2019).

[51] People v. Davis, 438 P.3d 266 (Colo. 2019).

[52] Id.

[53] See Rakas v. Illinois, 439 U.S. 128, 133-34 (1978).

[54] United States v. Oakes, 320 F.Supp.3d 956, 961 (M.D. Tenn. 2018). See also United States v. Peters, 333 F.Supp.3d 366, 377-78 (D. Vt. 2018) (determining that tracking cell phone of another person riding in defendant's vehicle did not violate the defendant's right to privacy under Carpenter); cf. United States v. Johnson, No. 17-10129, 2019 WL 917175, at *6-7 (D. Mass. Feb. 25, 2019) (distinguishing person's expectation of privacy in his or her own CSLI despite its being automatically shared with a cell service provider from the lack of expectation of privacy in e-mails voluntarily sent or forwarded to another user and subsequently obtained from that other user).

[55] See Nyabwa v. City of Corpus Christi, 2018 WL 6984561, No. 2:18-CV-103, at *3 (S.D. Tex. Dec. 4, 2018) (noting that discovery is designed to help a party prove a claim it reasonably believes to be viable rather than to figure out if it has any basis for a claim).

[56] Commonwealth v. Fredericq, 121 N.E.3d 166 (Mass. 2019).

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

[58] Commonwealth v. Johnson, 119 N.E.3d 669 (Mass. 2019).

[59] Commonwealth v. Feliz, 119 N.E.3d 700 (Mass. 2019).