# THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

## OFFICE OF THE ATTORNEY GENERAL
### ATTORNEY GENERAL ANDREA JOY CAMPBELL

A PROJECT OF THE CRIMINAL BUREAU
DIGITAL EVIDENCE LABORATORY
APPEALS DIVISION

---

APRIL 2026

---

**A NOTE TO READERS OF THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE**

The Massachusetts Digital Evidence Guide ("Guide") is to be used only as an educational resource. This Guide is not legal advice. The purpose of this Guide is to provide the reader with an understanding of the Massachusetts statutes and cases impacting criminal investigations and prosecutions that involve technology or digital evidence. This Guide, and its provisions, are not policy. This Guide does not suggest modifying or replacing any existing agency practices or procedure(s). Readers should consult with appropriate authorities, prosecutors, or legal counsel for necessary legal advice, case or statutory interpretation, or implementation of the document for any internal use. Readers who intend to rely on cases and statutes cited in this Guide should consult with the source document, confirm the interpretation, and investigate subsequent history. Questions or comments about, or suggestions for, this Guide can be e-mailed to agodel@mass.gov.

# THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

Office of the Attorney General, Andrea Joy Campbell

# I. Investigation

## A. The Search and Seizure of Digital Evidence

As with physical evidence, searches and seizures of digital evidence must be reasonable to be valid. This section provides a summary of Fourth Amendment law as it relates to the search and seizure of digital evidence. It also references Article Fourteen of the Massachusetts Declaration of Rights, which parallels the Fourth Amendment, but is sometimes more expansive.

The Fourth Amendment states:

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

U.S. Const. amend. IV.

Article Fourteen (art. 14) of the Massachusetts Declaration of Rights is similar to the Fourth Amendment, but since 1985, the Supreme Judicial Court ("SJC") has interpreted it as providing broader protections than its federal counterpart. Commonwealth v. Upton, 394 Mass. 363, 373 (1985) ("We conclude that art. 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause.").

To determine whether law enforcement action constitutes an unreasonable search or seizure, courts ask two questions. First, was the action a search or seizure within the meaning of the Fourth Amendment? E.g., Commonwealth v. Magri, 462 Mass. 360, 366 (2012) ("In deciding whether police conduct violates the Fourth Amendment or art. 14 of the Massachusetts Declaration of Rights, we first determine whether a search, in the constitutional sense, has taken place."). Second, was that search or seizure reasonable? See, e.g., Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness." (internal quotation marks omitted)).

### 1. Was There a Search or Seizure?

"A search implicating the Fourth Amendment occurs 'when an expectation of privacy that society is prepared to consider reasonable is infringed' and a seizure of property for purposes of the Fourth Amendment occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'" Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (quoting United States v. Karo, 468 U.S. 705, 712 (1984)) (finding installation and use of a GPS tracking device on a car to be a seizure under Massachusetts art. 14 because it requires entering the vehicle and using the electricity of the defendant's car).

## a) Searches and the Reasonable Expectation of Privacy

For a search to implicate the Fourth Amendment, the defendant must have a "reasonable expectation of privacy" in the place to be searched. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); see also United States v. Heckencamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding a college student had a reasonable expectation of privacy in the contents of his personal computer because it was located in his dorm room, was protected by a password, and was not subject to regular university monitoring). A person's expectation of privacy is reasonable "if he can demonstrate a subjective expectation that his activities would be private, and he can show that his expectation was one that society is prepared to recognize as reasonable." Heckencamp, 482 F.3d at 1146 (internal quotation marks, brackets, and citations omitted). Individuals generally have a reasonable expectation of privacy in their personal computers and files. See id. at 1146–47 (listing cases to that effect). In Heckencamp, "[t]he salient question [was] whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network." Id. at 1146.

When challenging the constitutionality of a search, the defendant bears the initial burden of establishing that a search occurred. See Commonwealth v. D'Onofrio, 396 Mass. 711, 714-15 (1986); Commonwealth v. Alvarez, 480 Mass. 1017, 1018 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer).

The sections below explore the contours of the reasonable expectation of privacy, discussing: (1) standing; (2) one-party consent; (3) the third-party doctrine; (4) surveillance in public; (5) file sharing over networks; (6) data shared with others or in data that is not one's own; and (7) diminished privacy expectations in the context of probationers, parolees, and court-ordered monitoring.

### (1) Standing

The SJC abolished the standing requirement in Commonwealth v. DeJesus, 489 Mass. 292 (2022), following U.S. Supreme Court precedent, which abandoned such a requirement under the Fourth Amendment "over four decades ago." Id. at 295.

- Commonwealth v. DeJesus, 489 Mass. 292 (2022). The defendant, Christopher DeJesus, was convicted of possessing a firearm without a license and possessing a large capacity feeding device. Id. at 292-93. Police learned of the firearm through a video recording posted on social media that showed DeJesus brandishing a firearm with an extended magazine. Id. The video led police to search the basement of a multifamily dwelling that did not belong to DeJesus. Id. at 294. Police found DeJesus in the basement; they also found a firearm with an extended magazine inside an open backpack. Id. Police subsequently identified the firearm as the same one DeJesus was holding in the video. Id. DeJesus moved to suppress the firearm on the ground that it was obtained pursuant to an unlawful warrantless entry; the motion was denied. Id. The SJC ultimately upheld the denial of the motion to suppress, concluding that DeJesus did not have a reasonable expectation of privacy in the basement. Id. at 297.

  Prior to this case, Massachusetts courts had held that under Art. 14 of the Massachusetts Declaration of Rights, a challenge to a search and seizure required "both standing and a reasonable expectation of privacy." Id. at 295. Standing required the defendant to either (1) have

a possessory interest in the place searched or the property seized, or (2) be present when the search occurred. Id. In DeJesus, the SJC abolished the separate standing requirement, clarifying that a defendant need only show a reasonable expectation of privacy in the place searched. Id. at 293. In abolishing the standing requirement, the SJC followed U.S. Supreme Court precedent, which abandoned such a requirement under the Fourth Amendment "over four decades ago." Id. at 295 (citing Rakas v. Illinois, 439 U.S. 128, 139 (1978)). The SJC reasoned that the additional standing requirement "pose[d] a potential constitutional dilemma" in that it could have "lead to the untenable result that the Massachusetts Declaration of Rights [did] not protect rights guaranteed by the Federal Constitution." Id. The court specifically explained that the constitutional dilemma would most often arise in the context of electronic data, where standing can be more difficult to establish. Id. For example, if a defendant has a reasonable expectation of privacy in text messages sent through an encrypted messaging service, the defendant may have a difficult time asserting possession of the data or presence at the time the data is searched. Id. Consequently, the defendant would be unable to establish standing. Id. Based on this reasoning, the SJC abandoned the two-pronged analysis previously required under Art. 14, specifically abrogating Commonwealth v. Delgado-Rivera, 487 Mass. 551 (2021), and Commonwealth v. Williams, 453 Mass. 203 (2009).

In the absence of a standing requirement, Art. 14 now only requires the defendant "to show his or her own reasonable expectation of privacy in the place searched" when challenging a search and seizure. Id. at 296. While this requirement is normally specific to the individual, a defendant can rely on another's reasonable expectation of privacy in one, limited situation. Id. When a defendant has been charged with possessing contraband at the time of the search, and the property searched was actually possessed by a codefendant who had a reasonable expectation of privacy, the defendant may assert the same reasonable expectation of privacy as the codefendant. Id. at 296–97. Here, the defendant did not have a reasonable expectation of privacy in the basement because "the only record evidence here of a connection between the defendant and the basement [was] that the defendant was in the basement when the videos were filmed." Id. at 298 (quoting Williams, 453 Mass. at 209 ("mere presence on the property does not create a reasonable expectation of privacy")).

Prior to the SJC's 2022 decision in DeJesus, 489 Mass. 292, defendants in Massachusetts had to establish that they had standing to challenge a warrantless search or seizure when the location or item searched or seized did not belong to the challenging party. Although this requirement no longer exists, the following cases provide background on previous decisions, which have now been overturned:

- Commonwealth v. Delgado-Rivera, 487 Mass. 551 (2021). Jorge Delgado-Rivera was implicated in a narcotics operation when his co-defendant's cellular phone was acquired and searched during a stop by a police officer. Id. at 553. Delgado-Rivera's co-defendant moved to suppress all evidence seized during the traffic stop, including material from the cell phone; he argued that because the search was without a warrant and without probable cause, it was in violation of the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights. Id. at 553-54. Delgado-Rivera moved to join his co-defendant's motion and the Commonwealth objected on the grounds that he lacked standing to challenge the search. Id. at 552. The Superior Court ruled that Delgado-Rivera had standing and allowed him to join his co-defendant's motion. Id. The Supreme Judicial Court reversed on interlocutory appeal and emphasized the trend in cases towards applying a one-step inquiry focused on a reasonable

expectation of privacy, instead of the usual two-part analysis, which focuses on both standing and a reasonable expectation of privacy. Id. at 557.

The SJC identified a distinction between its traditional analysis of the constitutionality of a search under article 14—involving a standing determination followed by separate consideration of whether the defendant had a reasonable expectation of privacy—and the analysis under federal law, which merges the question of standing with the reasonable expectation of privacy inquiry. Id. at 555-56. The court recognized a trend in its recent cases toward applying the federal one-step approach and noted that its "continued adherence to the standing analysis has become strained," though it left "for another day" the decision of whether to formally abandon the two-step test. Id. at 557-59.

Applying the one-step inquiry, the SJC held that Delgado-Rivera did not have a reasonable expectation of privacy in his text messages because he relinquished control of them when he sent them to his co-defendant. Id. at 560. The court emphasized that the text messages "created a record of the communications that was readily and lastingly available to, easily understood by, and almost instantaneously disbursable by the intended recipient, as well as unintended readers, all beyond the control of the sender." Id. at 561. The fact that Delgado-Rivera intended to share the messages only with one person did not affect the result, given how easily they could be shared with others. Id. at 561-62.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully suppressed CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105, 107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Commonwealth v. Almonor, 482 Mass. 35 (2019), the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Almonor, 482 Mass. at 47-48 (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because, "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Id. at 108. The court found that the defendant did have standing to challenge the search of his own cell phone, but the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 108-09.

### (2) One Party Consent

In Massachusetts, "one party consent" does not negate a reasonable expectation of privacy of the non-consenting party. While the Supreme Court held that warrantless electronic surveillance with "one party consent" does not implicate the Fourth Amendment, United States v. White, 401 U.S. 745, 751 (1971), the SJC found such surveillance impermissible under art. 14 of the Massachusetts Declaration of Rights, Commonwealth v. Blood, 400 Mass. 61, 70 (1987). Because it found there is a reasonable expectation of privacy in conversations that occur among "a narrow compass of known listeners" in private homes, the SJC concluded that the warrantless electronic surveillance was a violation of that constitutional provision. Id. Accordingly, "one party consent" did not obviate the need for a warrant under art. 14. Id.

### (3) The Third-Party Doctrine

In United States v. Miller, 425 U.S. 435 (1976), and Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court articulated what has become known as the "third-party doctrine." Under this doctrine, "the Fourth Amendment does not prohibit the obtaining of information revealed [by a suspect] to a third party and conveyed by him to Government authorities," regardless of the suspect's expectation of how the information might be used. Miller, 425 U.S. at 443. Massachusetts has traditionally followed the Supreme Court's guidance on the third-party doctrine. See, e.g., Commonwealth v. Cote, 407 Mass. 827, 833–36 (1990) (holding that a defendant had no reasonable expectation of privacy in telephone message records held by a third-party answering service for the reasons cited in Miller).

- United States v. Jones, 565 U.S. 400 (2012). Unanimous decision holding that a Fourth Amendment "search" occurs where law enforcement places a GPS device on defendant's car. Id. at 411. The Court's opinion, authored by Justice Scalia, focused on the Government's intrusion on the defendant's physical property and applied "an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted." Id. In contrast, Justice Sotomayor's concurrence in Jones emphasized that "the Fourth Amendment is not concerned only with trespassory intrusions on property," id. at 954, and brought the issues later addressed by Carpenter v. United States, 138 S. Ct. 2206 (2018), to the forefront, see Jones, 565 U.S at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age…").

Carpenter v. United States, 138 S. Ct. 2206 (2018) and Commonwealth v. Augustine, 467 Mass. 230 (2014) modified the third-party doctrine for at least one specific type of information—cell site location information ("CSLI"). The holding of Carpenter is that law enforcement effects a Fourth Amendment "search" by obtaining at least one week's worth of a defendant's CSLI from a third-party cellular provider. See Carpenter, 138 S. Ct. 2206, 2217 n.3. The comparable holding from Augustine is that subpoenaing two weeks' of CSLI information is a "search." See Augustine, 467 Mass. 230, 233, 255 (2014).

- Carpenter v. United States, 138 S. Ct. 2206 (2018). The Government successfully applied for two court orders directing Carpenter's wireless carriers to disclose Carpenter's CSLI for select time periods within a four-month span. 138 S. Ct. at 2212. The first order sought 152 days of CSLI from MetroPCS, and the second order sought seven days of CSLI from Sprint. Id. Based in part off the information the Government acquired from Carpenter's CSLI, the Government charged Carpenter with six counts of robbery and six counts of carrying a firearm during a federal crime of violence. Id.

  The Supreme Court held that the Government's acquisition of Carpenter's CSLI was a search of Carpenter that required a warrant supported by probable cause even though the Government acquired the CSLI from third-party wireless carriers. Id. at 2221. The Court declined to apply an expansive version of the third-party doctrine to CSLI partly because the data can reveal immense amounts of intimate information about who a suspect has been associating with and where a suspect has been travelling. Id. at 2219 ("There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today."). Furthermore, because cell phones are a nearly ubiquitous part of daily life and virtually every activity on a phone generates CSLI, the Court rejected the claim that Carpenter voluntarily disclosed his CSLI to his wireless carriers. Id. at 2220 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term.").

  While the Court stated that its ruling was "a narrow one" that applied only to CSLI, id., the dissents argued that the decision will have far-reaching consequences, e.g., Carpenter, at 2234 (Kennedy, J., dissenting) ("The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties."); see also id. at 2262 (Gorsuch, J., dissenting) ("Today the Court suggests that Smith and Miller distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to 'extend' those decisions to particular classes of information, depending on their sensitivity." (emphasis in original)); cf. Commonwealth v. Augustine, 467 Mass. 230, 253 (2014) (holding that although "we do not reject categorically the third-party doctrine," some forms of electronic evidence require "a different approach"). Given Americans' increasing dependence on technological devices that generate large amounts of personal data, it is possible that the Supreme Court's reasoning in Carpenter will someday result in a larger overhaul of the third-party doctrine.

- Commonwealth v. Lepage, 494 Mass. 67 (2024). Police obtained the call detail records for the defendant's cell phone without a warrant. Id. at 71-72. The SJC reiterated that individuals do not have a reasonable expectation of privacy in their call detail records. Id. at 76. The court noted that "[d]espite the narrowing of the third-party doctrine in other contexts, it remains applicable to call detail records. Notwithstanding recent technological changes, the phone numbers an individual dials are still conveyed voluntarily to a phone service provider, and providers still maintain those records for legitimate business purposes." Id. at 77. Additionally, the court concluded that the Federal Stored Communications Act (SCA) does not create a reasonable expectation of privacy in

call detail records under the Fourth Amendment or article 14 of the Declaration of Rights. Id. at 77-78. That is because a person "assumes the risk that the information will be conveyed by the service provider to the Government when he or she volunteers this information to the provider." Id. at 78 (quotation marks omitted).

- Commonwealth v. Perry, 489 Mass. 436 (2022). The police and the FBI were investigating six different robberies committed on six different dates in September and October of 2018. In addition, on October 6, 2018, a store clerk was shot and killed during an attempted robbery. Id. at 440. Each of these crimes "was perpetrated in a comparable manner by a man fitting a similar description." Id. Based on witness testimony and surveillance footage, investigators also believed that the robber had been assisted by a coventurer, acting as a getaway driver. Id. at 441. To identify the robber and his coventurer, the police and the FBI obtained cell site location information ("CSLI") for all devices that connected to specific cell towers during a particular time frame corresponding to the six robberies as well as the one attempted robbery that resulted in a homicide. Id. at 437. This information is known as a "tower dump." A tower dump "provides officers with CSLI from every device that connected to a particular cell site within a specified period[,] allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time." Id. at 440. The FBI obtained a search warrant for tower dumps corresponding to the dates for four of the robberies ("first warrant"). Id. at 441. Boston police obtained a search warrant for tower dumps corresponding to the two other robberies and the attempted robbery and homicide ("second warrant"). Id. The execution of the search warrants produced information on over 50,000 unique telephone numbers. Id. at 442. After cross-referencing these numbers, the investigators were able to identify the defendant and the coventurer. Id.

  To determine whether the investigators' collection of data from the seven tower dumps was a search under the Fourth Amendment and article 14, the SJC applied the "mosaic theory." Id. at 444. Under this theory, courts ask "whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life." Id. at 445 (quoting Commonwealth v. Mora, 485 Mass. 360, 373 (2020)). Here, the tower dumps spanned "seven different days over the course of slightly more than one month; each tower dump was limited in time to the period immediately before and after the specific robbery for which the CSLI was sought." Id. at 451. More specifically, each tower dump included CSLI data for "a forty-minute period around the time of each incident." Id. at 441. The Commonwealth argued that the government's actions should not be considered a search because the seven tower dumps only produced three hours of CSLI in total. To support this argument, the Commonwealth relied on Commonwealth v. Estabrook, 472 Mass. 852, 858 (2015), where the SJC found that collecting six continuous hours of location information did not intrude on a person's reasonable expectation of privacy because the six-hour time period was too brief. Id. at 452. The SJC disagreed, holding that the Estabrook exception did not apply to this case: the analysis of small increments of location information over several separate days "reveals a pattern of activity, which implicates comparatively greater privacy interests" than a six-hour period in one day. Id. at 453.

- Commonwealth v. Gumkowski, 487 Mass. 314 (2021). On appeal from a conviction for first-degree murder, the defendant argued that "his cell site location information (CSLI) and any 'fruits' derived from it should have been suppressed" (id. at 315) because it was obtained from Sprint, the victim's phone service provider pursuant to the exigent circumstances provision of the Stored Communications Act (SCA), 18 U.S.C. § 2702(c)(4), without a warrant. Id. at 318-19. Although the law enforcement officers request for CSLI records was under the voluntary disclosure provision of the 18 U.S.C §2702, the court held that by making a request to the service provider, the officer had instigated a search. Id. at 321. The government's request for information was State action subject to the protections of art. 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution. Id. at 321. Accordingly, the officer's request for more than six hours of CSLI data from the service provider without a warrant infringed on the defendant's reasonable expectation of privacy in his CSLI, [and] the CSLI should have been suppressed.". Id. at 321.

  The court next asked, as it does when the defendant moves to suppress CSLI before trial, whether the admission of CLSI was "harmless beyond a reasonable doubt." Id. at 321-22. The court's review for harmlessness in these circumstances is based on several factors, including: "[1] the importance of the evidence in the prosecution's case; [2] the relationship between the evidence and the premise of the defense; [3] who introduced the issue at trial; [4] the frequency of the reference; [5] whether the erroneously admitted evidence was merely cumulative of properly admitted evidence; [6] the availability or effect of curative instructions; and [7] the weight or quantum of evidence of guilt." Id. at 322 (quotations and citations omitted). The introduction of improperly obtained evidence is harmless if, based on the above factors and the record as a whole, the court is "satisfied beyond a reasonable doubt that the tainted evidence did not have an effect on the jury and did not contribute to the jury's verdicts." Id. In this case, the introduction of CSLI was harmless because (1) "it was cumulative of other evidence" (id.); (2) "the prosecutor did not mention the CSLI with any frequency" (id. at 322-23); and (3) "other evidence of guilt was substantial" (id. at 323).

  The court also held that call logs requested at the same time as the CSLI were not derived from the CSLI and were thus not fruits of the CSLI. Id. at 323-24. In addition, evidence obtained during the defendant's arrest was not fruit of the CSLI because evidence other than the CSLI originally made the defendant a suspect and the CSLI was merely "cumulative and corroborative" of other evidence. Id. at 324-325. Finally, the police found the defendant and arrested him using "traditional investigative technique" rather than CSLI. Id.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case, similar to Commonwealth v. Hobbs, 482 Mass. 538 (2019) (summarized below), considering retroactive application of Augustine's warrant requirement for CSLI data, the SJC again held constitutional a pre-Augustine CSLI request because the associated 18 U.S.C. § 2703 application satisfied the requisite probable cause standard. Id. at 166-72.

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). In 2011, the government received historical CSLI from defendant's cell service provider pursuant to a 18 U.S.C. § 2703 order, without a warrant — well before 2014, when Augustine first articulated the warrant requirement for historical CSLI requests. Id. at 542-44. The SJC held that the government could "still satisfy the warrant requirement if it can establish that its 'application for the § 2703[] order met the requisite probable cause standard of art. 14,'" i.e., the same probable cause standard required of an affidavit in support of a search warrant for historical CSLI. Id. at 544 (quoting Augustine, 467 Mass. at 256). (This also comports with Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016), an earlier case considering retroactive application of Augustine to CSLI data obtained pre-Augustine pursuant to an 18 U.S.C. § 2703 order.)

- Commonwealth v. Almonor, 482 Mass. 35 (2019). This case concerned an issue of first impression involving whether police action that causes an individual's cell phone to transmit its real-time location information violates any reasonable expectation of privacy. Id. at 41. Neither the Supreme Court's decision in Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018) nor the SJC's decision in Commonwealth v. Augustine, 467 Mass. 230, 4 N.E.3d 846 (2014) addressed this precise issue. The Commonwealth charged the defendant with murder after he shot and killed an individual and subsequently fled the scene of the crime. After a witness gave them the defendant's phone number, the police filed a "mandatory information for exigent circumstance requests" form with the telephone service provider. The telephone service provider "pinged" the defendant's phone and revealed the defendant's GPS coordinates to the police. Id. at 38-39. The court granted the defendant's motion to suppress the warrantless "pinging." Id. The SJC reversed, holding that the warrantless pinging of the defendant's phone constituted a search under the Article 14 of the Massachusetts constitution, but that the warrantless search was justified by exigent circumstances, namely that the defendant was at large and believed to be armed and dangerous. It noted that searches occur when the government intrudes on a person's reasonable expectation of privacy and concluded that the defendant had a reasonable expectation of privacy in his cellular location data. Id. at 43-44. The court held that real-time location data serves as a "proxy for the real-time location of the individual" because "cell phones are an indispensable part of daily life and exist as almost permanent attachments to their users' bodies." Id. at 45 (internal quotations omitted).

- Commonwealth v. Fulgiam, 477 Mass. 20 (2017). In Fulgiam, the Commonwealth obtained recent text messages of the defendant pursuant to § 2703(a) of the Federal Stored Communications Act. Id. at 28; 18 U.S.C. § 2703(a) (2012). The court held, on federal statutory and state constitutional grounds, that law enforcement required a warrant to obtain the text messages. See 477 Mass. at 31. An individual under Massachusetts state law has a "reasonable expectation of privacy in his text messages." Id. at 33. The third-party doctrine did not require otherwise because "the nature of cellular telephone technology . . . [and] use in our current society render the third-party doctrine inapposite" in this context. Id. at 34.

- Commonwealth v. Estabrook, 472 Mass. 852 (2015). The SJC considered a request for CSLI and concluded that a defendant's reasonable expectation of privacy under art. 14 of the Massachusetts

Declaration of Rights is not violated by a warrantless request for production of up to six (6) hours of historical CSLI. Id. at 854. It also established that the relevant consideration in determining the reasonable expectation of privacy is the length of time for which CSLI data is requested, not the time span ultimately sought to be introduced at trial. Id. at 858–59.

- Commonwealth v. Augustine, 467 Mass. 230 (2014). Police investigating a murder obtained the defendant's CSLI from his service provider pursuant to a 18 U.S.C. § 2703(d) order. Id. at 233. These orders are not warrants, so they cannot be used to effectuate a search for information protected by the Fourth Amendment or art. 14. The CSLI obtained helped police determine the defendant's location over the period they were investigating. See id. at 233–34. The court considered but ultimately rejected the Commonwealth's argument that the third-party doctrine negated any reasonable expectation of privacy the defendant had in his CSLI. Id. at 241–56. It reasoned that art. 14 does not protect information voluntarily and intentionally transmitted to third parties (like the number dialed to initiate a call) but it does protect information incidentally transmitted (like the location information the cell phone provider acquires as a result of cell phone technology). Id. at 249–52. The court found that the defendant therefore had a reasonable expectation of privacy in his CSLI, which, under art. 14, means that "the government must obtain a search warrant to obtain it." Id. at 252.

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). Law enforcement obtained thousands of emails related to fraudulent marketing claims from the defendant's Internet Service Provider (ISP). Id. at 281. The defendant challenged such access to his email on Fourth Amendment grounds. Id. at 282. The Sixth Circuit agreed and held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" Id. at 288 (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)). In finding that a reasonable expectation of privacy existed in this case, the Sixth Circuit analogized email transmitted via ISP to the contents of telephone conversations and closed letters, each of which received Fourth Amendment protection. See id. at 286–87. Rebutting the third-party doctrine argument, the Sixth Circuit—similar to the SJC in Augustine above—noted that the ISP in this case was an *intermediary* rather than the intended target of a conversation. Id. at 288. Thus, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." Id. Though binding only in the Sixth Circuit, this case has been cited by some of the largest email providers in requiring warrants to obtain the contents of email. See Brendan Sasso, *Facebook, email providers say they require warrants for private data seizures*, The Hill (Jan. 25, 2013), http://thehill.com/policy/technology/279441-facebook-email-providers-require-warrant-for-private-data. The Department of Justice also requires its prosecutors nationwide to follow this holding.

#### (4) Surveillance in Public: Public View Principle, Mosaic Theory, and More

Under the "public view" principle, individuals generally do not have a reasonable expectation of privacy in items or places that they expose to the public. California v. Ciraolo, 476 U.S. 207, 213 (1986)

("[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares"). In particular, "the government, without… a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance." Augustine, 467 Mass. at 252. (Note that this principle as stated in Augustine is in some tension with the SJC's decision in Mora, as discussed below.)

Courts have limited the public view principle in "constitutionally sensitive" settings (epitomized by the home) where individuals have a strong expectation of privacy that society is prepared to recognize, especially where technology has enabled previously infeasible collection of information about the inside of a home via surveillance technology situated outside the home (i.e., in public). See Kyllo v. United States, 533 U.S. 27 (2001) (holding warrantless surveillance of heat levels inside a home using thermal-imaging equipment outside the home to be an unconstitutional search).

Recent developments suggest that courts are increasingly recognizing constitutional warrant requirements in more situations involving surveillance in public places, when such surveillance is particularly expansive and detailed, or implicates "constitutionally sensitive" domains such as the home. The SJC has recognized the "mosaic theory" or "aggregation principle for the technological surveillance of public conduct," under which "'the cumulative nature of… information collected [when collected over a long enough period] implicates a privacy interest on the part of the individual who is the target of the tracking,'" even when the individual activities or data points surveilled would not enjoy constitutional protection taken alone. Commonwealth v. McCarthy, 484 Mass.493, 503-04 (2020)(quoting Augustine, 467 Mass. at 253); see also Jones, 565 U.S. at 416 (Sotomayor, J., concurring).

- Commonwealth v. McCarthy, 484 Mass. 493 (2020). The court considered the constitutionality of warrantless use of automatic license plate readers (ALPRs), which are "cameras combined with software that allows them to identify and 'read' license plates on passing vehicles." Id. at 494. Drawing on the "mosaic theory," the SJC stated that "[a] detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts," and noted that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." Id. at 504, 506. On the facts of the case, however, the SJC found no constitutional violation: "[T]he analysis should focus, ultimately, on the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance [at issue]. … [F]or this case, we consider the constitutional import of four cameras placed at two fixed locations… [and] conclude that the limited use of ALPRs in this case does not constitute a search within the meaning of either art. 14 or the Fourth Amendment." Id. at 506, 508,509.

Pole camera surveillance is a notable area where courts' approaches in applying the "public view" principle have been shifting recently, especially after Carpenter, 138 S. Ct. 2206, and Jones, 565 U.S. 400. While "[m]ost courts to have addressed pole camera surveillance have concluded that it does not infringe on any reasonable expectation of privacy" under the "public view" principle, "several courts have reassessed prolonged pole camera surveillance." Commonwealth v. Mora, 485 Mass. 360, 364-65 (2020)

(citing as examples United States v. Vargas, No. CR-13-6025 (E.D. Wash. Dec. 15, 2014) (six weeks of pole camera surveillance was search); State v. Jones, 2017 S.D. 59 (2017) (two months was search); People v. Tafoya, 2019 COA 176 (Colo. App. 2019) (three months was search)). Mora is the most recent Massachusetts case on pole camera surveillance.

- Commonwealth v. Comenzo, 489 Mass. 155 (2022). In a child pornography investigation, the police used a pole camera to determine which of three apartments in a multi-family building was occupied by the defendant. Id. at 157-58. After police used information gleaned from the pole camera to obtain a search warrant for the defendant's apartment, the defendant moved to suppress the evidence found during the search on the basis that the use of the pole camera was a warrantless, unconstitutional search. Id. at 156-57. Relying on Commonwealth v. Mora, 485 Mass. 360 (2020), the SJC held that the targeted, long-term pole camera surveillance was a search in the constitutional sense. Id. at 159-60. The SJC then turned to whether there was probable cause to support that search. Id. It held that the following facts provided probable cause for the pole-camera surveillance: (1) there was "probable cause that a crime had been committed by the defendant[,]" and (2) use of the pole camera "would lead to additional evidence of the crime, including, but not limited to, determining the defendant's unit number so that they could apply for a search warrant." Id. at 160-61. As such, the use of the pole camera was a lawful search. Id. at 161.

- Commonwealth v. Henley, 488 Mass. 95 (2021). In an appeal from a conviction for murder, the defendant argued that the trial court erred in failing to suppress data obtained from a warrantless search of the defendant's CharlieCard. Id. at 97. The MBTA records each time a CharlieCard is used to board a bus or train and electronically stores such data for fourteen months. Id. at 106. In this case, the Boston police used data from the defendant's CharlieCard to uncover his travel history on the day of the murder and to gather surveillance video footage from MBTA stations showing the defendant wearing clothing matching the suspect's description. Id. at 111.

  The SJC rejected the Commonwealth's argument that the third-party doctrine justified a warrantless search of the defendant's CharlieCard. Id. at 107. The SJC reasoned that a typical CharlieCard user does not knowingly transmit data to a third party or purchase a CharlieCard with the expectation of sharing information about their location with the MBTA. Id. Nevertheless, the SJC upheld the narrow warrantless search applying the mosaic theory. "The mosaic theory requires that [courts] consider the governmental action as a whole and evaluate the collected data when aggregated." Id. at 109. "Whether the aggregation of data collected by police implicates the mosaic theory depends on how much data police retrieved and the time period involved." Id. at 110. In applying the mosaic theory in this case, the court relied on several cases, including Commonwealth v. Estabrook, 472 Mass. 852, 858 (2015) (holding that a warrantless search of up to six hours of cell phone location data does not violate a defendant's reasonable expectation of privacy); and Commonwealth v. Mora, 485 Mass. 360, 370 (2020) (holding that "limited pole camera surveillance of [the defendants] away from their homes did not collect aggregate data about the defendants over an extended period"). Id. at 112-13. The SJC found that the limited search of MBTA data for a two-day period did not implicate the defendant's constitutionally

protected expectation of privacy because the CharlieCard only tracks when an individual enters the MBTA system, not the whole of their public movements, and because surveillance cameras are visible everywhere a CharlieCard transaction can occur. Id. at 113.

- Commonwealth v. Mora, 485 Mass. 360 (2020). Investigators installed pole cameras on public telephone and electric poles for the purpose of surveilling the defendants. Id. at 361. Most of the cameras were aimed at the homes of defendants or other individuals; one was aimed at a street that a defendant used to conduct his drug business. Id. at 362. The cameras had video but not audio recording capabilities, they could not view inside any residence, and they did not have infrared or night vision capabilities; however, investigators could remotely zoom and angle the cameras in real time. Id. The footage was stored in a searchable format that allowed officers to review previously-recorded events. Id. The SJC held that the pole camera surveillance of the defendants' homes was a warrantless search in violation of Article 14 of the Massachusetts Constitution. Id. at 370-76. Pole camera surveillance of public streets frequented by the defendants away from their homes was not subject to a warrant requirement, however, as defendants had no reasonable expectation of privacy in those locations. Id. at 369. The defendants' homes did not have fencing or other attempts to shield the residences from view, a fact that the court held immaterial to the constitutionality of surveillance. Id. at 366-67. The court noted that the Fourth Amendment might well require the same outcome, but declined to reach the federal constitutional question as the case could be resolved on state constitutional grounds. Id. at 361.

### (5) Whether an Activity Implicates the Wiretap Statute

This section discusses cases in which the courts have considered whether certain activity undertaken without a warrant, like an audio-visual recording obtained by law enforcement, had to be suppressed under the Massachusetts wiretap statute, G.L. c. 272, § 99.

- Commonwealth v. Du, 495 Mass. 103 (2024). The Commonwealth appealed the allowance of the defendant's motion to suppress an audio-visual recording. The Supreme Judicial Court suppressed the whole surreptitious audio-visual recording as a violation of G. L. c. 272, § 99. Where an unlawfully intercepted communication is an audio-visual recording showing one of the parties to the communication, the Wiretap Act's suppression remedy extends to the recording in its entirety, including the video footage. G. L. c. 272, § 99. The Court held that the whole video is content under the statute for two reasons. First, the footage shows the speakers and therefore contains information concerning the identity of a party to the communication. Second, the footage depicted the person engaging in the unlawfully intercepted communication and therefore contained "information concerning … the existence… of that communication." 495 Mass. at 107. Thus, under the statute's plain language, suppression of the whole video's "contents" is required.

- Vita v. New England Baptist Hosp., 494 Mass. 824 (2024). The plaintiff, Vita, alleged that defendant hospitals violated the Massachusetts Wiretap Act ("Act") by collecting and sharing her browsing activities on the hospitals' websites. Id. at 825. Vita alleged that the hospitals intercepted and shared her communications with third-party advertisers without her consent. Id. at

825. Vita did not allege "that private patient records or messages to nurses, doctors, or other healthcare providers were intercepted." Id. at 825.

The Massachusetts Wiretap Act, G. L. c. 272, § 99, prohibits the unauthorized interception of wire and oral communications, unless otherwise excepted by the Act (which exceptions are not at issue here). The Act does not define "communication." Id. at 826. On direct appellate review, the Supreme Judicial Court held that the Legislature did not "intend[] 'communication' to extend so broadly as to criminalize the interception of web browsing and other such interactions." Id. at 826. The SJC noted that when the statute was enacted, "wiretaps involved the interception of person-to-person conversations and messages using hidden electronic surveillance devices[.]" Id. at 826. Moreover, the SJC, citing Commonwealth v. Rainey, 491 Mass. 632, 645 (2023), reiterated that the Legislature's chief concern in enacting the Act was electronic eavesdropping and wiretapping. Here, "Vita's allegations do not claim the interception of person-to-person conversations or messaging of the kind clearly within the [Act's] ambit." Id. at 826. Accordingly, the SJC applied the rule of lenity and reversed the Superior Court's denial of the hospitals' motions to dismiss. Id. at 826-27.

Considering the legality, or even advisability, of the hospitals' alleged conduct more broadly, however, the SJC stated the following in dicta:

> Make no mistake, the hospitals' alleged conduct here raises serious concerns, and may indeed violate various other statutes and give rise to common-law causes of action more specifically directed at the improper handling of confidential information, particularly confidential medical information. And we do not in any way minimize the serious threat to privacy presented by the proliferation of third-party tracking of an individual's website browsing activity for advertising purposes. These concerns, however, should be addressed to the Legislature.

Id. at 827.

- Commonwealth v. Rainey, 491 Mass. 632 (2023). While on probation, the defendant forcibly entered his then girlfriend's home and assaulted her. Id. at 633. Responding to a domestic disturbance call, two police officers arrived at the victim's residence, and one of the officers activated his body-worn camera before entering. Id. at 633. As the victim reported the assault to the officers, one officer recorded her statement in writing while the officer, who was equipped with the body-worn camera, was able to capture audio-visual video footage of the victim's report, the state of her home within his plain view, and his own interview of the victim's two daughters. Id. at 633. The defendant was not recorded. Id. at 633. At the final surrender hearing, the body-worn camera footage was admitted into evidence and relied on by the judge in revoking the defendant's probation. Id. at 636.

  On appeal, the defendant argued that the wiretap statute, G. L. c. 272, § 99, precluded the use of the body-worn camera footage at his probation violation proceeding and that the recording violated the Fourth Amendment and art. 14. Id. at 633. The SJC held that the wiretap statute did

not preclude the use of the body-worn camera footage and that the defendant's rights were not violated. Id. at 633. First, the SJC noted that the exclusionary rule does not apply to probation violation proceedings. Id. at 638 (citing Commonwealth v. Vincente, 405 Mass. 278, 280 (1989)). Next, the SJC determined that the wiretap statute provides specific remedies, none of which applied to the defendant's situation. Id. at 638. The SJC concluded that the defendant's reliance on the wiretap statute in connection with a probation violation proceeding was "at best questionable." Id. at 639. Relying on a literal interpretation of the wiretap statute, the defendant argued that the camera-wearing police officer, prosecutor, probation officer, and Superior Court judge were all subject to criminal penalties. Id. at 640-41. The SJC rejected this argument, concluding that neither the statute's text nor its legislative history supported the defendant's statutory construction. Id. at 643-44. First, turning to the text of the statute, the SJC held that "nothing in the wiretap statute as a whole, including its codified preamble, evinces an intent to prohibit recording a victim's volunteered report of a crime where, as here, the victim was aware that officers already were memorializing her report in writing, much less an intent to criminalize the use of such a recording at a probation violation proceeding." Id. at 643. Next, addressing the legislative history of the statute, the SJC found that "the Legislature did not appear to have in mind law enforcement officers' use of devices to record a crime victim's voluntary reporting of a crime under circumstances where, as here, the victim understood her statement was being preserved by them." Id. at 646-47. With respect to the defendant's constitutional claims, the SJC cited Commonwealth v. Yusuf, 488 Mass. 379, 390 (2021), for the proposition that body-worn camera footage capturing items "in the plain view of the officer" does not constitute "a search in the constitutional sense." Id. at 647. Finally, the SJC affirmed the trial judge's ruling that the recorded statements were substantially reliable hearsay and held that the judge did not err in relying on the video footage. Id. at 648.

### (6) Peer-to-Peer and Other Network File Sharing

The following cases illustrate when making data accessible to the public or certain networks via peer-to-peer file sharing techniques eliminates one's reasonable expectation of privacy.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Defendant was an instructor at a high school's electronics shop. Police officers remotely observed pirated movies and child pornography in an open share folder of a computer named Joester7437, which was connected to the school's network. Id. at 103–05. [Note: Joester7437 was later determined to belong to a student. Id. at 105.] While searching the school for Joester7437, the police found a computer/server named "Nightcrawler." Id. at 105. Nightcrawler's screen displayed an open share folder with the same pirated movie as was found on Joester7437. Id. "The source of the open share was Sinister, another unauthorized computer logged onto the high school's network." Id. The police found Sinister in the defendant's office, but that computer was password protected. Id. They seized Sinister "on probable cause to believe that it contained child pornography and copyrighted intellectual property." Id. They then received a search warrant for it based on an affidavit alleging: (1) both shared folders (in Joester7437 and Sinister) had a copy of the same pirated movie, (2) Joester7437's open share folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 111. The defendant

did not dispute that he had no reasonable expectation of privacy in files shared with the network. Id. at 107. Instead, the defendant argued that he did have a reasonable expectation of privacy in his *private* files and that there was no probable cause to search the private files for child pornography. Id. The court held that the affidavit in support of the search warrant did not establish probable cause to believe that child pornography was located in the private files on the defendant's computer (Sinister). Id. at 111. The SJC noted: "None of these facts, even when considered together, provided a 'substantial basis' to believe that the defendant's private files contained child pornography." Id.

- Commonwealth v. Hay, 90 Mass. App. Ct. 1122 (2016) (unpublished). Defendant argued that the pre-warrant investigation was a "search" within the Fourth Amendment because the P2P [peer-to-peer] network was open only to a small group of known individuals, id. at *6, and because law enforcement used specialized SHA technology to identify a file on the defendant's computer that was likely to contain child pornography, id. at *7 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001) (government's use of device not in general public use "to explore details of the home that would previously have been unknowable without physical intrusion" is a search)). The appeals court held that, though it is possible that a file-sharing network open only to a small group of known individuals might give rise to a reasonable expectation of privacy in the files, the defendant had not argued or shown that the network in question here (Gnutella), as used with the specific software client used by the defendant (LimeWire), was such a network. Id. at *7. The appeals court also held the investigation was not a search because the defendant offered no evidence that the SHA technology enabled law enforcement to learn any more about the files than could any other P2P user. Id.

- United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010). Defendant shared child pornography over a peer-to-peer file sharing network that was being monitored by police using special forensic software. Id. at 1046–47. Police remotely downloaded the incriminating files from the defendant's folder on the peer-to-peer network. Id. at 1047. The Ninth Circuit held the defendant had no reasonable expectation of privacy in files that anyone who had access to the network could download. See id. at 1048. The court ruled this way notwithstanding the defendant's attempts to keep the files private because even though his subjective intent demonstrated a desire for privacy, it would be objectively unreasonable to uphold an expectation of privacy "in the face of such widespread public access." Id. The court also rejected the defendant's argument that the special forensic software used by investigators constituted a search. It cited several other cases supporting the proposition that special tools could be used to access already-public information, like the files in this case, because public information enjoys no Fourth Amendment protections. See id. at 1048.

- United States v. King, 509 F.3d 1338 (11th Cir. 2007). Defendant had child pornography on a personal computer connected to a military base network. Id. at 1339. His "files were 'shared' over the entire base network," id. at 1342, and an airman searching the network remotely downloaded those files, id. at 1340–41. The defendant took several steps—ultimately unsuccessful—that he believed shielded his hard drive from access by others. Id. at 1341. Even though the defendant

manifested a subjective expectation of privacy by attempting to secure the files, id., the court found that his failure to actually secure the files rendered that expectation objectively unreasonable, id. at 1342. In reaching this conclusion, the court analogized to a prior case holding that a defendant had no objectively reasonable expectation of privacy in the unsecured common area of a multi-unit apartment building. Id. In both cases, the fact of public access rendered any subjective expectation of privacy objectively unreasonable. Id.

- United States v. Ladeau, No. 09–40021–FDS, 2010 WL 1427523 (D. Mass. April 7, 2010). Defendant shared child pornography over a secured peer-to-peer network that allowed him to select who could download his files. Id. at *1. He allowed downloads by a private user who then turned his account over to the Royal Canadian Mounted Police. Id. The court held that even though the defendant manifested a subjective expectation of privacy through his actions, this expectation was not objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at *4. "No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access." Id. So, "[o]nce Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable." Id. at *5.

- United States v. Thomas, Nos. 5:12–cr–37, 5:12–cr–44, 5:12–cr–97, 2013 WL 6000484 (D. Vt. Nov. 8, 2013). Defendants in this case shared child pornography over peer-to-peer networks. Id. at *17. Police found the defendants by using automated scanning tools designed to detect child pornography shared on peer-to-peer networks. Id. After a lengthy explanation of file sharing, hash values, and investigative software and testing tools, id. at *2–6, the court held that the defendants had no reasonable expectation of privacy in files they shared publicly on a peer-to-peer network, id. at *19–20. In making this ruling, the court relied on United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010), along with other circuit cases. Id. at *19. The defendants argued against the inclusion of partially downloaded files in the evidence used against them, saying they would not have shared those files once the download was complete, but the court rejected this argument because those files were nonetheless being shared when the police searched and were therefore publicly accessible. Id. at *17. [Note: This case contains clear and thorough explanations of peer-to-peer networks, hash values, and TLO's CPS suite of tools.]

#### (7) Data Shared with Others or Data that Is Not One's Own

The following case addresses claims of a reasonable expectation of privacy in data shared with other through a post on a social network:

- Commonwealth v. Carrasquillo, 489 Mass. 107 (2022). Using an undercover account and a pseudonym, a police officer sent a friend request to the defendant's private Snapchat account. Id. at 110. The defendant accepted the friend request and thereby allowed the officer to view incriminating evidence the defendant was sharing. Id. at 111. The defendant moved to suppress the Snapchat evidence the police officer viewed, arguing that he had a reasonable expectation of privacy in the data he posted and shared with his "friends." Id. The SJC held that the officer's actions did not amount to a search in the constitutional sense, because the defendant had neither a

subjective nor an objective expectation of privacy. Id. at 120. The SJC determined that the defendant did not have a subjective expectation of privacy because he was unaware of his privacy settings. Id. at 119-20. The defendant did not have an objective expectation of privacy because the defendant's Snapchat stories could be viewed by approximately one hundred of his "friends." Id. at 122-23. The number of people who could view what the defendant shared was not necessarily dispositive of the question of a reasonable expectation of privacy, however, because, in the view of the SJC, a categorical application of the third-party doctrine to information shared electronically is ill-suited to the digital age. Id. at 123-24. But, in this case, the defendant did not have a reasonable expectation of privacy in what he had posted to Snapchat because he had allowed individuals he did not know, including an undercover officer, to view what he had posted. Id. at 125-26.

The following cases address claims of a reasonable expectation of privacy in data that, in some sense, is not the movant's.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105,107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Almonor, the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Commonwealth v. Almonor, 482 Mass. 35, 47-48 (2019) (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Lugo, 482 Mass. at 108. During the investigation, police became concerned that a second juvenile involved in the murder-robbery might be in danger, and contacted that individual's cell phone service provider, obtaining location data, and the names and numbers from recent calls. Id. at 106. Among these was the defendant's phone number, which police also "pinged," showing that he was at his residence with the second juvenile. Id. Police obtained a search warrant for the residence and "discovered evidence linking the defendant to the killing, including the murder weapon." Id. The SJC pointed out that, even if there had been no standing issue, the circumstances of police investigating a homicide and concerned for the cell phone user's safety would have rendered the defendant's challenge futile under the emergency aid exception. Id. at 108. The court also held that, while the defendant had standing to challenge the search of his own cell phone, the information gathered from that search—the location of his

residence—had already been gathered by other means, so no evidence came from the search. Id. at 109.

- Commonwealth v. Bryant, 447 Mass. 494 (2006). Law enforcement seized the "main file server" of a law firm pursuant to a warrant. See Commonwealth's Brief, 2005 WL 4062684, at *10 (Dec. 2005). The defendant, an employee of the firm, moved to suppress files he had worked on. See Bryant, 447 Mass. at 495. Denying the motion to suppress, the Supreme Judicial Court held that the defendant did not have a "reasonable expectation of privacy" in the firm's files and therefore did "not establish[] that he ha[d] standing to challenge the seizure of the files." See id. at 497.

### (8) Probationers, Parolees, and Court-Ordered Monitoring

Probationers subject to court-ordered monitoring have a diminished expectation of privacy.

- Commonwealth v. Roderick, 490 Mass. 669 (2022). Applying the balancing test described in Commonwealth v. Feliz, 481 Mass. 689 (2019), the SJC held that the Commonwealth failed to establish that "its interest in imposing GPS monitoring outweigh[ed] the privacy intrusion occasioned by the monitoring." Roderick, 490 Mass. at 670. GPS monitoring constitutes a search under both Article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution. Id. at 672. When such monitoring occurs without a warrant, it is both "presumptively unreasonable" and "presumptively unconstitutional." Id. (quoting Commonwealth v. Norman, 484 Mass. 330, 335 (2020)). That presumption can be overcome only when the government's interests outweigh the invasion of privacy. Id. (citing Feliz, 481 Mass. at 700). Here, as in Feliz, GPS monitoring "works a significant intrusion on a probationer's existing, albeit diminished, expectation of privacy." Id. at 675. Against that intrusion, the Commonwealth asserted three interests: (1) enforcing a court-ordered exclusion zone around the victim's home; (2) deterring the defendant from engaging in future criminal behavior; and (3) assisting the government in investigating any future criminal behavior. Id. at 670. The SJC rejected the first asserted interest and held that the second and third did not outweigh the invasion of privacy.

  As to the first interest, the SJC held that because—at the time of the hearing on the motion to vacate the condition of probation—the government did not know the location of the victim's residence, the trial court lacked evidence to support a finding that GPS monitoring would satisfy this interest. Id. at 678. The SJC left open the possibility that a properly configured exclusion zone *could* justify the burden that GPS monitoring imposes. Id. at 677. On the second and third interests (deterring and investigating future criminal behavior), the SJC held that the probationer's classification as a level two sex offender constituted the type of "individualized determination" sufficient to established that the defendant posed a risk of reoffending. Id. at 681. Given this risk of recidivism, the Commonwealth established that GPS monitoring would further its interest in deterring and investigating future sex offenses, id.; an interest that is particularly strong for a serious crime like rape, id. at 682. But the degree of the intrusion on the probationer's privacy occasioned by three years of mandatory GPS monitoring outweighed that interest for two complementary reasons. Id. at 683. First, in three years of monitoring, the government would be able to "store a staggering quantity of data" impossible to collect by other means, representing a

significant intrusion on the probationer's privacy interests. Id. Second, the probationer had successfully complied with the conditions of pre-trial release for nineteen months (including nine months of GPS monitoring) and displayed no individualized risks of recidivism other than his sex-offender classification. Id. at 682–83 (noting that "[t]he government has less of an interest in monitoring a potential recidivist than a proven one"). The same logic applied to the third interest (investigating future criminal behavior), which also hinged on the risk of recidivism. Id. Accordingly, the SJC ordered the lower court to modify the terms of the defendant's probation to eliminate GPS monitoring.

- Commonwealth v. Feliz, 481 Mass. 689 (2019) (decided on the same day as Commonwealth v. Johnson, 481 Mass. 710 (2019), infra). The SJC held that Mass. Gen. Laws ch. 256, § 47, which mandates GPS monitoring as a condition of probation in connection with most sex offense convictions, is "overinclusive" because "GPS monitoring will not necessarily constitute a reasonable search for all individuals convicted of a qualifying sex offense." Id. at *1; Mass. Gen. Laws ch. 256, § 47 (2018). The court held that, under Article 14 of the Massachusetts Declaration of Rights, an individualized determination of reasonableness is required for any search that is "more than minimally invasive," and "GPS monitoring is not a minimally invasive search." 2019 WL at *7. Thus, a judge must "conduct a balancing test that weighs the Commonwealth's need to impose GPS monitoring against the privacy invasion occasioned by such monitoring." Id. at *1. Whether the monitoring is determined to be reasonable "depends on a constellation of factors," and "no one factor will be dispositive in every case." Id. at *8. The fact that a probationer accedes to a contract of probation that requires GPS monitoring or signs a GPS equipment contract does not constitute consent that waives the probationer's Article 14 rights. Id. at *8. With respect to Mr. Feliz, the SJC held that "the Commonwealth's particularized reasons for imposing GPS monitoring . . . do not outweigh the privacy intrusion occasioned by the requirement of GPS monitoring." Id. at *8; accord id. at *10–13. In support of that conclusion, the court noted that the defendant "was convicted of noncontact sex offenses," and that the Commonwealth "ha[d] not presented evidence sufficient to indicate that th[e] defendant pose[d] a threat of reoffending or otherwise violating the terms of his probation." Id. at *10.

- Commonwealth v. Johnson, 481 Mass. 710 (2019) (decided on the same day as Commonwealth v. Feliz, supra). At defendant's trial for breaking and entering and larceny, the Commonwealth introduced GPS location data recorded from a GPS monitoring device that the defendant was wearing as a condition of probation. Id. at *1. The historical GPS data had been retrieved and reviewed without a warrant after the defendant's probation was completed. Id. at *2–3, *6. Defendant argued that the trial court erred in admitting the GPS location data at trial. Id. at *3. The SJC held that (1) the original imposition of GPS monitoring as a condition of defendant's probation was a search, but it was reasonable "in light of the defendant's extensive criminal history and willingness to recidivate while on probation"; and (2) no subsequent search occurred because, "once the GPS device was attached to the defendant, he did not possess a reasonable expectation of privacy in data targeted by police to determine his whereabouts at the times and locations of suspected criminal activity that occurred during the probationary period." Id. at *1. The SJC noted that the police had conducted a narrow analysis to determine whether the

defendant was present at times and places where crimes had been committed, and that a broader "indiscriminate rummaging" through months of GPS data "might raise different, more difficult constitutional questions about objective expectations of privacy, even for a probationer subjected to GPS monitoring." Id. at *10.

- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017). Police investigating a robbery "mapped" the location of a defendant wearing a GPS monitoring device while out on bail for a domestic violence offense. See id. at 298. This process revealed that the defendant was near the scene of the robbery at the time of the break-in. See id. The Commonwealth introduced the GPS evidence at trial and the defendant was convicted. Id. at 296–97. The Massachusetts Appeals Court affirmed, rejecting defendant's argument that he—subject to court ordered monitoring—retained a reasonable expectation of privacy in his movements and thus was subject to a Fourth Amendment "search". See id. at 306.

Parolees have a diminished expectation of privacy—lower even than that of probationers—both under the Fourth Amendment, Samson v. California, 547 U.S. 843, 850 (2006), and under art. 14, Commonwealth v. Moore, 473 Mass. 481, 485 (2016). In Moore, the SJC determined that, "at least with respect to a search of the parolee's home," the reasonable suspicion standard associated with stop and frisk is the appropriate standard for a warrantless search. Id. at 487. Reasonable suspicion for the search of the home was supplied here by an anonymous tip that the parolee was dealing drugs, coupled with evidence of the parolee's conduct consistent with that tip in light of the parole officer's experience with narcotics and with other parolees. Id. at 490.

### b) Seizures and Interference with Possessory Interest

Police actions reaching an individual's property constitute a seizure when "there is some meaningful interference with an individual's possessory interests in that property." Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (internal quotation marks omitted). As Justice Stevens noted in Texas v. Brown, 460 U.S. 730 (1983), "a seizure is usually preceded by a search, but when a container is involved the converse is often true . . . for example, the seizure of a locked suitcase does not necessarily compromise the secrecy of its contents . . . ." Id. at 747–48 (Stevens, J., concurring). Relying on ample precedent from other courts, the Supreme Judicial Court has found the entire computer analogous to such a closed container for seizure purposes. See Commonwealth v. McDermott, 448 Mass. 750, 766 (2007) (agreeing with lower-court "judge's analogy to closed containers with respect to the seizure of the computers and disks"). Whether a seizure has occurred is usually obvious and rarely contested. The following cases concern less-common circumstances.

- Berger v. New York, 388 U.S. 41 (1967). The Court held that wiretaps "seize" conversations in violation of the Fourth Amendment. Id. at 59. The Court did not expand further on how it came to this conclusion, but this case is often cited for the proposition that intangibles (e.g., data) can be seized in the constitutional sense. See, e.g., LeClair v. Hart, 800 F.2d 692, 695 (7th Cir. 1986) ("Following Berger, it has been clear that the Fourth Amendment embraces more than just the

forced physical removal of tangible objects . . . . Indeed, Berger stands for the proposition that the government may seize intangible items, such as the information contained in the financial documents which the IRS agents copied.").

- Commonwealth v. Connolly, 454 Mass. 808 (2009). As part of an investigation of a suspected drug dealer, police installed a GPS tracking device in his car. Id. at 10. To install the device, police opened the car's engine compartment, placed the tracking device inside, and attached it to the car's battery. See id. at 812. The Supreme Judicial Court held that installing the GPS device was a seizure within the context of art. 14 of the Massachusetts Declaration of Rights. Id. at 822. First, the installation and presence of the tracker constituted a physical intrusion on the defendant's property. Id. Second, the government's use of the vehicle to obtain information was itself an interference with the defendant's interest in it. Id. at 823 ("It is a seizure not by virtue of the technology employed, but because the police use private property (the vehicle) to obtain information for their own purposes.").

- United States v. Hicks, 438 F. App'x 216 (4th Cir. 2011). Defendant destroyed his hard drive after he found out he was under investigation for possession of child pornography. Id. at 18. After he was convicted of destroying records in a federal investigation, the defendant attacked his conviction on constitutional grounds. Id. One of these challenges was that by criminalizing his destruction of his hard drive, the government had interfered with his possessory interest in that hard drive, effectively seizing it in violation of the Fourth Amendment. Id. at 219. The Fourth Circuit found that there was no meaningful interference with the defendant's possessory interest because he did not have a property right in images of child pornography. Id. (citing Helton v. Hunt, 330 F.3d 242, 247 (4th Cir. 2003), for the proposition that there is no property right in contraband).

The case summarized below discusses the return of unlawfully seized property:

- Commonwealth v. Salmons, 96 Mass. App. Ct. 61 (2019). The defendant pled guilty to assault and battery by means of a dangerous weapon, intimidating a witness, strangulation, and other charges. The police had seized the defendant's three cell phones at the time of arrest, but the seizure was subsequently found unlawful based on the SJC's decision in Commonwealth v. White, 475 Mass. 583 (2016) (probable cause to seize or search a cell phone requires "information establishing the existence of particularized evidence likely to be found there," id. at 593). Salmons, 96 Mass. App. Ct. at 62. The defendant filed a motion for the return of his cell phones, which was granted. Id. at 62. Eight months later, the Commonwealth moved to wipe the content of two of the phones before returning them, because they contained "numerous and sexually explicit photographs and videos of the defendant and [the victim]." Id. The motion to wipe these phones was allowed, id. at 65, but the Appeals Court reversed. Relying on Commonwealth v. Sacco, 401 Mass. 204 (1987), the court found that "when, as here, property is unlawfully seized without a warrant, cannot be used as evidence, and is not unlawful to possess, it should be returned, upon proper motion, to its undisputed owner or the owner's representative." Salmons, 96 Mass. App. Ct. at 68. There was no factual finding that harm to

the victim would occur unless the phones were wiped. Id. at 69. Further, the Commonwealth's reliance on Beldotti v. Commonwealth, 41 Mass. App. Ct. 185 (1997) was misplaced because the public interest standard of G.L. c. 276, § 3 did not apply to property seized unlawfully and because the "connection between the crime and the property here [was] far more attenuated than in [Beldotti]." Id. at 69-70.

### c) Private Party Searches

#### (1) Initial Search Made by Private Party

"[W]hen the state conducts a search in response to information that a private party obtained and communicated to the government, 'the legality of the governmental search must be tested by the scope of the antecedent private search.'" Commonwealth v. Cormier, 28 Mass. L. Rptr. 489, at *4 (Mass. Super. Ct. 2011) (quoting United States v. Jacobsen, 466 U.S. 109, 116 (1984)). Where the government searches something in which a private party has already eroded a suspect's expectation of privacy, the Fourth Amendment is not implicated. Id. (citing Jacobsen, 466 U.S. at 116). Crucially, police examination of materials "initially discovered and viewed by a private party" can be more thorough than that private party's examination and still fall within the scope of the private party search. Id. at *5 (citing Commonwealth v. Raboin, 24 Mass. L. Rptr. 278, 282–83 (Mass. Super. Ct. 2008)). A more detailed analysis of Commonwealth v. Cormier below demonstrates how the private party search doctrine applies to digital evidence cases.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. at *2. Police found more child pornography at the defendant's house, and he was later charged with possession. Id. The trial judge denied defendant's motion to suppress because the warrantless search conducted by police was within the scope of the preceding private party search. Id. at *4–6. Because the computer technician had previously viewed files from the hard drive, the court found that the defendant's expectation of privacy "had already been eroded," so the subsequent police search did not implicate the Fourth Amendment. Id. at *5.

#### (2) Warrantless Search: Private Citizen or State Actor

If the intent of a private party conducting a search is not independent of the government's intent, however, the private party becomes an agent of the government, implicating the Fourth Amendment and art. 14. See Commonwealth v. Leone, 386 Mass. 329, 333 (1982). A party becomes a state actor if the police do anything to "solicit, provoke, or tempt" that party into obtaining evidence for them. Commonwealth v. Brandwein, 435 Mass. 623, 631 (2002). The cases below examine the state actor issue in the digital evidence context.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. The court found that the data recovery shop employee was not acting as a state agent because he was a private party not acting under the authority of the state. Id. at *4 (citing Commonwealth v. Leone, 386 Mass. 329, 333 (1982), for the proposition that "[e]vidence discovered and seized by private parties is admissible without regard to the methods used, unless State officials have instigated or participated in the search"). The court noted that the employee "made the decision to open the suspicious files . . . as a private citizen, while trying to repair the hard drive at [defendant's] request." Id. The court also found that authorities "did not know that [the defendant] asked [the employee] to repair his hard drive and did not instruct [the employee] to inspect the files." Id. They did nothing "to 'solicit, provoke, or tempt' [the employee] into viewing the files," so he was not a state actor. Id. (quoting Brandwein, 435 Mass. at 631).

- United States v. Lichtenberger, 19 F. Supp. 3d 753 (N.D. Ohio 2014). A private party called police after discovering child pornography on a computer, and the responding officer instructed that individual to boot up the laptop, enter the password, show the images, and gather other devices belonging to the defendant before seeking a warrant. Id. at 754–55. The court found these actions violated the Fourth Amendment because by giving instructions and directing the private party's actions, the police officer made that private party into a government agent. Id. at 758–59. The court therefore suppressed the evidence as having been collected in violation of the Fourth Amendment. Id. at 760.

#### (3) An ISP's Reporting Obligation Does Not Make it a State Agent

The reporting requirement of 18 U.S.C. §§ 2258A(a) and 2258B(a)—requiring an Internet service provider (ISP) to report any child pornography that it discovers—does not transform an ISP into a government agent when it chooses, voluntarily, to scan files sent on its network for child pornography. United States v. Stevenson, 727 F.3d 826, 829–30 (8th Cir. 2013).

### 2. Was a Search or Seizure Reasonable?

"The ordinary rule is that to be reasonable under the [Fourth] Amendment a search [or seizure] must be authorized by warrant issued by a magistrate upon a showing of probable cause." Almeida-Sanchez v. United States, 413 U.S. 266, 287 (1973); see also United States v. Carpenter, 138 S. Ct. 2206, 2221 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.") (quoting Riley, 134 S. Ct. at 2482). This section will lay out the requirements of a valid warrant in the cybercrime context and then highlight some applicable exceptions to the warrant requirement. Then, at the end of the section, there is a discussion of digital evidence cases in the context

of Commonwealth v. Long, 485 Mass. 711 (2020), which permits the suppression of the fruits of otherwise lawful searches or seizures if the search or seizure was the result of selective enforcement.

### a) Warrants

"The Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights require that a warrant be issued only on probable cause, supported by oath or affirmation." Commonwealth v. Nelson, 460 Mass. 564, 568 (2011). Massachusetts law specifically "require[s] an affidavit and an oath." Id. (citing G.L. c. 276, §§ 1 and 2B). A neutral magistrate must issue the warrant, see Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971), and it must be particular as to the items to be seized and places to be searched, see Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Warrants must contain information that has not been rendered stale, see United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (to evaluate staleness, courts "must assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information"). Officers may hold a seized item for a relatively short period of time while obtaining a search warrant, but the delay in obtaining a warrant may not be unreasonable. Commonwealth v. White, 475 Mass. 583, 593 (2016). In addition, officers must execute warrants in a timely fashion, see Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 329–30 (2014) ("[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event no later than seven days from the date of issuance thereof." (quoting Mass. Gen. Laws c. 276, § 3A)). Warrants must be executed in a reasonable manner. Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). Finally, executing officers must have the signed warrant with them when commencing the search. The sections below focus on probable cause, particularity, staleness, delay in obtaining a warrant, timely execution, and the manner of executing warrants in the digital evidence context.

#### (1) Probable Cause / Affidavit

"Under the Fourth Amendment and art. 14, probable cause requires a substantial basis for concluding that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues." Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009) (internal quotation marks and citations omitted) (detailed below). Further:

> The affidavit need not convince the magistrate beyond a reasonable doubt but must provide a substantial basis for concluding that evidence connected to the crime will be found on the specified premises. Moreover, affidavits for search warrants should be interpreted in a commonsense and realistic fashion and read as a whole, not parsed, severed, and subjected to hypercritical analysis. All reasonable inferences which may be drawn from the information in the affidavit may also be considered as to whether probable cause has been established.

Commonwealth v. Donahue, 430 Mass. 710, 712 (2000) (internal quotation marks and citations omitted).

In order to establish probable cause, law enforcement officials must typically submit an affidavit to a magistrate. That magistrate's probable cause determination is confined to the "four corners" of the affidavit. Commonwealth v. Anthony, 451 Mass. 59, 68 (2008) (detailed below). Probable cause by definition deals with "probabilities," which "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Id. (internal quotation marks and citations omitted). The following cases address probable cause and affidavits in the digital evidence context.

- Commonwealth v. Carleton, 497 Mass. 11 (2026). The defendant was convicted of first-degree murder and possession of a firearm without a license. Id. at 12. At the time of the murder, which was a drive-by shooting, security footage from both the scene of the crime and the parking lot where the defendant drove directly after the shooting showed the defendant wearing a distinctive green t-shirt with an orange and white "Airmax" logo. Id. at 13–14. After the shooting, police found a Facebook account with the defendant's first and last name. Id. at 14. The account featured a "selfie" photograph of the defendant wearing a green t-shirt with an orange and white Airmax logo with the caption "Just me my blunt n my thoughts," and it was posted less than two hours before the shooting. Id. at 14. At trial, the Commonwealth's evidence included four photographs and their associated metadata from a cell phone that had been found next to where the defendant had been sleeping in his home at the time of his arrest, including the same selfie from the Facebook account. Id. at 26. After the cell phone was seized, the police obtained a search warrant to search the phone for photographs, specifically, the Facebook selfie. Id. at 27.

  On appeal, the defendant argued that "photographs and associated metadata obtained from a cell phone seized from his home should have been suppressed because there was no probable cause to believe there was a nexus between the cell phone and the crimes and because the search of the cell phone was unreasonably delayed and exceeded the scope of a warrant obtained after the cell phone was seized." Id. at 12. The SJC held that there was probable cause to believe that there was a sufficient nexus between the cell phone and the crimes because the police "ha[d] information establishing the existence of particularized evidence likely to be found there." Id. at 26, citing Commonwealth v. White, 475 Mass. 583, 590–91 (2016). Specifically, it was permissible for the police to infer that the Facebook photograph was posted by the defendant given that the name of the Facebook account included the defendant's first and last name and the photograph's caption was in the first person. Carleton, 497 Mass. at 26. Given that (1) "cell phones are routinely used to take selfies" and that (2) "the close proximity of the cell phone to the defendant as he slept tied the defendant to it … there was ample evidence to establish that particularized evidence—namely, the selfie photograph of the defendant wearing the Airmax T-shirt—would be contained in the cell phone located next to the defendant while he slept." Id. at 26–27.

- Commonwealth v. Dunn, 494 Mass. 42 (2024). Police received a report from the National Center for Missing and Exploited Children (NCMEC) concerning potential child pornography. Id. at 44. NCMEC is a nonprofit organization dedicated to, among other goals, protecting children from sexual exploitation. Id. at 44. NCMEC created the CyberTipline, a national platform for tips regarding child sexual exploitation. Id. at 44. The report was received through the CyberTipline

and then shared with the Internet Crimes against Children (ICAC) task force of the State Police. Id. at 44. The report contained two flagged images that allegedly depicted "a pubescent minor in any image of lascivious exhibition depicting nudity." Id. at 44. The images were then analyzed utilizing a tool comparing hash values calculated from suspected child pornography with values previously marked as being submitted to NCMEC's child recognition and identification system. Id. at 45. A subpoena to Comcast for the subscriber information linked to the Internet protocol (IP) address in the CyberTipline report identified the defendant as the subscriber for the designated IP address and his place of residence as the service address. When cross-referenced with the CyberTipline report, the IP address from the subpoena is the same IP address listed for the two images reported. Id. at 46. This information was included in the application for a search warrant for any computers, cell phones, or other digital devices located at the defendant's residence. Id. at 46.

The defendant argued that only using descriptions of the two images did not establish probable cause for the search. Id. at 47. The defendant also asked the Court to institute a new rule requiring magistrates to view allegedly lewd images before making a probable cause determination. Id. The court denied both claims, holding that the description of the photos along with the CyberTipline report, hash search results, and the electronic service provider employee's observations gave sufficient information to find probable cause without viewing the photos. Id. at 53; see id. at 43 ("Although attaching the photographs or providing a more thorough description would have been preferable in this case, the affidavit read in its entirety was sufficient to establish probable cause."). The court noted that whether a description of images will suffice for purposes of probable cause will depend on the nature of the subject matter and surrounding circumstances. Id. at 55.

- Commonwealth v. Janvier, 104 Mass. App. Ct. 93 (2024). In an interlocutory appeal, the Massachusetts Appeals Court addressed "whether the search warrant applications established probable cause to believe that the defendant owned or was using [two mobile] phone numbers and [a mobile] phone during the eighteen-day period in which he was suspected of committing a series of crimes." Id. at 94. Because of the attachment that the average person has to their cell phone, a magistrate or judge may reasonably "infer that the location data from a particular phone will yield the suspect's location at any given time." Id. at 99. It was uncontested that the warrant affidavits provided probable cause to believe that the defendant committed the crimes. Id. at 99. "As it can generally be inferred that people keep the same mobile phone number for extended periods of time to maintain contact with family, friends, and business associates," the court "readily infer[red] that the defendant had been using [one of the numbers] for at least twelve days . . . ." Id. at 102. "As with the [first] number, it is reasonable to infer that the defendant did not just happen to activate the [second] number on the day he was arrested; therefore, the affidavit provided probable cause to believe that he had been using the [second] number at least for some time prior to" the day he was arrested. Id. at 103. Thus, the court determined that the affidavits provided probable cause to believe that the location information associated with either phone number would be reasonably likely "to provide evidence of the defendant's whereabouts during the relevant time period." Id. at 104, 105. The court noted that, "[f]or the purposes of this case,

[it] need not determine the outer limit of the likely duration of use of any given mobile phone number." Id. at 103.

- Commonwealth v. Hayes, 102 Mass. App. Ct. 455 (2023). The defendant was convicted of multiple counts of trafficking of persons for sexual servitude in violation of G. L. c. 265, § 50(a); deriving support from prostitution in violation of G. L. c. 272, § 7; keeping a house of ill fame in violation of G. L. c. 272, § 24; and money laundering in violation of G. L. c. 267A, § 2. Id. at 456 n.2. During the investigation, the police obtained a warrant to search the defendant's cell phone. Id. at 458. On appeal, the defendant argued that the information provided in support of the search warrant application was inadequate to establish a nexus between the alleged crimes and his cell phone. Id. at 456-57. The Appeals Court held that "the warrant application furnished probable cause to search the defendant's cell phone." Id. at 464. The court concluded that "[t]he defendant's communications with [an accomplice], in conjunction with the central role that cell phones play in commercial sex operations and the pair's reliance on [website] advertisements to conduct their business, provided probable cause to search the defendant's cell phone." Id.

- Commonwealth v. Perry, 489 Mass. 436 (2022). The police and the FBI were investigating six different robberies committed on six different dates in September and October of 2018. In addition, on October 6, 2018, a store clerk was shot and killed during an attempted robbery. Id. at 440. Each of these crimes "was perpetrated in a comparable manner by a man fitting a similar description." Id. Based on witness testimony and surveillance footage, investigators also believed that the robber had been assisted by a coventurer, acting as a getaway driver. Id. at 441. To identify the robber and his coventurer, the police and the FBI obtained cell site location information ("CSLI") for all devices that connected to specific cell towers during a particular time frame corresponding to the six robberies as well as the one attempted robbery that resulted in a homicide. Id. at 437. This information is known as a "tower dump." A tower dump "provides officers with CSLI from every device that connected to a particular cell site within a specified period[,] allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time." Id. at 440. The FBI obtained a search warrant for tower dumps corresponding to the dates for four of the robberies ("first warrant"). Id. at 441. Boston police obtained a search warrant for tower dumps corresponding to the two other robberies and the attempted robbery and homicide ("second warrant"). Id. The execution of the search warrants produced information on over 50,000 unique telephone numbers. Id. at 442. After cross-referencing these numbers, the investigators were able to identify the defendant and the co-venturer. Id.

  The defendant moved to suppress any evidence resulting from the search, arguing that the FBI and the police lacked probable cause for the warrant. Id. at 454. Specifically, the defendant alleged that the warrants did not demonstrate a nexus between the criminal activity and the CSLI to be searched. Id. The SJC held that the second warrant (obtained by the Boston police) was supported by sufficient probable cause, but the first warrant (obtained by the FBI) was not. Id. at 456-58. According to the court, "the nexus requirement is satisfied as long as there is a substantial basis to conclude that the defendant used his or her cellular telephone during the relevant time

frame, such that there is probable cause to believe the sought after CSLI will produce evidence of the crime." Id. at 455. The second warrant satisfied this requirement by providing a number of significant details: (1) it described notable similarities between the offenses to establish "a substantial basis to believe that the same individual had committed all of the offenses," id. at 456 (citations omitted); (2) it described evidence showing that a coventurer had been involved as a getaway driver, id.; (3) it "described facts suggesting some reason to believe that the defendant and a coventurer had communicated with one another from a distance, either prior to or after the commission of the offense," id.; (4) because there was reason to believe that the defendant and the coventurer communicated around the time of the crimes, "there also was probable cause to believe that either the perpetrator's telephone or the coventurer's telephone would have produced telephone call CSLI that would appear in the requested tower dumps." Id. The first warrant, by contrast, did not provide "particularized information" suggesting that the defendant and the coventurer used cell phones in the commission of the crimes. The general statement in the warrant affidavit that it is common for people to have a cell phone with them was insufficient to establish probable cause. Id.

- Commonwealth v. Lavin, 101 Mass. App. Ct. 278 (2022). In an armed home invasion investigation in which the defendant and a co-defendant were suspects, the police obtained search warrants for their CSLI. Id. at 299-300. The Appeals Court found that the warrants were properly issued. The supporting affidavits gave a detailed description of the home invasion and the evidence linking the defendants to the crime. Id. The court noted that "probable cause to obtain CSLI is created by 'an affidavit establishing that a suspect committed a crime and that the suspect was known to own or use a particular cell phone, along with the reasonable inferences drawn therefrom.'" Id. at 299 (quoting Hobbs, 482 Mass. at 547). Here, the affidavits included detailed descriptions of the home invasion and the evidence linking defendants Lavin and Desiderio to the crime. For example, "[w]hen searching Lavin's residence, officers recovered jewelry matching the description of the jewelry stolen during the home invasion, a handgun matching the description of the one used during it, and numerous other items linking Lavin to it." Id. at 299. Further, the affidavit explained that the home invasion "was a complex and carefully planned endeavor." Id. In addition, Lavin's mother provided the police with his phone number, so the police knew that he owned or used that particular phone. Id. As to co-defendant Desiderio, the evidence linking Lavin to the crime, "combined with Desiderio's motive to rob the victim, his knowledge of the victim's home and belongings, and the fact that a getaway vehicle was waiting for the intruders, provided probable cause to obtain Desiderio's CSLI." Id. at 300.

- Commonwealth v. Lowery, 487 Mass. 851 (2021). The defendant was convicted of trafficking of persons for sexual servitude in violation of G. L. c. 265, § 50(a). During the investigation, the police obtained warrants to search the phone of a sex worker ("Jane") and five phones belonging to the defendant. Id. at 854-55. At trial, the defendant moved to suppress evidence obtained from the phones, arguing that there was insufficient nexus between the crime of human trafficking and the phones. Id. at 856. The SJC found that the motion to suppress was properly denied. The court concluded that "the averments in the warrant affidavit support[ed] the inference that Jane was communicating with the defendant while she was in the hotel room with [the undercover officer],

which in turn support[ed] a finding of probable cause to search the cell phones for evidence of sex trafficking." Id. at 859. The following facts supported the nexus between Jane's phone and the sex trafficking offense: Jane's phone was used to set up a commercial sexual transaction with the undercover officer; she generally used the phone to respond to clients; the police saw Jane speak with the undercover officer on her phone; the undercover officer saw Jane use her phone to correspond with the defendant; and there was a reasonable inference that Jane had used her phone's GPS to locate the hotel to meet with the undercover officer. Id. at 857-58. As to the defendant's five phones, the warrant affidavit stated that after Jane had received payment, she had immediately sent one or more text messages and had received a message that prompted her to commence the commercial sexual act. Id. at 858. Further, as part of an inventory search of the defendant's vehicle, the police found a business card with the defendant's phone number that stated that the company was "hiring new talent escort/strippers," and that "MAKING MONEY SHOULD BE FUN & EASY." Id. Moreover, the police found condoms of the same brand that Jane had in her possession, personal lubricants, and women's undergarments in the defendant's car. Id. These facts supported a finding of probable cause to search the defendant's cell phones for evidence of sex trafficking. Id. at 859.

- Commonwealth v. Louis, 487 Mass. 759 (2021). The defendant was convicted of murder in the first degree on the theory of felony-murder, unlawful possession of a firearm, and attempted armed robbery. Id. at 759–60. On appeal, he argued that his CSLI and text messages were improperly admitted at trial. Id. at 760. The SJC disagreed, finding that the search warrant affidavit for the text messages and historical CSLI data included sufficient information to establish probable cause for the search. As to the text messages, the court found that the affidavit "established the requisite nexus between the robbery and the defendant's telephone communications." Id. at 764. The following facts supported this finding: (1) the victim had received texts from one of the coventurers on the night of the crime; (2) another coventurer was heard talking on a cell phone with someone about bringing a gun; (3) the coventurers "picked up the defendant, who was identified elsewhere in the affidavit as the person who brought the gun and shot the victim"; (4) the coventurers communicated with each other using their cell phones; and (5) each of the attempted armed robberies were preceded by calls between at least one coventurer and the intended victim. Id. at 764. The court also found that there was probable cause to access the defendant's CSLI data. Id. at 765. The affidavit provided sufficient detail to establish that "the defendant was present at and a part of the planned robberies and subsequent shooting, that he owned the cell phone subject to the desired search, and that he communicated with another robbery suspect via cell phone on the date of the murder." Id. The court further noted that this would be a sufficient foundation for probable cause to access the location information even if the defendant had not been using his phone. Id.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone.

Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. The warrant affidavit "provided a substantial basis to conclude both that the defendant had committed the homicide [with a] coventurer and that it was reasonable to expect that his cell phone would contain evidence related to that specific crime." Id. at 587. Here, unlike in Commonwealth v. White, 475 Mass. 583 (2016), there was specific evidence of a nexus between the crime and the defendant's cell phone. Id. at 589. This evidence included the following facts: "the defendant made a cell phone call soon after the shooting to the person who rented the car used in the murder, there [was] a reasonable inference that the crime was preplanned, and there [were] records of threatening cell phone communications between [the defendant's [coventurer] and the victim." Id.

- Commonwealth v. Vasquez, 482 Mass. 850 (2019). The defendant was indicted on charges of murder in the first degree and two related firearms offenses. He moved to suppress witnesses' identification of him from surveillance footage, his statements to the police, as well as evidence obtained from the search of his phone and the CSLI. Id. at 851. The SJC found that the witness identification did not require suppression. But the SJC agreed with the trial court's finding that the Miranda warnings were rendered in Spanish "in such a fragmented and confusing manner so as to be incoherent." Id. at 862. More specifically, the improper translation rendered the warnings "inadequate to apprise the defendant of his rights, and [ ] the defendant's limited comprehension of English did not suffice to compensate for these deficiencies." Id. at 852. Because the Miranda warnings were insufficient and the search of the defendant's cell phone arose from the statements the defendant made after the defective warnings, the search was not sufficiently attenuated from the unwarned statements. Id. at 865. Further, without the tainted information from the unwarned statements (such as the defendant's disclosure of his phone number), the Commonwealth failed to establish "the requisite nexus between the commission of [the] crime and the CSLI for the defendant's device." Id. at 867. The Commonwealth also failed to establish a connection between the crime and the thirty-two days for which it sought CSLI. Id. In sum, the search warrant affidavit did not "support a determination of probable cause, and the CSLI obtained as a result must be suppressed." Id. at 868. The SJC remarked in a footnote, however, that CSLI evidence may be admissible later, if the Commonwealth could show by a preponderance of the evidence that there was an untainted source for the nexus between the crime and CSLI. Id. at 868 n. 27 (quoting Commonwealth v. Estabrook, 472 Mass. 852, 865 (2015)).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). Following conviction for first-degree murder, the defendant argued on appeal, among other things, that the motion judge erred in denying his pre-trial motion to suppress cell site location information (CSLI) that was introduced as evidence during his trial. Id. at 539. The defendant's brother had identified the defendant as the man leaving the crime scene in video footage, and provided police with a phone number he claimed belonged to the defendant. Id. at 541. Police then requested a court order requiring the service provider to produce CSLI from the cell phone for several months surrounding the day of the crime. Id. at 541. The CSLI placed the owner of the cell phone in the general vicinity of the crime at the time of the killing. Id. The court ruled that, although it was a close call, the police affidavit in support of a search warrant for historical CSLI satisfied the requirement that "there be a

substantial basis to believe that the sought-after CSLI 'will produce evidence of [the] offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed . . . such offense.'" Id. at 545-46 (quoting Commonwealth v. Augustine, 472 Mass. 448, 453 (2015)). The court rejected the defendant's assertion that the police must demonstrate that the cell phone was used or possessed during the commission of a crime in order to show nexus between "the crime . . . the items sought, and the location to be searched." Id. at 546. This is not necessary because "[c]ell phones physically accompany their users everywhere such that tracking a cell phone results in near perfect surveillance of its user." Id. at 547 (quoting Commonwealth v. Almonor, 482 Mass. 35, 45 (2019) (internal quotation marks omitted)). The defendant's brother's statement that the cell phone belonged to the defendant, together with subsequent corroboration by the defendant's former girlfriend, was enough to establish the requisite nexus. Id. at 548-49.

- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019). The indictments in this case alleged that the defendant and two co-conspirators broke into the defendant's uncle's home and beat him on the head and face with a crowbar. Id. at 618. The defendant was charged with home invasion, assault, and multiple other offenses. Id. at 618, n. 1. She moved to suppress the fruits of a search of her cell phone. The Superior Court allowed the motion, but the Appeals Court reversed, finding that the police had probable cause to seize the phone, and that the defendant voluntarily consented to an unlimited search of her phone. There was probable cause to seize the cell phone because the defendant told the police it contained videos that "could establish where, when, and with whom the defendant was in the hours before the home invasion." Id. at 623. The police were also aware of multiple facts connecting the defendant to the crime. For example, her car was seen near the victim's home less than two hours before the assault, she had a key to the victim's residence and there was no sign of forced entry, the victim had a restraining order against the defendant, and there were blood stains in the exterior of the defendant's car. Id. In sum, the seizure was lawful because the police had "a substantial basis for concluding" that the phone contained "evidence connected to the crime under investigation." Id. The court also ruled that the defendant's subsequent "consent to search her cell phone was without limitation." Id. at 625-26. The police communicated their intent to search the entire cell phone to the defendant, and she consented to the search, providing the police with passwords to the phone and to her Snapchat account. Id. at 626. Applying "a common sense interpretation" to the defendant's entire exchange with the police detective, the Appeals Court found that her "consent to search her cell phone was free, voluntary, and unlimited." Id.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police approached the defendant sleeping in the stairwell and seized a cell phone on the floor nearby. Id. at 282. There was probable cause to seize the phone because the police "had information that the defendant and victim had been together on the day of the murder, and also that [the murder victim's boyfriend] had recently overheard the defendant confessing to the murder to an unidentified person on a cell phone." Id.

- Commonwealth v. Martinez, 476 Mass. 410 (2017). State police used law enforcement version of P2P client to investigate sharing of child pornography, identified such activity coming from a

Massachusetts IP address, and subpoenaed Comcast for information regarding the IP address for the 30-minute period on March 9, 2012, during which police downloaded four suspected child pornography video files shared from the account associated with the IP address. Id. at 411–13. The ISP gave police a name (Angel Martinez) and an address. Id. at 413. Local law enforcement then obtained a warrant to search the apartment located at the address for computers and related items connected to the suspected possession and distribution of child pornography. Id. The apartment was leased to the grandmother of the Comcast account holder and of the defendant (Adalberto Martinez). Id. at 413 n.2. Law enforcement seized two laptops belonging to the defendant and found five videos containing child pornography on one of them. Id. The SJC held that the affidavit in support of the search warrant (containing information that a particular IP address was used to share child pornography and that this IP address had been assigned at the time to a subscriber at the specific physical address to be searched) was sufficient to establish probable cause for the search, even though the named subscriber was neither listed as, nor confirmed to be, living in the apartment searched, and even though police had no information before the search linking the defendant to the residence. According to the SJC, law enforcement did not have to verify that the account holder lived at the address searched. Id. at 418. Once the nexus between the crime and the service address was established, the names of the account holder and of the leaseholder were incidental. Id. The SJC rejected the argument that law enforcement had to show that the network was secure or that no one outside the address could access the network. Id. at 419. Where the warrant was for the search of a place (not for the arrest of a person), law enforcement needed only demonstrate a sufficient nexus between the criminal activity under investigation, the items sought, and a place to be searched. Id. Even assuming law enforcement could know a network was not secured, unauthorized use of the network did not negate the substantial basis to think the evidence would be located at the address. Id. at 420–21 ("[P]robable cause does not require investigators to 'establish to a certainty that the items to be seized will be found in the specified location,' nor does it require them to 'exclude any and all possibility that the items might be found elsewhere.'" (quoting Anthony, 451 Mass. at 70)).

The decision came with caveats. The SJC cautioned that its decision here does not mean that probable cause always exists any time investigators link illegal computer activity to an IP address and then link that IP address to a physical address. Martinez, 476 Mass. at 422. To support probable cause, law enforcement should use reliable methods—such as the administrative subpoena here—to connect the IP with a physical address, not IP address mapping services. Id. at 423. Additionally, some technologies (e.g., Tor exit relays, VPNs, and proxy server connections, which can mask originating IP addresses) may erode the connection between an IP and a physical address. Id. Law enforcement may be required to disclose in affidavits the possibility that one of these technologies was, or may have been, used based on facts known or reasonably knowable to investigators at the time. Id. "If such technologies become more common, it is entirely possible that we would require police to proceed in multiple steps, obtaining subpoenas related to each intermediary IP address or warrants to search each location hosting those IP addresses." Id. In some cases, law enforcement may be required to determine, by forensic examination of a wireless router, which devices were connected to it and when before searching particular computers. Id.

- Commonwealth v. Perkins, 478 Mass. 97 (2017). "Based on intercepted telephone conversations between defendant's alleged middleman and street-level distributor of cocaine, police surveillance of suspected drug transaction, and other information, the judge issued a warrant authorizing a search of the defendant's apartment for evidence including a cellular telephone and drug-related records." Id. at 99. The warrant also included authorization to seize currency, distribution paraphernalia, documentation about the premises and its contents, among other items. Id. at 101. The affidavit did not seek authorization to search for narcotics. Id. at 98. Police seized a large quantity of cocaine, several cell phones, drug paraphernalia, and ammunition. Id. at 101. The SJC concluded that the affidavit justified searching the apartment for the defendant's phone. Id. at 105–06. They further concluded that the seizure of nine additional phones found in the apartment was supported by probable cause, but that the police did not have discretion to "search every portion" of these additional phones. Id. at 106. Instead, the plain terms of the warrant restricted their search to call activity and contact lists and did not authorize police to "rummage through the entirety of the defendant's cellular telephones." *Id*. at 106. With regards to searching the defendant's apartment for records, proceeds, and paraphernalia, however, the SJC held that the affidavit:

  > did not contain sufficient particularized information to justify [such] a search of the defendant[']s apartment . . . . The affidavit included a single, conclusory statement that probable cause existed based on the affiant's "training and experience and the facts and circumstances learned during the course of this investigation," [but] contained no facts, or opinion based upon the affiant's considerable experience as a narcotics officer, that would have establish[ed] probable cause to believe that the defendant would be likely to store particular items of [drug-related records, proceeds, or paraphernalia] in his home.

  Id. at 109.

- Commonwealth v. Jordan, 91 Mass. App. Ct. 743 (2017). In a murder investigation in which defendant was a suspect, police obtained search warrant for his CSLI, call details, text messages, and subscriber information for a six-week period surrounding the date of the homicide. Id. at 744. The Appeals Court found that the trial judge properly suppressed the text messages. Id. Although the affidavit in support of the warrant established probable cause to believe that the victim had been murdered (i.e., a crime had been committed), it made no connection between the defendant's use of his cell phone and his involvement in the crime, and thus did not establish probable cause to conclude that the text messages would provide evidence connected to the crime. Id. at 749–51. The affidavit did establish probable cause to conclude that the defendant committed the crime and showed that the defendant had a cell phone and that it was in use around the time of the murder, and so it established probable cause to believe that the CSLI would provide evidence of the defendant's involvement in the crime. Id. at 750–53. The SJC also held that the trial court had properly suppressed "contact information" insofar as that meant an address book or contact list because the affidavit failed to establish a nexus between the crime and the defendant's contact information. Id. at 753–54. However, if "contact information" meant subscriber information and call records, there was no basis for suppression. Id.

- Commonwealth v. Keown, 478 Mass. 232 (2017). Defendant was suspected of murdering his wife by poisoning her. In the course of the investigation, police obtained a warrant to search his computer and discovered evidence of incriminating Internet searches, which was introduced at trial. Id. at 234–37. The SJC held the affidavit established a sufficient nexus between the crime and the item sought where: (1) it established the defendant's sophistication with computers (he had worked as a Web designer), and showed that he had forged contracts and admissions letter/other communications from Harvard Business School (can infer he used computer); (2) it described forgeries related to the motive alleged in the affidavit, i.e., to kill his wife to prevent her finding out about their impending financial ruin and his lies and to collect her life insurance benefits; (3) it specified that the victim had died from ethylene glycol poisoning which, the affiant noted, would likely have involved online research. Id. at 238–39.

- Commonwealth v. Broom, 474 Mass. 486 (2016). At the time of defendant's arrest for murder, his cell phone was seized. Id. at 494. Ten months later, law enforcement applied for and obtained a search warrant for its contents. Id. The affidavit contained information about the investigation and the fact that no CSLI information could be obtained for the time surrounding the murder but that the defendant's phone records showed he sent and received text messages and accessed the Internet at the relevant timeframe. Id. It then described the many types of data the detective wanted to search in order to uncover information pertinent to the investigation. Id. at 494–95. The SJC held the search was not supported by probable cause. Id. The court held that "it is not enough that the object of the search *may* be found in the place subject to search. Rather, the affidavit must demonstrate that there is a reasonable expectation that the items sought *will* be located in the particular data file or other specifically identified electronic location that is to be searched." Id. at 496 (citations omitted) (emphasis in original). Police here already had the defendant's CSLI (except for the time period surrounding the murder) and call records and would have known that the victim's number did not appear in those records. Id. The warrant was also found to be too broad. Id. at 495, 496 n.13.

- Commonwealth v. White, 475 Mass. 583 (2016). A police investigation of an armed robbery and shooting led to the defendant as one of three suspects. Id. at 584. After suspicion focused on him, the detective located his phone, which was held by the defendant's school administrator pursuant to school policy. Id. The detective then "seized the telephone to prevent the defendant from retrieving it and removing evidence or destroying the device." Id. Police had no information at the time indicating that the phone had been used to plan, commit, or cover up the armed robbery they were investigating, or that it contained any evidence of the crime, but instead relied on knowledge that cell phones are frequently used when the offense involves multiple perpetrators. Id. Sixty-eight days after the seizure, police obtained a warrant to search the cell phone and found evidence that was later ordered suppressed. Id. The SJC held that the seizure was not supported by probable cause because probable cause may not be based solely on an officer's opinion that the device is likely to contain evidence of the crime under investigation. Id. at 584–85. "[E]ven where there is probable cause to suspect the defendant of a crime, police may not seize or search his or her cellular telephone to look for evidence unless they have information establishing the existence of particularized evidence likely to be found there." Id. at 590–91. A contrary decision

would mean that, where probable cause to charge someone with a crime existed, the person's phone would almost always be subject to seizure and subsequent search. Id. at 591.

- Commonwealth v. Williams, 90 Mass. App. Ct. 1118 (2016) (unpublished). The victim was shot after a drug deal with two suspects. Id. at *1–2. Two witnesses testified that the victim had arranged the deal via phone. Id. Police zeroed in on an 857 (area code) number linked to a person named Patrick Malone. Id. Defendant was then identified as the second suspect and was interviewed by police; he stated that he had known Malone for twenty years and that they had a phone conversation on the morning of the shooting. Id. at *3–4. Police seized the defendant's iPhone and secured it to get a warrant. Id. The Appeals Court held that "there was probable cause to believe that the defendant's iPhone would contain evidence linking his alleged coventurer Malone to the 857 number and thus to the shooting." Id. at *5. See also Commonwealth v. Perkins, 478 Mass. 97, 105–06 (2017), (where police had detailed and specific knowledge about the defendant's use of a cell phone to arrange drug transactions, and a particular phone number with which that cell phone had been in contact at a specific time, there was probable cause to believe that the defendant used a cell phone to arrange a drug sale and that he had done so on other occasions and the seizure of nine cell phones from his apartment was proper). But see Commonwealth v. Fulgiam, 477 Mass. 20, 34 (2017) (where warrant application established a personal relationship between defendant and victim and the circumstances of the murders suggested a connection to drugs, it did not, without more, justify intrusion into the content of the communications between defendant and victim).

- Commonwealth v. Finglas, 81 Mass. App. Ct. 1102 (2011) (unpublished). Police were sent information about the defendant, whose email address had received five images depicting child pornography. Id. at *1–2. On interlocutory appeal, the Appeals Court granted the defendant's motion to suppress evidence obtained as a result of a search of his residence. Id. at *3. It did so because the affidavit in support of the warrant was "inadequate to establish a timely nexus between the defendant and the location to be searched and to permit the determination that the particular items of criminal activity sought reasonably could be expected to be found there." Id. The Appeals Court held that the affidavit did not provide any evidence that a computer at the residence had been used to search for or download any child pornography or that the defendant had actually accessed the emailed images. Id. at *2. Further, a police officer's opinion about the common practices of child pornography collectors was not enough, without further facts, to support a finding that the defendant's computer likely contained child pornography. Id. at 3.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it based on an affidavit alleging: (1) both shared folders had a copy of the same pirated movie, (2) the second computer's shared folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 105, 107–09. The court invalidated the search warrant because it found police did not provide a "substantial basis" to believe there would be

child pornography on the computer. Id. at 111. The court found it unreasonable to infer that somebody interested in sharing a commercial movie would also be interested in sharing child pornography. Id. at 112. That the defendant had access to child pornography did not help the Commonwealth's case. Id. Nor was a suspicious statement, standing alone, enough to provide the substantial basis necessary for probable cause. Id. at 113.

- Commonwealth v. Anthony, 451 Mass. 59 (2008). Police received a tip about a person soliciting child pornography online. Id. at 60–62. They traced these solicitations to a library and arrested a homeless suspect there. Id. at 62–63. Shortly after the arrest, the suspect took a receipt (along with other pieces of paper) out of his pocket and tore it up. Id. at 63. This receipt was from a repair shop for the repair of two laptops. Id. Police also determined he rented a storage locker. Id. at 64. Police sought and received a search warrant for the locker, the laptops, and a hard drive from the library. Id. at 65–66. A Superior Court judge granted the defendant's motion to suppress for lack of probable cause, however, and the Commonwealth pursued an interlocutory appeal. Id. at 67–68. The SJC reversed the motion judge's suppression of the warrant, finding the affidavit established probable cause. Id. at 73. Specifically, the court found information about the suspect's prior conviction for child pornography, the outside tip, and the suspect's admission to viewing child pornography in violation of his probation established probable cause for the crime. Id. at 70–71. From there, it found the fact that a homeless individual rented a storage locker using a false address—along with the detective's experience that viewers of child pornography tend to collect it—supported the idea that the suspect might hide child pornography at his storage locker, the only space under his control. Id. at 71–72. The court found the suspect tearing up the receipt supported the inference that he was trying to hide child pornography. Id. at 71. It emphasized that the affidavit did not rely solely on the opinions of the affiant with respect to general characteristics of collectors of child pornography. Id. at 72. Rather, the affidavit contained enough facts and inferences to support a nexus between the alleged crime and the locations to be searched. Id. 72–73.

### (2) Independent Source Doctrine

- Commonwealth v. Wilson, 486 Mass. 328 (2020). The police initially obtained defendant's CSLI data pursuant to an § 2703 order, without a warrant, in 2010. Id. at 336. The CSLI placed the defendant in "the victim's hotel, at the commuter lot where the [victim's] rental vehicle was found, and in the location where the victim's body would later be discovered, at relevant times on the night of the murder." Id. at 331. In 2014, the police obtained the same CSLI information pursuant to a search warrant. The court found that the 2014 warrant satisfied the "independent source doctrine," "a well-recognized exception to the exclusionary rule under both the Fourth Amendment and art. 14." Id. at 335. The doctrine provides that "evidence initially discovered as a consequence of an unlawful search may be admissible if later acquired independently by lawful means untainted by the initial illegality." Id. (quoting Commonwealth v. DeJesus, 439 Mass. 616, 624 (2003)). Here, the affidavit supporting the 2014 warrant for the CSLI was based on facts wholly independent of the CSLI data obtained in 2010. Id. at 336. These facts included the following: the defendant's public statements about having a firearm like the one used in the murder, his status as the likely father of the victim's unborn child, causing financial obligations to

the victim and the "ire of the defendant's wife," the victim's statement to a friend that the defendant asked her to get an abortion, the cellphone communications between the defendant and the victim until shortly before the victim's cellphone activity ceased at 10:49 P.M. on the night of the murder, and a Facebook message from the victim's account after she was reported missing "claiming she was in the hospital after an abortion, although police determined that she was not a patient at any area hospitals." Id. at 337.

- Commonwealth v. Gosselin, 486 Mass. 256 (2020). The defendant appealed his conviction for first-degree murder, arguing, *inter alia*, that his trial counsel was ineffective for not moving to suppress CSLI evidence, as such evidence provided probable cause for the search warrant for his home—the search of which produced critical inculpatory evidence. Id. at 264. The court declined to resolve whether the § 2703 warrant was supported by probable cause, on the grounds that "the search warrant affidavit satisfied probable cause when excising the unconstitutionally obtained CSLI," such that the defendant failed to demonstrate prejudice and his trial counsel was not ineffective. Id. at 264-66 & n.9.

### (3) Particularity / Scope

The Fourth Amendment, art. 14, and G.L. c. 276, § 2, all require that search warrant applications particularly describe the places to be searched and the items to be seized. See Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Massachusetts courts treat these provisions as coextensive. Id. The dual purpose of these requirements is (1) to protect people from general searches and (2) to provide the Commonwealth the opportunity to demonstrate to a court that officers' search authorization was properly limited. Id. Additionally, the requirement provides essential information to a person whose property is being searched. Id. (citing Katz v. United States, 389 U.S. 347, 356 (1967)). The cases below explore the tension between the particularity requirement and the amorphous nature of data in the digital era.

- Commonwealth v. Carleton, 497 Mass. 11 (2026). The defendant was convicted of first-degree murder and possession of a firearm without a license. Id. at 12. At the time of the murder, which was a drive-by shooting, security footage from both the scene of the crime and the parking lot where the defendant drove directly after the shooting showed the defendant wearing a distinctive green t-shirt with an orange and white "Airmax" logo. Id. at 13–14. After the shooting, police found a Facebook account with the defendant's first and last name. Id. at 14. The account featured a "selfie" photograph of the defendant wearing a green t-shirt with an orange and white Airmax logo with the caption "Just me my blunt n my thoughts," and it was posted less than two hours before the shooting. Id. at 14. At trial, the Commonwealth's evidence included four photographs and their associated metadata from a cell phone, including the same selfie from the Facebook account. Id. at 26. After the cell phone was seized, the police obtained a search warrant to search the phone for photographs, specifically, the Facebook selfie. Id. at 27.

  On appeal, the defendant argued that "photographs and associated metadata obtained from a cell phone seized from his home should have been suppressed because there was no probable cause to believe there was a nexus between the cell phone and the crimes and because the search of the cell phone was unreasonably delayed and exceeded the scope of a warrant obtained after the cell phone was seized." Id. at 12. The SJC held that the scope of the warrant was not exceeded

because three of the four photographs "showed the defendant wearing a green Airmax T-shirt on the day of the shooting and thus fall squarely within the ambit of the search warrant." Id. at 29. While "the fourth photograph did not depict the defendant wearing the Airmax T-shirt, and was created approximately two months before the shooting," the burden is on the defendant to establish that "the items seized [from a warranted search] exceeded those named on the warrant." Id. at 29, citing Commonwealth v. Taylor, 383 Mass. 272, 280 (1981). Here, the defendant neither showed that "the photograph file was located in an area of the cell phone the police could not reasonably [search] to locate the items described in the warrant," Carleton, 497 Mass. at 30, citing Commonwealth v. Dorelas, 473 Mass. 496, 502 (2016), nor that the "discovered objects were of a different type than what were authorized to be located by the warrant" because "the warrant authorized a search for photographs and—from all that appears—only photographs were located." Carleton, 497 Mass. at 30.

- Commonwealth v. Colina, 495 Mass. 13 (2024). Defendant was arrested for murder and improper disposal of human remains. Id. at 16-17. After the defendant's arrest, officers obtained and executed three separate search warrants, resulting in the discovery of two songs by the defendant and his online purchase history. At trial, "The Virus," a song seized from the defendant, was admitted in evidence. Id. at 20. So too was the defendant's online purchase history. On appeal, the defendant asserted that the three warrants were unsupported by probable cause, insufficiently particular, and lacked temporal limits.

  The SJC upheld all three search warrants. While a warrant to search a cell phone must "contain some temporal limit," id. at 28 (quoting Commonwealth v. Snow, 486 Mass. 582, 594 (2021)), a temporal limit is not required for warrants seizing, but not searching the contents of, devices, assuming Snow extended to computers (where the defendant's songs and purchase history were found). Id. at 28. Since the first two warrants did not authorize a search of the computer's contents, they did not need a temporal limit.

  The third warrant "authorized a forensic examination of the defendant's computer tower and three external hard drives seized pursuant to the first two warrants." Id. at 30. "When determining the proper temporal scope for a cell phone search, judges consider the type of crime, the nature of the evidence sought, and normal inferences about how far back in time the evidence could be found." Id. at 28 (citation modified). Here, the SJC held that the song "was saved on the defendant's computer about two weeks before the killing and less than one week before the latest online communication between the defendant and the victim, negating the defendant's temporal limit claim." Id. at 33.

- Commonwealth v. Perry, 489 Mass. 436 (2022). The police and the FBI were investigating six different robberies committed on six different dates in September and October of 2018. In addition, on October 6, 2018, a store clerk was shot and killed during an attempted robbery. Id. at 440. Each of these crimes "was perpetrated in a comparable manner by a man fitting a similar description." Id. Based on witness testimony and surveillance footage, investigators also believed that the robber had been assisted by a coventurer, acting as a getaway driver. Id. at 441. To identify the robber and his coventurer, the police and the FBI obtained cell site location

information ("CSLI") for all devices that connected to specific cell towers during a particular time frame corresponding to the six robberies as well as one attempted robbery that resulted in a homicide. Id. at 437. This information is known as a "tower dump." A tower dump "provides officers with CSLI from every device that connected to a particular cell site within a specified period[,] allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time." Id. at 440. The FBI obtained a search warrant for tower dumps corresponding to the dates for four of the robberies ("first warrant"). Id. at 441. Boston police obtained a search warrant for tower dumps corresponding to the two other robberies and the attempted robbery and homicide ("second warrant"). Id. The execution of the search warrants produced information on over 50,000 unique telephone numbers. Id. at 442. After cross-referencing these numbers, the investigators were able to identify the defendant and the coventurer. Id.

The defendant moved to suppress any evidence resulting from the search, arguing that the warrant lacked sufficient particularity because it allowed the police to search the CSLI of third parties who were merely in the vicinity of the crime. Id. at 458-59. The SJC rejected the defendant's argument that warrants for tower dumps are per se unconstitutional. Id. at 438. The court found that one of the search warrants in this case was sufficiently particular, while the other was not. Id. The supporting affidavit for the second warrant limited the scope of the search by explaining "that investigators sought to obtain the tower dumps in order 'to identify and/or verify commonalities within [the] requested records'" for the purpose of identifying the defendant and the co-venturer. Id. at 461. This limitation in scope was sufficient to satisfy the particularity requirement, and it would be unreasonable to require "police to identify a presently unknown suspect by name." Id. However, the court "recognize[d] the potential invasions of privacy that could befall those innocent and uninvolved third parties whose CSLI is revealed once an application for a search warrant is allowed." Id. at 462. Accordingly, the SJC used its superintendence powers under G.L. c. 211, § 3, to place prospective limits on future tower dump searches: first, only a judge may issue search warrants for tower dumps; and second, "[t]he warrant must include protocols for the prompt and permanent disposal of any and all data that does not fit within the object of the search following the conclusion of the prosecution." Id. at 462-63. This "holding applies prospectively and to those cases that are active or pending on direct review on the date of issuance of the rescript in this case." Id. at 464.

- Commonwealth v. Melendez, 490 Mass. 648 (2022). The defendant was arrested for first-degree murder after a firefighter was called for a supposed electrical fire in the apartment building and found the victim's body during a separate welfare check. Id. at 650-51. The victim's son provided investigators with descriptions of jewelry that was missing from the victim's apartment. Id. at 652. Further investigation showed that the defendant had sold some of that jewelry to a jewelry store in Everett. Id. Detectives obtained a warrant to search the defendant's cell phone records, which showed numerous calls to pawn shops. Id. at 653. During a search of the defendant's apartment, police seized his cell phone and obtained a warrant to search it. Id. at 654. At trial, the Commonwealth introduced evidence obtained from the defendant's phone, including text messages. Id. On appeal from his conviction for first-degree murder, the defendant argued, in

relevant part, that his attorney rendered ineffective assistance by failing to move to suppress evidence gathered from his cell phone because "the affidavit in support of the application for a search warrant to extract personal data from his cell phone did not establish probable cause that evidence of the alleged crimes would be found on the cell phone." Id. at 657.

The SJC agreed that "the affidavit, on its face, contained insufficient information to establish probable cause to search the cell phone" and, consequently, counsel was "ineffective for failing to file a motion to suppress" evidence gathered from this search. Id. at 661. However, the court concluded that the defendant was not prejudiced by counsel's failure to file a motion to suppress, "because the remaining evidence . . . sufficed to support the defendant's conviction." Id. While the affidavit demonstrated probable cause to believe that the defendant committed the charged offenses, this information was insufficient to justify a search of the phone. Id. at 661. More specifically, "[t]he affidavit lacked any information 'demonstrat[ing] a nexus between the alleged crime and the device to be searched.'" Id. at 559 (quoting Commonwealth v. Henley, 488 Mass. 95, 115 (2021)). Distinguishing this case from Henley and other precedent in which a nexus between the use of the phone and the crime had been established, the court noted that the affidavit did not allege that the crime was premeditated, that the defendant may have communicated with accomplices, or even that he had used the phone before, during, or after the crime. Id. at 661. The court also rejected the Commonwealth's argument that the cell phone was used in relation to the defendant's attempts to sell the victim's jewelry at a pawn shop. Id. at 660 (finding that the connection between the phone and the sale of jewelry was "speculative in the absence of additional facts to support such inferences").

- Commonwealth v. Henley, 488 Mass. 95 (2021). In an appeal from a conviction for murder, the defendant argued that the search warrant police used to search his phone lacked particularity. Denying the appeal, the SJC clarified the requirement related to particularity it had set out in Commonwealth v. Dorelas, 473 Mass. 496, 502 (2016). In Dorelas, the SJC had concluded that officers must conduct a "search in a way that avoids searching files of types not identified in the warrant." Id. at 502, quoting United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001), cert. denied, 535 U.S. 1069 (2002). The SJC clarified that while "general or exploratory searches are [still] not permitted, requiring a search warrant application to identify specific locations or files on a cell phone to be searched places an unrealistic burden on law enforcement and restricts legitimate search objectives, given the storage capacity and file structure of most cell phones." Id. at 119. Therefore, in cases "where the location of evidence on a cell phone is unknowable to law enforcement, the Dorelas requirement that officers identify file types to be searched in the warrant is impractical." Id. at 120.

  Here, the warrant properly limited the search to eight enumerated categories of evidence related to the crime: "ownership of the cell phone, contacts with persons at the homicide, discussion or knowledge of the homicide, familiarity with persons involved in the homicide, familiarity or contact with locations or items associated with the homicide, communications that led [the defendant] to arrive at the scene of the shooting, evidence of gang activity, and discussions of firearms." Id. at 119. The warrant was sufficiently particular "without limiting where in the

electronic contents of the cell phone the search would take place." Id. at 120. By contrast, the failure to include a temporal limit on the search "rendered the warrant impermissibly broad." Id. at 121. Based on the particular facts of this case—including that the crime was a gang-related-murder—the SJC concluded that "a temporal limit of two months would have been reasonable." Id. at 122 (emphasizing that this finding is based on a fact-intensive inquiry and does not amount to a general rule about temporal scope). However, the defendant was not prejudiced by the lack of a temporal limit in the warrant here because "[t]he text messages were sufficiently limited in content and scope such that the Commonwealth did not capitalize on the lack of particularity in the warrant." Id. (quotation marks omitted).

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. However, the court concluded "that the search of the phone was not sufficiently particular because it lacked any temporal limit." Id. at 583. More specifically, the court held "that (1) the correct remedy for the warrant lacking particularity in this case [was] partial suppression; (2) the search of text messages, call logs, and Snapchat video recordings was proper; yet (3) the lack of time restriction rendered the warrant impermissibly broad." Id. at 590. Accordingly, the SJC remanded the case to the Superior Court to determine whether "the proffered evidence fell outside what would have been a reasonable temporal limit." Id. First, as to partial suppression, the court noted "that an overbroad warrant generally requires only partial suppression of the information for which there was not the requisite nexus, as long as the Commonwealth had not relied on or otherwise exploited it at trial. Id. at 591-92 (quotations and citations omitted). Second, because the police here had probable cause to search the defendant's cell phone for evidence of joint venture, the scope of the search properly included communications such as call logs, text messages, and Snapchat videos. Id. at 593. Third, a cell phone search warrant cannot be sufficiently particular without some temporal restriction that should "err on the side of narrowness." Id. at 594. Where the initial search provides probable cause to broaden the search, "nothing precludes" officers from requesting another, broader warrant. Id.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case involving partial suppression of CSLI, the government requested 48 hours of a shooting suspect's CSLI around the time of the shooting, received 34 hours of CSLI in response to this request, and then had all but three hours of CSLI ("covering the period approximately ninety minutes before and ninety minutes after the shooting") suppressed by the trial judge. Id. at 164. The SJC upheld this partial suppression of CSLI data but noted in dicta that the "severance doctrine [of Hobbs] is not without limits," and that "where a warrant so lacks particularity or is so overbroad that it begins to resemble a general warrant, total suppression is required." Id. at 168-69. The court deemed the CSLI request at issue "not so overbroad on the facts of this case so as to be akin to a general warrant" and found it to "represent 'a reasonable period of time encompassing the commission of

and flight from the crime.'" Id. at 169 (quoting Hobbs, 482 Mass. at 550). However, the SJC declined to provide further guidance on exactly "how overbroad a request for CSLI must be in order for total suppression to be appropriate." Id.

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). The government requested three and a half months of historical CSLI from defendant's cell service provider, from December 1, 2010 to March 15, 2011, where defendant was a suspect in a December 16, 2010 killing. Id. at 543, 550. "This extended request was in part the result of the failure to identify the defendant as a suspect for nearly two and one-half months, and the absence of any evidence of his current location once he was identified as a suspect." Id. at 550. The SJC considered the question of whether "either the Fourth Amendment or art. 14 require[s] total suppression of the entire amount of CSLI collected," or whether "the proper remedy [is] to suppress only the CSLI for which there is not the requisite nexus to the crime," and concluded that "where the requisite nexus for probable cause clearly exists for a reasonable period of time" contained within the requested period, "the CSLI for [the relevant] period of time need not be suppressed so long as the CSLI for which there is not the requisite nexus to the crime is not relied on or otherwise exploited by the Commonwealth at trial." Id. However, the court suggested its holding was fairly narrow, noting that "[g]iven the uncertainty in the case law regarding overbroad requests for CSLI, we proceed cautiously on this issue." Id. The court also "emphasized the significant constitutional issues raised by the collection of extended amounts of historical CSLI, and the importance of limiting the requests accordingly." Id. at 550 n.13.

- Commonwealth v. Holley, 478 Mass. 508 (2017). In a murder investigation, law enforcement examined the victim's call records and learned that the last call the victim answered before the shooting came from the defendant's telephone number. Id. at 511. Law enforcement then obtained cell phone records through a warrant served on the carrier and found multiple incriminating communications via text and call between the victim and the defendant's joint venturer. Id. The warrant for the phone records sought "subscriber information; billing records and detailed airtime; outbound call detail; call origination and termination location; stored GPS location information, and/or stored cellular tower records, cell tower sector information, range from cell tower information (RTT) and physical address of cell sites; and all stored contents of electronic or wire communications including stored or deleted voicemail, read, unread, deleted, or sent electronic mail or text messages, and stored files; and listing of all associated phone numbers, of a subscriber to or customer of such service" between October 1 and 18, 2012. Id. at 524–25. The broad scope of the search raised "significant concerns" for the SJC because it did not sufficiently limit the scope of the search so as to prevent "exploratory rummaging." Id. at 525, 528. But because the record was silent on how the provider conducted the search and on what information, if any, it provided to the Commonwealth beyond the text messages (it was even unclear whether the provider kept any stored content apart from text messages as part of its business records) and because the only communications used at trial were the defendants' redacted text messages from four and two days before the shooting, respectively, the day of the shooting, and the day after the shooting, the court could find no error in the denial of the motions

to suppress. Id. at 525 (noting that the "Commonwealth did not capitalize on the lack of particularity in the warrant").

- Commonwealth v. Molina, 476 Mass. 388 (2017). Police investigating a P2P network found child pornography shared by a Massachusetts IP address. They subpoenaed Verizon and obtained a name (Hermes Delcid) and service address. Id. at 390–91. Further investigation found the name on the mailbox outside of the address and RMV records showed Delcid at the address. Id. at 391. Police then obtained a search warrant for the apartment and in particular for electronic devices containing evidence of child pornography, evidence of child pornography in other formats, evidence related to access to the Verizon account and the P2P network, and evidence related to access to electronic devices at the apartment. Id. In a bedroom later identified as the defendant's, police observed the P2P program running on an open laptop (computer screen showed downloads and uploads of child pornography files in progress). Id. at 392. The search team seized numerous electronic devices from the apartment, including the defendant's laptop and desktop computers and his external hard drive. Id. On appeal, the defendant argued that the search warrant was impermissibly overbroad as to both places and "things" to be searched. Id. at 393. The SJC disagreed. Id. at 389. It found that the warrant appropriately substantiated a connection between the apartment and the evidence of child pornography reasonably expected to be located therein. Id. at 394. That the apartment was shared by multiple people was immaterial because the warrant authorized a search of the location associated with the IP address, not a search of any single associated subscriber. Id. at 395. Computer devices using the monitored IP could have been anywhere in the apartment, so where the defendant's unlocked bedroom showed no indicia of separate ownership from the rest of the apartment, the search of his bedroom was proper. Id. at 396. With regard to the things to be searched, the SJC made the following finding: "Because that evidence, in the form of electronic files, could be easily transferred between devices at the same location, police need not have limited the devices to be searched. Id. at 396. The SJC raised the reasonableness of the search *sua sponte.* Id. at 397. It found that where "multiple electronic devices that may well belong to multiple individuals are seized and searched, the reasonableness of the undertaking will be judged, at least in part, by whether the searches of those devices are conducted in a manner that seeks to limit the scope of the search as much as practicable in the particular circumstances." Id. at 397–98. The SJC may in the future "consider whether to require, as some courts have, a digital search protocol that would affirmatively demonstrate 'a high regard for rights of privacy and take all measures reasonable to avoid unnecessary intrusion.'" Id. at 398 (quoting Commonwealth v. Vitello, 367 Mass. 224, 262 (1975)).

- Commonwealth v. Keown, 478 Mass. 232 (2017). "The scope of the search authorized by the warrant included files on the laptop related to the health or death of the victim; other prominent poisoning cases; ethylene glycol or other poisons; and the financial records, life insurance plans, and wills of the victim and the defendant." Id. at 240. The affidavit "established probable cause to search for evidence on the laptop computer relating to the defendant's role in his wife's death." Id. "These categories of evidence were related to the means of committing the crime and the motive of the defendant, and provided sufficient guidance to the examiners so that they were not on a fishing expedition." Id. In addition, the search was conducted reasonably. Id. at 241.

Examiners used a list of 50 search terms that was later supplemented by 19 additional terms. While not part of the warrant application, the terms were related to the categories of evidence sought in the affidavit. "[T]he examiner only looked closely at approximately 325 files of the nearly 400,000 found on the laptop computer." Id. The search in this case "took place more than a decade ago in an entirely different technological landscape"; thus, the absence of an ex-ante search protocol did not defeat particularity. Id. at 41.

- Commonwealth v. Dorelas, 473 Mass. 496 (2016). The defendant, who was a suspect in an assault and battery by means of a dangerous weapon (firearm) and an assault with intent to murder, was involved in a shooting. Id. at 497. Interviews with his family and friends indicated that prior to the shooting he had received threatening calls and texts. Id. at 498. Police believed the defendant's iPhone contained evidence linking the defendant and the other shooter to the assaults and obtained a warrant authorizing a search for, among other things, saved and deleted photographs. Id. at 498–99. The search resulted in the discovery and seizure of incriminating photographs. Id. at 499. The defendant contended that police only had probable cause for his call logs and text messages, but not his photographs. Id. at 500. On direct appellate review, the SJC reached the following holding: "Communications can come in many forms including photographic, which the defendant freely admits. So long as such evidence may reasonably be found in the file containing the defendant's photographs, that file may be searched." Id. at 503. Therefore, such a search is "neither outside the scope of the warrant nor unreasonable." Id. The defendant further argued that a search using the Universal Forensic Extraction Device (UFED) could have been conducted for communications, including photographic communications, without reviewing his photograph file. Id. at 504. The SJC held that such a retrieval method was not constitutionally required where the photographic evidence would also reasonably be found in the phone's photograph file. Id. The court was concerned that texts and their attachments might be overwritten over time and the evidence would thus only be found in the photograph file. Id.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the shooting. Id. at 764–65. They seized five computers and disks. Id. at 765. The defendant asserted that this was unlawful because the warrant did not specifically authorize the seizure of these items. Id. at 770. The warrant did authorize, however, seizure of several types of documents. Id. at 771. The court held that the seizure of the computers was reasonable because they functioned as "closed containers" storing documents. Id. at 766, 771. [Note: In Preventative Medicine Assocs. v. Commonwealth, 465 Mass. 810 (2013), the SJC clarified that in McDermott, the fact that the warrant was issued before an indictment as part of an investigation and the Commonwealth's use of preset search terms during the preliminary review of the defendant's files were important to its holding, id. at 830–32. The court stated that it took "seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may

not actually fit within the scope of the search warrants obtained." Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.]

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. 2001). Police received information that defendant was distributing child pornography over the Internet. Id. at *1. They obtained a warrant allowing them to seize the defendant's computers and associated storage devices, to bring those items to a search location, and to search them for "visual images depicting children in a state of nudity or sexual conduct." Id. at *8. The defendant challenged the warrant as not particular enough because it allowed for seizure and search of all files on the computer, many of which were not related to child pornography. Id. The court denied the defendant's motion, noting that "where the commingling of legitimate and illegitimate items makes an on-site examination impracticable, a temporary seizure of the whole is permitted." Id. (citing various federal cases to that effect). It noted that "[t]he investigators could not have known in what form—whether on the computer hard drive or other various storage devices—the defendant was storing the target images. To insulate such images from search and seizure merely because other, non-incriminating items may have sheltered the images would pervert the accepted purpose of the constitutional bar against general searches." Id. at *9.

- United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013). Police received a tip that a Washington resident was sharing child pornography over a peer-to-peer networking site. Id. at 1043. They prepared a search warrant affidavit setting forth the information they had received about the suspect's IP address, the pornography he shared, general peer-to-peer network operations, data storage, and known characteristics of child pornography offenders. See id. The magistrate granted the warrant, which authorized seizure of all of the defendant's computers and data storage devices, and police discovered large quantities of child pornography. Id. at 1043–44. The trial judge suppressed the evidence reasoning that the warrant was facially overbroad. Id. at 1045. The Ninth Circuit reversed this decision. Id. at 1046. It based this ruling on the "practical, common-sense decision" judges make in issuing warrants. Id. at 1046. Specifically, the Ninth Circuit found that "[t]he government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files" and reasoned that "[t]he government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner." Id. Given this reasoning and supportive precedent, the court found the warrant permissible. Id. at 1047.

- In re a Warrant for All Content & Other Info. Associated with Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386 (S.D.N.Y. 2014). Federal agents investigating illegal money remitting applied for a search warrant to access a suspect's entire email account in search of specified emails. Id. at 388. The Magistrate considered and rejected the reasoning that such a search was akin to a general warrant and therefore failed the Fourth Amendment's particularity requirement. Id. at 390–91. First, the judge noted that extensive authority supported the proposition that investigators could briefly examine a wide variety of documents during a search in order to determine relevance. Id. at 391–

92. Though that examination is essentially a seizure, it is also a practical necessity to determine which documents can be more permanently seized. Id. at 392–93. Next, he noted that courts have been more flexible with searches and seizures of electronic evidence because the large mass of undifferentiated information makes an on-site search impossible. Id. at 392. Courts have recognized the practical necessity of copying hard drives for later examination, allowing the government to access electronic information outside the scope of its search in order to effectuate that search. Id. at 393. Finally, the judge found that email provider employees would not be capable of performing the search themselves because they would not know enough about the investigation in order to properly recognize relevant emails. Id. at 395.

#### (4) Staleness of Information Supporting Probable Cause

In order to provide probable cause sufficient for a search warrant, the information contained in an affidavit supporting such a warrant must be sufficiently fresh. See United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (detailed below). In assessing staleness, courts "do not measure the timeliness of information simply by counting the number of days that have elapsed" but rather "assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." Id. (citing United States v. Pierre, 484 F.3d 75, 83 (1st Cir. 2007)). This requirement should not be confused with the separate Massachusetts statutory requirement (examined next) that warrants be timely executed after they have been issued. The following cases address staleness in the digital evidence context.

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that affidavit in support of the warrant to search his home did not establish probable cause because it was based on stale information: namely, an image depicting child pornography that was uploaded from the defendant's computer to the Skype service seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time (id. at 29), the court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the court identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]" – an act that required multiple, intentional

steps. Id. at 32. In such circumstances, the seven-month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020). Defendant was convicted of unlicensed carrying of a firearm outside his residence or place of business. Id. at 420–21.The police obtained a search warrant based an affidavit that described (1) a series of images and videos of the defendant and an acquaintance handling a TEC-9 firearm at the acquaintance's house, which the two of them posted on Snapchat, and (2) location data from a GPS device that the acquaintance, Santos, who was subject to GPS monitoring, was wearing at the time of the Snapchat posts. Id. The defendant argued that because "Snapchat videos and images that are posted on a particular date may have been taken, created, or recorded at an earlier date and uploaded much later… the Commonwealth failed to prove that the information officers relied on from the timestamps on the defendant's and Santos's Snapchat uploads was not stale." Id. at 424. The court rejected the defendant's arguments on staleness, finding probable cause was established by a Snapchat post by Santos from two days before the search warrant was obtained and executed: an image of a TEC-9 (semiautomatic) firearm captioned "Shyt change on my block trust issues I got put all my trust in semi autos." Id. at 421, 424. The court characterized the caption as "a present tense statement about Santos's perceived need for semiautomatic weaponry[, g]iven [which] there was probable cause to believe that the Snapchat image was taken contemporaneously with its posting" (which, in turn, was only two days before the warrant was executed). Id. at 424. The court did not discuss whether, or under what circumstances, similar posts absent such a present-tense caption could have sufficed to establish probable cause.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police waited ten days to apply for a search warrant on a seized phone. See id. at 283. This delay was permissible because "the defendant's minimal possessory interest was far outweighed by the government's interest in obtaining evidence regarding a recent murder." Id.

- United States v. Morales-Aldahondo, 524 F.3d 115 (1st Cir. 2008). Defendant was convicted of possessing child pornography as a result of an investigation targeting a child pornography website and its subscribers. Id. at 117–18. The download information obtained from the website was over three years old by the time the search warrant in this case was issued. Id. at 119. On appeal, the court upheld the trial judge's denial of the defendant's motion to suppress for staleness. Id. Focusing on the characteristics of child pornography collections, the court found that the warrant application (along with testimony by the same officer during a subsequent Franks hearing) "provided considerable support for the government's position that customers of child pornography sites do not quickly dispose of" their collection. Id. Given this support, the court found that three years was not so long a period that the information had become stale. Id.

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished). In this case, the Attorney General's Office investigated the defendant based on a tip they had received from a New Hampshire police officer. Id. at *1. Using information from online exchanges the defendant had with the officer four months prior, the AG's Office obtained

a search warrant for the defendant's premises where they located the evidence at issue in this case. Id. at *1, *6. The defendant alleged that the warrant was defective because, among other reasons, "there was no temporal proximity between the events constituting probable cause and the issuance of the warrant." Id. at *5. The court rejected this argument for two reasons. First, it found that the affidavit demonstrated continuous contact between the defendant and the undercover officer for several months. Id. at *6. Even though that information was itself four months old, the court found that it gave rise to an inference that the contact had continued. Id. Second, the court focused on the special circumstance of transmitting child pornography via computer. Id. at *7. Specifically, the affidavit described how computers retain data and how collectors of child pornography tended to retain those collections for long periods. Id. The court found that these descriptions "provided the magistrate with reason to conclude that the passage of time did not constitute a disabling tardiness." Id.

### (5) Delay in Obtaining a Warrant

"Police are permitted to hold a seized item for 'the relatively short period of time needed . . . to obtain a search warrant,' [but] they must 'release the item if a warrant is not obtained within that period.'" Commonwealth v. Cruzado, 480 Mass. 275, 283 (2018) (quoting Commonwealth v. White, 475 Mass. 583 (2016). "[T]here is no bright-line rule that demarcates when a delay is unreasonable." Id. Courts "analyze each case on its own facts, 'balanc[ing] the nature and quality of the intrusion on the individual's [interests under the Fourth Amendment to the United States Constitution] against the importance of the government interests alleged to justify the intrusion.'" Id. (quoting White, 475 Mass. at 593-94. This section discusses cases in which courts considered whether the delay in obtaining a warrant was reasonable.

- Commonwealth v. Diaz, 105 Mass. App. Ct. 809 (2025). Defendant was arrested pursuant to a warrant for crimes involving child sexual assault. Id. at 811. The police, incident to the arrest, seized Defendant's phone. Id. at 811. At time of arrest, the police did not have a search warrant for Defendant's phone. See id. at 811. The police placed the phone in "'secure evidence storage' at the Chelsea Police Department" for 123 days, when they "applied for and received a warrant to search the contents of the cell phone." Id. at 811, 812.

  Defendant moved to "suppress the evidence obtained from the search of the cell phone." Id. at 813. The Superior Court motion judge granted the motion to suppress, holding that the Defendant's privacy and possessory interest in his phone and the 123-day delay outweighed the Commonwealth's interest in the phone. Id. at 813; see also Commonwealth v. White, 475 Mass. 583, 593-94 (2016) (evaluating a motion to suppress evidence obtained after a delay in searching a cell phone by balancing the "nature and quality of the intrusion on the [defendant's] Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion").

  The MAC affirmed the Superior Court's suppression order. The MAC recognized the Commonwealth's strong interest in the phone given defendant "was alleged to have used the cell phone . . . to perpetrate the crimes" and Federal caselaw permitting some delay between seizure

and search. Id. at 818-19. But the MAC also recognized the Defendant's strong "material possessory interest" and "privacy interest," strengthened by the Defendant's use "at time of his arrest." Id. at 819. The MAC also noted that "there is no Massachusetts precedent upholding as reasonable anything remotely approaching the 123-day delay in the present case." Id. at 820. Accordingly, the MAC affirmed the trial judge's suppression order. See id. at 821-22.

- Commonwealth v. Bile, 105 Mass. App. Ct. 1123 (2025) (unpublished). Defendant was convicted of two counts of aggravated rape and his motion for a new trial based on ineffective assistance of counsel was denied. Id. at *1. At trial, defense counsel did not file a motion to suppress text messages extracted from the defendant's cell phone. Id. at *3. Police seized the cell phone without a warrant and without the defendant's consent. Id. at *2. Police obtained a warrant for the cell phone forty (40) days after the initial seizure. Id. At trial, the text messages served as the basis for the Commonwealth's case-in-chief in establishing a joint venture theory of aggravated rape and in proving the defendant's guilt. Id. at *5. On appeal, the defendant claimed that trial counsel was ineffective in failing to argue that forty days constituted unreasonable delay in obtaining a warrant. Id. at *3. The Appeals Court agreed. Id. at *3.

  Distinguishing the instant case from Commonwealth v. Cruzado, 480 Mass. 275 (2018), the court held that forty days was unreasonable delay because (1) the defendant had a strong possessory interest in his cell phone and (2) the police were not diligent in obtaining a warrant in a "relatively short" or "reasonable" time after initial seizure. Id. at *3-4. As to the first factor, the court found the defendant demonstrated a strong possessory interest in his cell phone when he declined to have his phone seized. Id. at *4. As to the second factor, there was no evidence police "put the ball in motion soon after seizing the phone" in preparing a warrant affidavit. Id. at *4. The police demonstrated a lack of diligence in obtaining this warrant in allowing forty days to pass while timely executing eight other warrants relevant to this case. Id. at *4. In conducting a balancing test, the court determined that these factors outweighed the government's strong interest in initially seizing the cell phone. Id. at *4. The court held that an ordinary, fallible lawyer would have filed a motion to suppress the text messages on this basis. Id. at *3. Next, the court held there was a reasonable probability of a different verdict if the text messages were not admitted into evidence. Id. at *5. The court emphasized the Commonwealth's reliance on the "highly prejudicial nature" of these messages during opening and closing arguments and on cross-examination of the defendant. Id. at *6. The text messages exposed conversations between and amongst the victim, the defendant, and the codefendants after the alleged rape. Id. at *6. The court reversed the order denying the defendant's motion and remanded the case to the trial court. Id. at *6.

- Commonwealth v. Williams, 103 Mass. App. Ct. 1119 (2024) (unpublished). This decision considers whether the length of time between seizure of a suspect's device and the obtaining of a warrant to search that device was reasonable. Id. at *4. In this homicide case, the defendant was found with two cell phones, a red iPhone in his hand and a black CoolPad phone in his pocket. Id. at *2. Both phones were seized by police and not returned to the defendant after questioning concluded at the station and he was released. Id. at *2. The defendant did not inquire about either

phone at that time or after. Thirty-four days later the police obtained a search warrant for one of the phones. Id. at *2.

The court upheld the suppression of the evidence discovered on the phone, finding the delay in obtaining a warrant to be unreasonable. Id. at *1. The court again emphasized its opposition to establishing a bright line rule on when delay in obtaining a warrant becomes unreasonable. Id. at *4. Instead, it followed the controlling case law on factors that can be considered. First, it is not whether officers were diligent in investigating the case in general, but instead whether they were diligent in seeking a warrant. Commonwealth v. White, 475 Mass. 583, 594 (2016). Unless police learn new information that weighs in favor of probable cause to issue a search warrant, failure to obtain a warrant when police first know of the potential importance of evidence indicates unreasonableness. Id. at *6; see also Commonwealth v Kaup, 453 Mass. 102, 109 (2009); White, 475 Mass. at 594. Extended delay in procuring a warrant for items in police custody may be permissible if police obtained the item through the owner's consent, which was absent here. Id. at *7. Consent must be explicit; failure of the defendant to object to the seizure or seek the return of the item cannot justify the delay. Id. at *7. Simply, the property interest of the defendant is not lowered based on their lack of action. Id. at *5. The court did not describe what type of police conduct might permit a delay of this kind. Instead, it continued to emphasize the fact-specific nature of this assessment and the necessary balancing of the Commonwealth's interests and the defendant's individual rights.

Of note, the court discussed an argument made by the Commonwealth that the court did not consider for procedural interests. While the police did not immediately know which phone was the defendant's, the court did not consider that fact in determining whether the delay was reasonable, because the Commonwealth did not include that argument in its brief and first raised it at oral argument. Id. at *8-*9. Thus, the court did not consider whether that would be an effective argument. Id. at *8-*9.

### (6) Timely Execution of the Warrant

General Laws Chapter 276, Section 3A, provides that "[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event not later than seven days from the date of issuance thereof . . . ." See also Fed. R. Crim. P. 41(e)(2)(A) (requiring return of a warrant within fourteen days in federal courts). Given the complexities inherent in searching digital devices, the requirement that warrants be executed within seven days of issue could prove burdensome when investigating computer crimes. Fortunately, Massachusetts courts have interpreted the provision liberally with regard to digital evidence, as the cases below demonstrate.

- Commonwealth v. Carleton, 497 Mass. 11 (2026). The defendant was convicted of first-degree murder and possession of a firearm without a license. Id. at 12. At trial, the Commonwealth's evidence included four photographs and their associated metadata from a cell phone. Id. at 26. After the cell phone was seized, the police obtained a search warrant to search the phone for photographs. Id. at 27. The day after the police obtained this search warrant, they connected the cell phone to GrayKey, a device that "continuously runs sequences until it finds the code needed

to unlock a device," then returned the search warrant six days after its issuance. Id. at 27. It took GrayKey "almost nine months" to crack the code needed to unlock the phone, then it took two additional months for Cellebrite software to extract and read the files from the phone. Id. at 27.

The SJC held that the search was not unreasonably delayed because under G. L. c. 276, § 3A, "police do not need to complete forensic analysis of a seized computer and other electronic data storage devices within the prescribed period for executing a search warrant," Id. at 28, citing Commonwealth v. Kaupp, 453 Mass. 102, 115 (2009), the cell phone was connected to GrayKey "within a day" of the search warrant's issuance, Carleton, 497 Mass. at 18, the cell phone "remained connected to GrayKey continuously for almost nine months" while GrayKey attempted to crack the code, id., and "[n]othing in the record suggests that this process could have been accomplished more quickly," id.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. Relying on the reasoning in Commonwealth v. Kaupp, 453 Mass. 102 (2009), the court concluded that "if police have obtained a warrant to search and seize evidence from a cell phone in their custody, they must *attempt* but need not *complete* a forensic examination of the device within seven days of the warrant's issuance," id. at 330 (emphasis added) (Commonwealth v. Kaupp is summarized below). The court provided no guidance about what exactly constituted an "attempt" to conduct a forensic examination.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it. Id. at 105–06. Though the Supreme Judicial Court invalidated the warrant on probable cause grounds, it noted that, had the warrant been valid, the fact that it took more than seven days to fully search the computer would not have required suppression. Id. at 114–15. The court cited other jurisdictions in support of the proposition "that the police do not need to complete forensic analysis of a seized computer and other electronic data storage devices within the prescribed period for executing a search warrant." Id. at 115. The court held that a written return listing the devices to be examined that was filed within seven days after the search warrant issued satisfied Mass. Gen. Laws ch. 276, § 3A. Id.

### (7) Manner of Executing the Warrant

"Under both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, the manner in which a search is conducted must be reasonable."

Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). The cases below deal with this requirement in the digital evidence context.

- Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810 (2013). This case dealt with the search of a defendant's email account after indictment, and the possibility of intercepting privileged communications. Id. at 811. The court held that "[w]hen an indicted defendant's e-mails are the object to be searched by the Commonwealth, because there is a risk that they contain privileged communications . . . a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege." Id. The SJC distinguished McDermott in part on the ground that the warrant in that case was issued before an indictment as part of an investigation, and the Commonwealth used preset search terms during the preliminary review of the defendant's files. Id. at 831. The court stated that it took

  > seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained.

  Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the shooting. Id. at 751, 764–65. As part of that search, they seized computers and disks. Id. at 765. The court upheld this seizure as reasonable because it recognized the impracticality of searching computers on-site. Id. at 776. It also analogized this seizure to that of a firearm, stating that it "must be listed in the inventory taken from the premises in the timely return of the warrant but it may be submitted for specialized examination at an off-site forensic setting for the further extraction of evidence." Id. (citation omitted). The court stressed the need to minimize the intrusion caused by digital searches. Id. at 777. In this case, police met that burden through the procedure they employed: "A forensic duplicate was made of the . . . hard drives and storage media to preserve all original data," and investigators used a keyword search that "resulted in a cursory inspection of only approximately 750 files . . . which amounted to less than one per cent of the defendant's files." Id. The court also suggested that "[i]n conducting the actual search . . . considerable discretion must be afforded to the executing officers regarding how best to proceed" and that "[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary." Id. at 776.

### b) Exceptions to the Warrant Requirement

"Warrantless searches are per se unreasonable unless they fall within one of the few narrowly-drawn exceptions to the warrant requirement." Commonwealth v. Durham, No. 9610398, 1998 WL 34064623, at *2 (Mass. Super. Ct. Oct. 13, 1998). "When a warrantless search is conducted, the Commonwealth has the burden of showing that the search, and any resulting seizure, falls within this narrow class of permissive exceptions." Id. The sections below examine searches incident to arrest, the plain view doctrine, and exigent circumstances in the digital evidence context.

#### (1) Search Incident to Arrest

One of the recognized exceptions to the warrant requirement is for searches made incident to a suspect's arrest. In Massachusetts, such searches are governed not only by the Fourth Amendment and art. 14 but also by Mass. Gen. Laws ch. 276, § 1, which is generally seen as more restrictive than the Fourth Amendment. See Commonwealth v. Blevines, 438 Mass. 604, 607 (2003). This statute permits searches incident to arrest "only (1) for the purpose of seizing evidence of the crime for which the arrest has been made in order to prevent its destruction or concealment or (2) for the purpose of removing any weapon the person arrested might use to resist arrest or to escape." Id. (quoting Commonwealth v. Wilson, 389 Mass. 115, 118 (1983) (internal quotation marks omitted)).

Whether the search is permissible is based on an objective standard, so an officer's subjective intent as to the search is irrelevant as long as the search could reasonably have been expected to uncover weapons or evidence facing destruction. Id. at 608 (permitting removal of defendant's car keys from his pocket during search because an officer "discovering a hard object in [a] defendant's rear pocket, [is] justified in retrieving that object as a potential weapon"). Further, having removed an item, "police need not ignore obvious aspects of or markings on" it, id. at 609 (citing Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 770 (1989)), but "detailed scrutiny" is disallowed, id. The cases below involve digital evidence in the context of a search incident to arrest.

- Riley v. California, 134 S. Ct. 2473 (2014). In two consolidated cases, law enforcement officials inspected the contents of an arrestee's cell phone—citing the search incident to arrest (SITA) exception—and used information therefrom in aid of further investigation. Id. at 2480–82. The Supreme Court held that these searches did not fall within the SITA exception because the justifications undergirding the exception did not apply to cell phones. Id. at 2484–85. First, digital contents of a cell phone cannot pose an immediate risk of physical injury to an officer. Id. at 2485–86. Second, once the phone has been seized by law enforcement (which the Court did allow), the arrestee cannot hide or destroy any evidence thereon (at least according to the Court). Id. at 2486. Confronting the issues of automatic locking, encryption, and remote wiping, the Court expressed doubt that these issues were particularly common, drew a distinction between such actions and the arrestee-initiated destruction of evidence in a typical SITA exception case, and allowed police to employ other means of preventing such actions. Id. at 2486–88 (noting that police may power off the phone or block its network connection and hypothesizing that the police may be allowed to alter a phone's settings to prevent it from locking). Finally, the Court noted

that in exceptional cases—such as an imminent threat that the phone will be remotely wiped—the exigent circumstances exception may apply on a case-by-case basis. Id. at 2487–88.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone, James provided it, and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC held that the warrantless search of the digital camera was not a valid search incident to arrest under art. 14 of the state constitution. Id. at 592–93; see also id. (declining to address the constitutionality of the search under the Fourth Amendment). The SJC applied Chimel and Riley and found the twin threats of "harm to officers and destruction of evidence" were not present with regard to the data on a digital camera. Id. at 592. The SJC reasoned that, once the camera was secured, the data on it posed no danger and the risk of destruction of evidence was mitigated (and was less of a concern with respect to digital cameras lacking network connectivity than with cell phones). Id. at 592–93.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Police apprehended the defendant after giving chase to two men. Id. at 550. Defendant claimed he was not one of the two men. Id. When asked why he was breathing heavily, he claimed to have been arguing on the phone with his girlfriend. Id. at 550–51. After he was booked, the defendant placed a phone call he claimed was

to his girlfriend. Id. at 551. Police then examined his cell phone call log about five hours after the arrest, without obtaining a warrant; the log belied both of defendant's statements. Id. The booking sergeant testified that it could take several days to get a warrant, and that he was concerned that incoming calls would "push out" previous calls on the call log, which he believed permitted only a limited number of calls. Id. The SJC held that under Riley (described above), decided a year earlier, the search of the call log was not a proper search incident to arrest and was not justified by exigent circumstances. Id. at 557. The SJC found that—absent testimony suggesting the phone was password protected or that police were concerned about remote wiping—preservation of the call log could have been achieved by "turning the cell phone off, placing the cell phone in a Faraday bag, or securing the cell phone and seeking a warrant for it." Id. at 558–59.

### (2) The Plain View Doctrine

Under the plain view doctrine, law enforcement may make a warrantless seizure of evidence when four conditions are met. See Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 333 (2014) (explained below). First, the officers must lawfully be in a position to view the evidence. Id. Second, they must have a lawful right of access to the object. Id. Third, they must have a reason for seizing it. Id. In cases concerning (a) items possessed illegally, the incriminating character of the object should be immediately apparent. Id. (citing Horton v. California, 496 U.S. 128, 136 (1990) (explained below)). In cases concerning (b) other types of evidence, the particular evidence must plausibly be related to criminal activity of which the police are already aware. Id. (citing Commonwealth v. Sliech-Brodeur, 457 Mass. 300, 306–307 (2010)). Fourth, art. 14 requires that police come across the object inadvertently. Id. (citing Sliech-Brodeur, 457 Mass. at 307). The following cases address the plain view doctrine in the digital evidence context.

- Commonwealth v. Yusuf, 488 Mass. 379 (2021). A police officer responded to a domestic disturbance request and entered the home of the defendant. Id. at 381. The officer was equipped with a body-worn camera that recorded the inside of the defendant's home as the officer moved through it. Id. A gang unit from the same department, conducing a distinct investigation, downloaded and viewed the body-worn camera video from the domestic violence response. Id. at 383. The review of that footage resulted in one or more observations that were then used in support of an application to obtain a search warrant for the defendant's home. Id. at 383-84. The defendant moved to suppress the evidence obtained during the execution of the warrant and argued that the application for the warrant was based on information gathered through one or more unlawful searches. Id. at 385. The SJC held that the use of the body-worn camera was not a search in the constitutional sense, but the subsequent, warrantless review of the footage for an unrelated matter was an unlawful search. Id. at 389, 396. The initial use of the body-worn camera fell under the plain view doctrine, as the officer was lawfully present in the defendant's home, the officer stayed within the locations of the home relevant to his duties, and the body-worn camera merely recorded the officer's plain-view observations. Id. at 387-88. The permissible use of the body-worn camera did not, however, allow the police to subsequently review the footage without a warrant and for an unrelated investigation, because such a review would be the virtual equivalent of a general warrant and would be unrelated to the purposes of body-worn cameras, such as ensuring police accountability. Id. at 391-96.

- Commonwealth v. Tarjick, 87 Mass. App. Ct. 374 (2015). Defendant's stepdaughter disclosed he abused her and took sexually explicit photos/made recordings of her. Id. at 375. Police obtained a warrant authorizing the search of the defendant's home and the seizure of the defendant's cell phone, the family computer, and the family video camera. Id. Three memory cards that were in the camcorders or digital cameras were also seized when the warrant was executed, though they were not included in the warrant. Id. A second warrant was obtained to search the contents of the memory cards and evidence from the cards was later used at trial. Id. at 375–76. The Appeals Court held that the seizure was within the plain view exception. Id. at 378. The cards, though not included in the original warrant, were plausibly related to the crime. Id. "The officers were . . . aware that data may be freely transferred from one device to another through memory cards, and they could reasonably have concluded that the memory cards might have contained the alleged recordings." Id. The inadvertence requirement was also satisfied because there was "no indication that the police had probable cause to believe, prior to the search, that these specific memory cards or the cameras containing them would be found." Id.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. On appeal, the court upheld this seizure under the plain view doctrine. Id. at 333. Fulfilling the first and second plain view requirements, the warrant authorizing seizure of the tank top image means the police "were lawfully situated to view and to secure the [penis] images" because police are authorized to conduct cursory inspection of computer files to determine whether they match items listed in the warrant. Id. at 333–34 (citing Commonwealth v. McDermott, 448 Mass. 750, 776–77 (2007)). Third, the images of the defendant's penis were plausibly related to criminal activity of which the police were aware. Id. at 334. The defendant's statements of intent to exchange pictures of his nude body with pictures of the minor gave police reasonable ground to believe the pictures were evidence of enticing the minor to pose in a state of nudity. Id. The same statements made it plausible that the pictures were evidence of possession of matter harmful to minors with intent to disseminate. Id. Fourth, police discovered the images inadvertently because they "lacked probable cause to believe, prior to the search, that specific items would be discovered during the search." Id. (quoting Commonwealth v. Balicki, 436 Mass. 1, 9–10 (2002)).

- United States v. Burdulis, No. 10–40003–FDS, 2011 WL 1898941 (D. Mass. May 19, 2011). Defendant in this case emailed a police officer impersonating a young boy an explicit image. Id. at *1. Police obtained a warrant to search the defendant's computer. Id. at *2. During their search of image files on the computer, police uncovered child pornography. Id. After finding the seizure of those images authorized by the initial warrant, the court held in the alternative that the plain view doctrine also authorized the use of those images in evidence. Id. at *11–12. First, the officer

searching the computer was lawfully in a position to view the evidence because he was conducting a search pursuant to a warrant. Id. at *11. As he was looking for image files, he was authorized to briefly examine all images to determine if they were a match. Id. Second, by this same logic, the officer had a lawful right of access to the files. Id. at *12. Third, the prohibited nature of child pornography images would have been immediately apparent. Id. [The court did not examine the fourth requirement—inadvertence—because it exists only under Massachusetts law. See above for more detail on inadvertence.]

### (3) Exigent Circumstances

"One well-recognized exception [to the warrant requirement] applies when 'the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" Kentucky v. King, 563 U.S. 452, 460 (2011) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)). Among the exigencies that the Court has identified in the context of searching a home are "emergency aid" (entering a home to render assistance to an injured occupant), "hot pursuit" (chasing after a fleeing suspect), and the need to prevent the "imminent destruction of evidence." Id.

- Commonwealth v. McCarthy, 495 Mass. 736 (2025). Defendant's cell phone was seized outside his residence in Nashua, New Hampshire by a Lowell, Massachusetts police detective. Id. at 738. The defendant's motion to suppress the evidence found on his cell phone was granted. Id. at 739. On appeal, the Commonwealth challenged the motion judge's conclusion that the detective lacked extraterritorial authority to seize the phone. Id. at 739. The SJC noted that if all the events had occurred in Lowell "the warrantless seizure of the defendant's telephone would have been constitutionally permissible." Id. at 739. Because the seizure was in Nashua and the Lowell detectives did not act pursuant to one of the recognized exceptions for extraterritorial authority, the SJC affirmed the allowance of the motion to suppress. Id. at 745.

  The court discussed one of the exceptions in greater depth: extraterritorial authority at common law. Id. at 743. This exception posed the question of whether a private citizen had the authority to make a "citizen's seizure" of the cell phone. Id. at 743. The SJC differentiated between a "citizen's arrest" and the novel theory of a "citizen's seizure" of another's property. Id. at 743. The court noted that the Lowell detectives "could have affected a citizen's arrest under New Hampshire law" for the destruction of evidence. Id. at 743. However, they (1) did not make any such arrest and (2) a private New Hampshire citizen would not be authorized to seize another's property "in the absence of" a citizen's arrest. Id. at 743-744.

- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020). Police seized defendant's phone, then answered an incoming call to the phone approximately one hour and fourteen minutes after the seizure. Id. at 437–48. The Commonwealth argued that exigent circumstances justified answering the call, but it did not offer "any evidence that it was impracticable to obtain a search warrant before the call was received." Id. at 441. The court allowed defendant's motion to suppress the call and evidence derived from it, explaining that "because there [was] no evidence in the record that obtaining a warrant was impracticable here, the Commonwealth failed to meet its burden of

showing exigency, and [the court was] constrained to conclude that the motion to suppress should have been allowed." Id. at 442. The court noted, however, that the burden to show that it was impracticable to obtain a search warrant in one hour and fourteen minutes was not a heavy one and could potentially have been met by an officer's testimony about the steps necessary to obtain a warrant. Id. This case indicates that courts are unlikely to treat a "one hour or two hour time frame" as *by itself* sufficient to justify a search under exigent circumstances, id. at 439, but leaves open the possibility that the same search might have been found justified had the government produced evidence showing why that short timeframe made obtaining a warrant impracticable. Id. at 442 (but see Alvarez, 480 Mass. 1017 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer and absent any argument by the defendant that "observation of the outside of the… phone constituted a search")).

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police found a cell phone lying near the defendant in a stairwell. Id. at 282. Having probable cause, the police seized the cell phone. Id. The Supreme Judicial Court held that "exigent circumstances supported the warrantless seizure: the risk of someone taking or tampering with the cell phone. Left unattended, especially in an area to which many people had access, the cell phone would have been at the risk of theft or vandalism." Id. at 283.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Possible degradation of a call log on a cell phone was deemed not an exigent circumstance because such degradation could be prevented in a number of different ways, such as by turning off the phone. Id. at 558–59.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's (a teacher) computers in a school classroom. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized both computers and subsequently obtained a search warrant. Id. at 105. The court upheld the seizure of defendant's computer as appropriate because of exigent circumstances. Id. at 105–06. Specifically, the court noted that "impoundment of an object pending the issuance of a search warrant violates the Fourth Amendment . . . only if it is unreasonable," which "turns on the facts of each case, requiring courts to 'balanc[e] the need to search or seize against the invasion that the search or seizure entails.'" Id. at 106 (quoting Commonwealth v. Catanzaro, 441 Mass. 46, 55–56 (2004)). The court held that "[g]iven the ease with which computer files may be accessed and deleted, and the disruption that would have been created by posting an officer in the defendant's office and preventing students from entering pending the issuance of a search warrant . . . the seizure was reasonable." Id. In a footnote, the court noted that while exigent circumstances justified the seizure, they would not have justified the subsequent search had it been warrantless because "[t]he exigency necessitating [the computer's] seizure dissipated once the computer had been secured." Id. n.7.

### (4) Emergency Aid Exception

The emergency aid exception to the warrant and probable cause requirements originated in the context of searching a home, "permit[ting] the police to enter a home without a warrant when they have an objectively reasonable basis to believe that there may be someone inside who is injured or in imminent danger of physical harm." Commonwealth v. Peters, 453 Mass. 818, 819 (2009). The exception has since been extended to "uphold warrantless searches of places other than homes, in order to find and assist a victim of serious physical harm or to prevent such harm from occurring," and most recently to searches of the digital information. Commonwealth v. Raspberry, 93 Mass. App. Ct. 633, 639-40 (2018).

- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018). Police officers listening to a wiretap had "grave concerns about the defendant imminently causing serious bodily harm" to another with a firearm. Id. at 635 (internal quotation marks omitted). To locate the defendant and prevent the harm, police "asked AT&T to perform 'emergency pings' and give the police real-time CSLI about the approximate location of the defendant's cell phone." Id. The Commonwealth did not contest that a Fourth Amendment "search" took place, instead arguing that the "search" was "reasonable" under the emergency aid doctrine. See id. at 638, 640. The Massachusetts Appeals Court agreed. See id. at 641 ("We have no difficulty concluding that these standards were met here . . . What police did not know here, at the time of the call, was the whereabouts of the defendant. In the circumstances, it was objectively reasonable for the police to request real-time CSLI, in order to determine the defendant's current location and the direction in which she was moving, and thus to find and intercept her before she could shoot Dorsey.").

The emergency aid exception differs from the exigent circumstances exception: the former requires no probable cause to conduct a search, whereas the latter permits a warrantless search where probable cause exists but the circumstances make obtaining a warrant impracticable. Raspberry, 93 Mass. App. Ct. at 638, n. 8.

### (5) Inventory Exception

Seizures of items on an arrestee's person may also be permissible, subject to police inventory policies. "[B]efore a person is placed in a cell, the police, without a warrant, but pursuant to standard written procedures, may inventory and retain in custody all items on the person . . . ." Commonwealth v. Seng, 436 Mass. 537, 550 (2002). For such seizure to be lawful, police must follow the rules of a written inventory policy that is "explicit enough to guard against the possibility that police officers would exercise discretion with respect to whether to open closed [containers] as part of their inventory search." Commonwealth v. Rostad, 410 Mass. 618, 622 (1991). "Inventory searches are intended to be noninvestigatory and are for the purpose of safeguarding the defendant's property, protecting the police against later claims of theft or lost property, and keeping weapons and contraband from the prison population." Barillas, 484 Mass. at 256. As such, "[i]n making an inventory — taking from the person, noting what is received, and placing it in safekeeping — the police are to act more or less mechanically, according to a set routine, for to allow then a range of discretion in going about a warrantless search would be to invite conduct which by design or otherwise would subvert constitutional requirements." Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 772 (1989) (cited in Barillas, 484 Mass. at 259).

Investigatory use of items seized under the inventory exception is impermissible unless the police have a search warrant or "obtain consent from the appropriate person (as determined by the inventory policy)." Barillas, 484 Mass. at 257. Any evidence resulting from investigatory use of inventory items without consent or a warrant is subject to suppression. Id.

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC rejected the argument that the search of the camera was a valid inventory search, holding that it was instead investigatory in nature because the camera was suspected stolen and the search was meant to identify the owner. Id. at 595–96.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found the defendant hiding in his home, conducted a pat frisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

### (6) Consent

Warrantless searches are permissible with appropriate advance consent.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a pat frisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James,

who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77. The court further held that the consent search of the defendant's residence was tainted by the illegal CSLI search. Id. at 71. Believing that the defendant and a second individual were transporting narcotics from Florida to Massachusetts, police obtained a court order pursuant to 18 U.S.C. § 2703 (2006) requiring the second individual's cellular service provider to "ping" the location of his cell phone. Id. at 73-74. After the two returned to Massachusetts, police knocked on the defendant's door and told him they knew he had just "purchased a large amount of narcotics" in Florida and was possibly storing it at his apartment. Id. at 74. The defendant then consented to a search, and police discovered a large amount of cash and two bricks of cocaine in his residence. Id. at 75. The SJC considered three factors in determining whether the defendant's consent was attenuated from the tainted CSLI data: "(1) the amount of time that elapsed between the defendant being confronted with the illegally obtained CSLI evidence and his grant of consent; (2) the presence of any intervening circumstances during that time period; and (3) the purpose and flagrancy of the official misconduct." Id. at 81-82 (internal quotes omitted). As to factors (1) and (2), the court held that the lack of time and intervening events between the acquisition of the CSLI data and the police officer's confrontation with the defendant claiming that he had just returned from Florida with drugs weighed heavily against attenuation. Id. at 82-83. As to factor (3), while the court "recognize[d] that the illegal police misconduct here was neither purposeful nor flagrant," it was still not dispositive in attenuating defendant's consent from the tainted CSLI data. Id. at 84. In her dissent, Justice Cypher explained that she would not reach the conclusion of the majority that a passenger in a tracked car has standing to challenge a CSLI search. Id. at 86 n.1 (Cypher, J.,

concurring in part and dissenting in part). In addition, she encouraged the SJC to adopt the good faith exception to the exclusionary rule in cases where the police acted under a "reasonable good faith belief that their conduct was lawful at the time." Id. at 92. While Justice Lowy agreed that Massachusetts should adopt a good faith exception, he did not believe the issue was properly raised by the Commonwealth in this case. Id. at 85-86 (Lowy, J., concurring).

#### c) Allegations of Selective Enforcement/Racial Discrimination

Under Commonwealth v. Long, 485 Mass. 711 (2020), if an inference of selective enforcement, such as a racially discriminatory stop or search, is successfully raised, the Commonwealth must rebut that inference to prevent suppression of the evidence obtained as a result of that stop or search. This principle has been applied to searches and seizures of digital evidence that are alleged to the result of selective enforcement.

- Commonwealth v. Rodriguez, 496 Mass. 627 (2025). A member of the Lowell police department's gang unit created an undercover profile on Snapchat, a social media platform. Id. at 628. The officer became Snapchat "friends" with defendant. Id. at 628. The defendant later posted a video in which he "discharge[ed] a firearm out the window of a car." Id. at 628. Police "subsequently used that data to locate the defendant in the suspect vehicle[.]" Id. at 630. After obtaining a search warrant to search the vehicle, "police found a firearm" and "spent shell casings [matching those] at the location of the shooting." Id. at 630.

  Defendant was charged with, and ultimately pled guilty to, various firearms-related offenses. Id. at 628. In a motion to suppress, the defendant argued that the "officer's Snapchat investigation of the defendant was racially motivated" selective enforcement and, thus, the Snapchat video evidence was "obtained in violation of [the defendant's] equal protection rights." Id. at 628.

  On appeal, the SJC held that "the defendant successfully raised a reasonable inference of selective enforcement under the 'totality of the circumstances' test" of Commonwealth v. Long, 485 Mass. 711 (2020). Id. at 628. First, the SJC noted that the officer used a "nonwhite" username and bitmoji while representing himself as "nonwhite." Id. at 635. Second, the officer characterized neighborhoods with high gang activity as having "a variety of cultures." Id. at 635. Third, the SJC noted that the Lowell police department did not have procedures governing social-media monitoring, and all five persons charged by the department because of Snapchat monitoring appeared to be "exclusively nonwhite." Id. at 636. Accordingly, the SJC remanded for "a further evidentiary hearing" where the Commonwealth "will have the burden of rebutting the inference of selective enforcement[.]" Id. at 628.

### 3. The Exclusionary Rule

Generally, the exclusionary rule prohibits the introduction of evidence obtained as a result of a violations of the Fourth, Fifth and Sixth Amendments to the U.S. Constitution, and their counterparts under the Massachusetts Declaration of Rights. See Commonwealth v. Lora, 451 Mass. 425, 439 & n.26 (2008).

### a) Good Faith / Substantial and Prejudicial

The Supreme Court has limited the application of the exclusionary rule in federal cases where officers acted in good faith, but Massachusetts does not recognize the good faith exception under art. 14. See Commonwealth v. Porter P., 456 Mass. 254, 273 (2010). Instead, it looks to "the foundational purpose of the rule—to deter unlawful police conduct . . . as a guiding principle" to determine whether evidence should be excluded. Commonwealth v. Maingrette, 86 Mass. App. Ct. 691, 697 (2014) (citing Commonwealth v. Wilkerson, 436 Mass. 137, 142 (2002)). Where:

> an arrest is wrongly made on the basis of mistaken information chargeable solely to the police, the burden is on the government to show . . . that the [government's] mistake was reasonable in the circumstances, and that the violation was minor or insubstantial and nonprejudicial and that exclusion of the evidence would not be likely to deter future police misconduct.

Id. (citations omitted).

### b) Inevitable Discovery

> "Under the inevitable discovery doctrine, if the Commonwealth can demonstrate by a preponderance standard that discovery of the evidence by lawful means was certain as a practical matter, the evidence may be admissible as long as the officers did not act in bad faith to accelerate the discovery of evidence, and the particular constitutional violation is not so severe as to require suppression."

Commonwealth v. Fontaine, 84 Mass. App. Ct. 699, 709 (2014) (citation omitted). Though there are no Massachusetts cases applying this doctrine to a computer search, the First Circuit case below applying a slightly different federal test is instructive:

- United States v. Crespo-Rios, 645 F.3d 37 (1st Cir. 2011). In this case, the FBI searched the defendant's computer and external hard drive for evidence of chats between both him and an undercover agent and him and minors. Id. at 40–41. The search for these chats was conducted pursuant to a warrant that also listed, among other things, child pornography as something being sought. Id. at 40. During this search, agents found child pornography. Id. Following his indictment, the defendant moved to suppress the evidence, arguing that there was insufficient probable cause to support the overly-broad search warrant. Id. at 41. The First Circuit overturned the lower court by applying the inevitable discovery doctrine. Id. at 42-44. In searching the computer and hard drive for the chat evidence—for which there was undoubtedly probable cause—the court found that government agents would inevitably have discovered the child pornography because searching for computer files allows brief scanning of all possibly relevant files on the computer. Id. [This analysis is quite similar to that of the plain view doctrine, discussed elsewhere in this guide.]

## B. Search of Electronic Service Providers

### 1. General Overview of Stored Communications Act

In 1986, Congress enacted the Stored Communications Act (SCA). See Pub. L. 99-508, 100 Stat. 1848, Title II. It provides limited privacy protections to the customers of "electronic communication service[s]" (ECS) and "remote computing services" (RCS). Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 383 (2014). ECS providers are email services like Gmail or Yahoo! along with certain elements of social media platforms, like a user's Facebook "wall." See generally Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 8–11 (2013).

RCS providers are harder to define and include any company that provides "computer storage or processing services by means of" the Internet to the public. Pub. L. 99-508, 100 Stat. 1848, § 2710. Cloud storage providers like Dropbox clearly fit this definition. Jeffrey Paul DeSousa, Self-Storage Units and Cloud Computing, 102 Geo. L.J. 247, 250 n.19 (2013). Courts have also found that YouTube belongs in this category. Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 11 (2013).

For a discussion of the argument that text messaging services are "remote computing services" under 18 U.S.C. § 2703(b) see Commonwealth v. Fulgiam, 477 Mass. 20, 31–33 (2017). The SJC held that the Commonwealth may not obtain the content of text messages without a warrant because text messaging is an "electronic communication service" subject to the requirements of § 2703(a). Id. at 32–33. The SJC also decided that a warrant supported by probable cause was also required for the content of text messages under art. 14. Id. at 33–34.

### 2. Search warrants served on out-of-state Internet service providers

Out-of-state corporations providing ECS or RCS to Massachusetts residents are subject to the jurisdiction of Massachusetts courts and must comply with search warrants issued by them. See Mass. Gen. Laws ch. 276, § 1B (2018); see also 18 U.S.C. § 2703 (2018) (outlining process by which state courts exercise jurisdiction over ECS and RCS providers).

## C. Encryption and Self Incrimination

### 1. The Foregone Conclusion Doctrine

The Fifth Amendment to the United States Constitution states, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." This does not mean that a defendant cannot be compelled to produce some types of incriminating evidence, however, because only compelled *testimonial* communication that incriminates is barred. See Commonwealth v. Gelfgatt, 468 Mass. 512, 519 (2014) (citing Fisher v. United States, 425 U.S. 391, 408 (1976)). Written or oral communication created in response to government demand is plainly testimonial. See id. at 520. Compelled action that communicates something can also be testimonial in nature. Id.

"Whether an act of production is testimonial depends on whether the government compels the individual to disclose 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Gelfgatt, 468 Mass. at 520 (quoting United States v. Hubbell, 530 U.S. 27, 43 (2000)). For example, giving blood, producing a voice exemplar, or standing in a lineup are all nontestimonial because the suspect in question "is not required to disclose any knowledge he might have, or to speak his guilt." Id. at 521 (citations omitted). By contrast, complying with the government's demand could be testimonial "where [the act of production] is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence." Id. (citing Hubbell, 530 U.S. at 36 & n.19).

Even in cases where the act of producing evidence that the government seeks to compel is testimonial, however, that production loses its testimonial character if the information that would be disclosed by the production is a "foregone conclusion." Id. at 522. The forgone conclusion exception obtains "where the facts conveyed already are known to the government, such that the individual 'adds little or nothing to the sum total of the Government's information.'" Id. (quoting Fisher, 425 U.S. at 411). In other words, "the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production." Commonwealth v. Jones, 481 Mass. 540, 547 (2019).

Several State and Federal courts have "applied the foregone conclusion exception in the context of compelled decryption," but neither the United States Supreme Court nor the courts of appeals have ruled on the government's burden of proof that applies to the "foregone conclusion" exception under the Fifth Amendment. Jones, 481 Mass. at 550. One federal district court "concluded that the appropriate standard of proof under the Fifth Amendment is clear and convincing evidence. Id. (citing United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018).

- In re a Grand Jury Investigation, 92 Mass. App. Ct. 531 (2017). During a grand jury investigation, a judge ordered petitioner to enter his personal identifying number (PIN) access code into his iPhone smartphone. Id. at 532. A warrant had previously issued for a search of the phone. Id. The Appeals Court held that production of the PIN was within the foregone conclusion exception to the Fifth Amendment. Id. at 534. To meet its burden under the doctrine, the prosecution had to demonstrate knowledge of the ownership and control of the cell phone and its contents, as well as "knowledge of the fact of [PIN code protection], and knowledge of the [existence of the PIN code]." Id. (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 524 (2014)). The prosecution was not required to show that it knew the specific content of the cell phone, but it did need to demonstrate knowledge of the existence and the location of the content. Id.

Article Twelve (art. 12) of the Massachusetts Declaration of Rights—analogous to the Fifth Amendment—provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself." Article Twelve provides greater protection than the Fifth Amendment in some contexts, but this broader protection "does not change the classification of evidence to which the privilege applies," so only "testimonial or communicative" evidence is protected from compelled disclosure. Commonwealth v. Gelfgatt, 468 Mass. 512, 525 (2014) (citations omitted). Massachusetts also recognizes the "foregone conclusion" exception to art. 12. Id. at 526.

For the exception to apply in the context of an order compelling decryption of an electronic device, Article Twelve requires that "the Commonwealth . . . prove beyond a reasonable doubt that the defendant knows the password." Commonwealth v. Jones, 481 Mass. 540, 552. But the Commonwealth does not need to "prove any facts with respect to the contents" of the device to be decrypted. In addition, "the entry of the password alone does not convey the fact of 'ownership' of the device or its contents." Id. at 547 n.8.

### 2. Encryption

In an affidavit the Commonwealth submitted in Gelfgatt, the director of the Massachusetts Attorney General's computer forensics laboratory explained that "encryption" is:

> the process by which 'readable' digital media, that is, digital media or data that can be viewed and accessed, is scrambled in such a way as to render that digital media or data 'unreadable' without decryption. Encryption can be performed both by hardware and by means of software tools.

Commonwealth v. Gelfgatt, 468 Mass. 512, 516 n.9 (2014). The director described "decryption" as:

> the process by which encrypted, scrambled data is rendered 'readable' again. In order to decrypt data, the person seeking decryption performs some action such as the entering of a password, scanning of a fingerprint or [insertion of] a USB Thumb drive with a pass code key on it. The encryption software then translates this action into a 'key,' essentially a string of numbers or characters. The encryption software then applies this key to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again.

Id. In Gelfgatt, the Commonwealth represented that the defendant's encryption software was virtually impossible to decrypt. Id. at 516–17. The Commonwealth represented that files thus encrypted could only be viewed if an authorized user entered a password. Id. at 517. But compelling the user to enter or disclose their password presents a possible violation of the Fifth Amendment and art. 12. The Gelfgatt court examined the interplay of these issues in Massachusetts:

- Commonwealth v. Gelfgatt, 468 Mass. 512 (2014). Defendant in this case was allegedly involved in a mortgage fraud scheme. Id. at 513. Law enforcement believed proof of that scheme would be found on the defendant's computers, and they obtained a search warrant, but encryption on the computers foiled their search. Id. at 516–17. When interviewed by police, the defendant admitted to owning multiple computers, stated that the police would be unable to access them because they were encrypted, and stated that he was able to decrypt the computers but refused to do so. Id. at 517. The lower court found that compelling him to do so would violate his Fifth Amendment and art. 12 rights against self-incrimination. Id. at 518–19. The SJC reversed and held that he could be

compelled to enter his password in the circumstances presented by this case. Id. at 519–26.

First, the court stated that compelling a defendant to enter a decryption password, in the abstract, implicated the Fifth Amendment because the defendant would be implicitly "acknowledging that he has ownership and control of the computers and their contents," which could itself be relevant to the Commonwealth's case against him. Id. at 522. Next, the court considered the "foregone conclusion" exception (explained above) and held that it applied because the defendant had already admitted to owning multiple computers, that their contents were encrypted, and that he was capable of decrypting them. Id. at 523-24. As a result, the facts that would have been communicated by compelling him to decrypt the computers were already known to the government, making them a foregone conclusion. Id. Finally, the court examined the issue under art. 12 but held that the same analysis applied. Id. at 524–26. [Note: Crucially, the Commonwealth proposed a protocol for decrypting the files that limited the scope of what was communicated through the compelled decryption. That protocol is outlined above.]

- Commonwealth v. Jones, 481 Mass. 540 (2019). Defendant was charged with trafficking a person for sexual servitude, Mass Gen. Laws ch. 265, § 50(a) (2018); id. at 541, and deriving support from the earnings of a prostitute, Mass. Gen. Laws ch. 272, § 7 (2018); id. at 541. The Commonwealth seized an LG cell phone from the defendant at his arrest and later obtained a warrant to search the phone. Id. at 541, 544. The LG phone had to be decrypted with the entry of a password before the search could be executed. Id. at 541. The Commonwealth moved for a Gelfgatt order, compelling the defendant to decrypt the LG phone under the "forgone conclusion" exception to the privilege against self-incrimination under the Fifth Amendment to the U.S. Constitution and Article 12 of the Massachusetts Declaration of Rights. Id. at 541–42. The SJC found that in order to obtain a Gelfgatt order compelling a defendant to decrypt an electronic device, the Commonwealth must "prove that the defendant knows the password beyond a reasonable doubt for the foregone conclusion exception to apply." Id. at 542–43. The court also concluded that the Commonwealth met its burden in this case. Id. at 543. Finally, the SJC concluded that judges can consider new information in deciding renewed Gelfgatt motions, "without first finding that [the new information] was not reasonably available to the Commonwealth at the time the earlier Gelfgatt motion was filed." Id.

  To meet its burden of proving beyond a reasonable doubt that the defendant's knowledge of the password was a "foregone conclusion," the Commonwealth offered the following evidence: a witness testified to the defendant's regular use of the LG phone to answer calls and communicate through text messages (the record revealed several communications between the witness's phone and the LG phone related to prostitution); the defendant's phone number was listed with his name in the witness's contacts; the LG phone was in the defendant's possession at the time of arrest; the defendant had characterized the telephone number of the LG phone as his number to police when he was being booked following an arrest in an unrelated matter; police records showed that a backup number listed for the LG phone was registered to a person with the same name, social

security number, and date of birth as the defendant; CSLI records revealed that the LG phone was in the same location at the same time as another phone that was found to be the defendant's phone. Id. at 556–57. All of this evidence, "taken together with the reasonable inferences drawn therefrom, prove[d] beyond a reasonable doubt that the defendant [knew] the password to the LG phone." Id. at 557 (noting that "it is hard to imagine more conclusive evidence" showing that the defendant knows the LG phone's password). The SJC also noted that even if the LG phone was used by more than one person, proof of ownership or exclusive control was not required. Id. at 547 n.8.

### 3. Sample Decryption Protocol

In Commonwealth v. Gelfgatt, the Commonwealth employed the following protocol to limit the amount of information that would be communicated by the compelled decryption:

> 1. The defendant, in the presence of his counsel, shall appear at the [Digital Evidence Laboratory] of Massachusetts Attorney General [Andrea Campbell] within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
>
> 2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
>
> 3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
>
> 4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
>
> 5. The defendant is expressly ordered not to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program;
>
> 6. The Commonwealth shall not view or record the password or key in any way; [and]
>
> 7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter.

Id. at 517 n.10.

## D. Searches Implicating Attorney-Client Privilege

Searches that may intercept privileged communications between a suspect and his lawyer should be handled with special care. See generally Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 811 (2013). This problem is especially acute when a search is executed after a suspect has already been indicted and retained counsel. See, e.g., id. Even when a post-indictment search targets a different crime than the one for which the defendant was indicted, such a search runs a risk of encountering privileged communications. Id. at 817–18. The section below detail how such a search should proceed in Massachusetts.

### 1. Post-Indictment Email and File Searches

The Commonwealth may seize emails of a defendant under indictment by means of an ex parte search warrant. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 821–22 (2013). Because of the sensitive nature of such a seizure, however, "only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment." Id. at 822. The affidavit supporting the warrant application must inform the judge at the outset that the subject of the email search is under indictment and must explain the connection, if any, between the indictment and the search warrant being sought. Id. Finally, the affidavit must explain why a search warrant rather than a rule 17(a)(2) summons is necessary to obtain the emails. Id. One possible explanation the SJC has suggested is cases where the Stored Communications Act requires a warrant, which it does for emails not yet opened that are 180 or less days old. See id. at 819 n.17 (citing 18 U.S.C. § 2703(a)), 822.

Once seized, emails possibly containing privileged material may be searched only after the Commonwealth receives a Superior Court judge's approval of a search protocol including specific procedures to protect against searches of privileged communications between a defendant and his attorneys. Id. at 823. One such procedure that the court has approved is laid out below in the "Taint Team" section.

### 2. Taint Teams

A "taint team" is a group of attorneys or agents employed by a government office who have not at any time been involved in the investigation and/or prosecution of the defendants and who will not be assigned to any such investigation or prosecution in the future who sort the defendant's communications into privileged and unprivileged so that the latter group may be investigated by the government without eroding a defendant's attorney-client privilege. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 824–25 (2013).

There is "widespread skepticism" about the ability of government agents to properly review privileged communications without affecting that privilege, id. at 825, but the SJC has concluded that taint teams can "offer adequate protection to the Commonwealth's citizens," id. at 827. To that end, the SJC has put in place a two-tiered set of requirements surrounding the use of taint teams.

First, before a judge may authorize a team that will use members of a prosecutor's office as its members, "the Commonwealth must establish the necessity of doing so" because "use of an independent

special master offers a far greater appearance of impartiality and protection against unwarranted disclosure and use of an indicted defendant's privileged communications." Id. at 829. In ruling on the prosecution's request to use a taint team, "the judge may consider factors such as the number of documents to be searched, the relative cost of a special magistrate, and the Commonwealth's unique ability to perform such a search due to specialized computer forensic examiners in its employ." Id. Further, the judge will consider "the Commonwealth's ability to erect an impenetrable wall between members of the taint team and members of the prosecution team." Id. at 829–30. In making this determination, the judge will consider "the size of the particular prosecutor's office," and the court expressed "less confidence that a small District Attorney's office can screen off members of the taint team as effectively as the Attorney General's office may be able to do." Id. at 830.

> Second, to pass constitutional muster, the taint team must comply with each of four requirements:
>
> (1) the members of the taint team must not have been and may not be involved in any way in the investigation or prosecution of the defendants subject to indictment—presently or in the future; (2) the taint team members are prohibited from (a) disclosing at any time to the investigation or prosecution team the search terms submitted by the defendants, and (b) disclosing to the investigation or prosecution team any e-mails or the information contained in any e-mails, subject to review until the taint team process is complete and in compliance with its terms; (3) the defendants must have an opportunity to review the results of the taint team's work and to contest any privilege determinations made by the taint team before a Superior Court judge, if necessary, prior to any e-mails being disclosed to the investigation or prosecution team; and (4) the members of the taint team must agree to the terms of the order in writing.

Id. at 828.

### 3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails)

"'Generally, disclosing attorney-client communications to a third party undermines the privilege.'" Dahl v. Bain Capital Partners, LLC, 714 F. Supp. 2d 225, 227 (D. Mass. 2010) (quoting Cavallaro v. United States, 284 F.3d 236, 246–47 (1st Cir. 2002)).

"'An exception to this general rule exists for third parties employed to assist a lawyer in rendering legal advice,'" including CC'ed emails. Id. at 227 (quoting Cavallaro, 284 F.3d at 247). In order for the exception to obtain, three criteria must apply: (1) the communication must be "necessary, or at least highly useful" for effective consultation between client and lawyer; (2) the exception only applies if the third party is playing an interpretive role between the lawyer and client (e.g., an accountant if he is helping the lawyer understand complex financial information); and (3) the communication must be made for the purpose of rendering legal advice, and not business advice or otherwise. Id. at 227–28.

# II. Evidentiary Matters

## A. Judicial Discretion

### 1. Trial Judge's Discretion

"A judge has broad discretion in the admission" of "demonstrative aids, including digital photographs and computer-generated images." Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing Commonwealth v. Noxon, 319 Mass. 495, 536 (1946)).

For an example of related flawed evidentiary practice, see Commonwealth v. Mienkowski, 91 Mass. App. Ct. 668 (2017). At a trial for aggravated rape of a child, posing a child in a state of nudity, and of dissemination of matter harmful to minors, the defendant's cell phone was admitted into evidence. Id. at 669. After some initial ambiguity about how the jury could examine the phone during deliberation, the judge adopted the Commonwealth's position and instructed the jury to limit their examination to the evidence already admitted (screenshots of relevant text messages). Id. at 675–77. On appeal, the defendant argued that the judge's initial admission of the cell phone without limitation and statements he made at the charge conference led defense counsel to rely in her closing on the jury's ability to examine the cell phone unconstrained and then "cut the legs out from under" her argument. Id. at 677–78. The SJC found it was possible that "neither the litigants nor the judge fully had considered the plethora of difficult issues that may be raised when a cell phone containing troves of unidentified electronic data is delivered into a jury's hands." Id. at 678. Though it held that it would have been preferable to resolve the ambiguity earlier, the SJC found no reversible error in the judge's handling of the issue. Id. at 678–69.

### 2. Demonstrative Photographs

"When, as here, the demonstrative photograph is generated as a digital image or video image, the judge must determine whether the image fairly and accurately presents what it purports to be, whether it is relevant, and whether its probative value outweighs any prejudice to the other party." Renzi v. Paredes, 452 Mass. 38, 52 (2008) (citing Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006)). "Concerns regarding the completeness or production of the image go to its weight and not its admissibility." Id. (citing Leneski, 66 Mass. App. Ct. at 295–96).

## B. Discovery

### 1. Pornographic Images in Child Pornography Cases

"That forensic examination of the computer data by an expert retained by the defense is an essential component of effective assistance of counsel" in a child pornography case "is self-evident." Commonwealth. v. Ruddock, No. 08–1439, 2009 WL 3400927, at *3 (Mass. Super. Ct. Oct. 16, 2009). If an expert's access to evidence for purposes of examination is limited to the Commonwealth's facilities in order to prevent dissemination of such materials, the defendant's right to effective assistance of counsel will be unduly burdened. Id. A copy of the mirror image of a seized drive, including pornographic

images, must be given to the defendant's counsel of record and expert forensic examiner under a protective order limiting access to defense counsel and the expert. Id. (citing Mass. R. Crim. P. 14(a)(6)).

### 2. Wiretap transcripts

- Commonwealth v. Tavares, 482 Mass. 694 (2019). The defendant was convicted of murder in the first degree. During the investigation, police had recorded conversations between the defendant and a confidential informant using a wiretap. Id at 698. Prior to trial, the defendant moved successfully to suppress the recordings because "the investigation was not in connection in with organized crime" and thus violated G. L. c. 272, § 99. Id. at 714. After he was convicted, the defendant filed a motion for a new trial, arguing that his counsel was ineffective for failing to seek suppression of evidence derived from the recordings, as well as a "motion for postconviction discovery to obtain copies or transcripts of the wiretap recordings." Id at 714. The trial court denied both motions. Id. "Under the Massachusetts wiretap statute, a criminal defendant 'may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom' if the interception was made in violation of the statute." Id at 715 (quoting G. L. c. 272, § 99). On appeal, the SJC affirmed denial of the ineffectiveness motion, ruling that the defendant "failed to identify any specific evidence admitted at trial that was derived from the unlawful recordings." Id. But the court reversed the denial of the motion for post-conviction discovery, concluding that the defendant is entitled to a copy of the wiretap transcript prior to any retrial. Id. at 715-16. The SJC found that the transcript would enable defense counsel to examine whether there is any improper reliance on the suppressed recordings at any future trial. Id.

### 3. Cell phone data

- Commonwealth v. Valotto, No. SJ-2023-0504 (Jan. 24, 2024). In this single justice decision, the court reversed an order by the trial court that had allowed for the defendant to search and extract back-up data from the victim's cell phone under Mass. R. Crim. P. 17. Id. at 2. The victim no longer had the same cell phone, and, therefore, any production would have required a search and seizure of stored data that had been transferred to the new device. Id. at 2. The matter surrounded an alleged attack on the victim by three individuals that resulted in the victim's hospitalization, after playful wrestling among friends turned violent. Id. at 3. The defendant sought all communications and social media posts from the date of the alleged incident forward, claiming that conversations the victim had with others were relevant and could aid in his defense. Id. at 1. This assertion was based on alleged inconsistences between the victim's statements to police and on a screenshot provided to investigators of a Snapchat conversation between the victim and one of the other alleged attackers inquiring about what happened after the victim had blacked out. Id. at 3-4. The trial court had originally allowed the motion and was influenced by a 2020 single justice ruling in R.C. v Chilcoff, No. SJ-2020-0081 (Dec. 15, 2020). The trial court's order in Chilcoff was not contested by the victim, nor did that order cover an extended period. The only similarity between the facts in Chilcoff and the facts in this case related to the need to access back-up data for the search. Id. at 4.

Ultimately, the single justice reversed the trial court's order, distinguishing Chilcoff on its facts and finding that the relevancy grounds were too attenuated and that the order was too broad. Id. at 5. The court held that the request was overbroad in that it sought wide swaths of data over too long of a period to be justified. Id. The single justice made a point to say that even limiting the order would not make the order permissible, because later conversations related to an event are not automatically relevant, and the potential inconsistencies in the victim's statements were not as apparent as the trial court had found. Id. The court concluded by stating that the request felt like a fishing exercise and was being used as a discovery tool, which is plainly impermissible under the scope of Rule 17. Id. at 6.

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.). The defendant, indicted on one count of rape, filed a Mass. R. Crim. P. 17(a)(2) motion to obtain information from the victim-witness's cell phone relating to her electronic communications and use of social media over a twelve-day period beginning with the day of the incident. Id. at *2–3. The motion judge ordered the victim-witness to produce her cell phone and/or any "backups" for forensic examination to recover the sought-after information. Id. at *3. The judge also ordered that the victim-witness provide the names and login information for third-party service providers that possessed the information, and directed Facebook to provide Facebook and Instagram data associated with the victim-witness's accounts, including photographs and the contents of messages. Id. The victim-witness, joined by the Commonwealth, petitioned a single justice of the Supreme Judicial Court for relief from the order under G.L. c. 211, § 3, asking that (1) the twelve-day period for which cell phone data was sought be more narrowly tailored to the time of the incident, and (2) the order be vacated insofar as it required the victim-witness to provide the names and login information for third-party service providers. Id. The single justice granted the requested relief. First, the justice summarized the Lampron requirements for a successful Rule 17 motion: relevance, admissibility, necessity, and specificity. Id. at *4. The justice then noted that Massachusetts case law had yet to address the use of Mass. R. Crim. P. 17 to obtain a victim-witness's cell phone communications or third-party service providers. Id. Observing that "individuals have significant privacy interests at stake in their cell phones," the justice concluded that, "when ruling on a request under Rule 17 for a victim-witness's cell phone or cell phone records, the judge must include a consideration of these inherent privacy concerns." Id. The justice also examined decisions in which other state and federal courts had confronted similar issues, including a Minnesota Supreme Court decision holding that the fact that a "cell phone could contain exculpatory information was insufficient to order its production for examination." Id. at *5 (citing In re B.H., 946 N.W.2d 860, 870-71 (Minn. 2020)). Finally, the justice noted that Rule 17 "is a rule of production, not a rule of discovery." Id. After taking the above factors into account, and in light of the fact that the defendant could only speculate that relevant evidence might be obtained from the broad sweep of sought-after information, the justice granted the victim-witness's requested relief.

#### 4. Evidence of Allegedly Discriminatory Policing

- Commonwealth v. Dilworth, 494 Mass. 579 (2024). In a case stemming from a 2018 indictment charging the defendant with unlawful possession of a firearm and related offenses, the

Commonwealth refused to comply with a discovery order that required "[c]olor copies of the [Snapchat] user icons or bitmojis, and other user names" used by undercover police officers to infiltrate and monitor Snapchat accounts belonging to suspected gang members. Id. at 583-84. The scope of the discovery order was limited to undercover Snapchat accounts used between August 2017 and July 2018. Id. at 580, 583. The defendant filed a motion to dismiss with prejudice based on the Commonwealth's failure to comply with the discovery order, and a Superior Court judge dismissed the case with prejudice to sanction the Commonwealth for its discovery violation. Id. at 585. The defendant's equal protection challenge was based on allegations regarding "the patterns of decisions police made from the outset of the investigatory scheme, and how those patterns of decisions reflect a choice to target people based on race." Id. at 584. Notably, the Superior Court judge found that the Commonwealth's opposition to the motion to dismiss failed to present sufficient factual evidence to reveal how "icons, bitmojis and user names deployed by the BPD four-to-five years ago would imperil the safety of confidential informants and/or undercover officers and impede *ongoing* investigations." Id. at 585 (emphasis in original).

After concluding that this information would "persuasively and visually" demonstrate the racial compositions of individuals targeted for Snapchat monitoring, coupled with the Commonwealth's repeated refusal to comply with the discovery order, the SJC determined that the Superior Court judge did not abuse his discretion by dismissing the case with prejudice. Id. at 585, 593. The SJC articulated that the Long equal protection standard can apply to allegedly discriminatory policing in the investigatory phase of a case, such as Snapchat monitoring. Id. at 588; Commonwealth v. Robinson-Van Rader, 492 Mass. 1, 18 (2023) ("[T]he equal protection standard applies beyond traffic stops to claims of selective law enforcement, such as pedestrian threshold inquiries and 'other claims of discriminatory law enforcement'") (citing Commonwealth v. Long, 485 Mass. (2020)). Additionally, a privilege justifying non-disclosure of undercover social media account usernames or profile images created four-to-five years prior to the discovery motion requires establishment of a "nexus between disclosure of the requested information [] and potential danger to a confidential informant" and more than conclusory testimony that disclosing such information would "jeopardize other investigations" and "render that account useless in future investigations." Id. at 590-91.

## C. Authentication

### 1. Generally

To find that evidence is authentic, a judge must determine whether, by a preponderance of the evidence, there is sufficient evidence, including "confirming circumstances," to permit a "reasonable jury to conclude that this evidence is what the proponent claims it to be." Commonwealth v. Purdy, 459 Mass. 442, 449 (2011). Confirming circumstances are other facts that imply that evidence is what the proponent represents it to be. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011).

### 2. Photographs and Digital Images, Videos, and CDs

Authentication of photographs and videos is "typically… done through one of two means—having an eyewitness testify that the [photo or] video is a fair and accurate representation of what he saw on the day in question, or having someone testify about the [recording] procedures and the methods used to store and reproduce the [photo or] video material." Commonwealth v. Connolly, 91 Mass. App. Ct. 580, 586 (2017) (citing Commonwealth v. Pytou Heang, 458 Mass. 837, 855 (2011); Commonwealth v. Rogers, 459 Mass. 249, 267 (2011)). Digital photographs and videos are treated as equivalent to their analog counterparts. See Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294–95 (2006).

These are not the only possible ways to authenticate photo and video evidence, however. Commonwealth v. Davis, 487 Mass. 448, 466 (2021). More generally, admissibility may be established by any "evidence sufficient to support a finding that the matter in question is what its proponent claims." Mass G. Evid. § 901(a). For example, a witness may authenticate a digital photograph or video by testimony about the process used to create it and "showing that it produces an accurate result." Mass. G. Evid. § 901(b)(9).

- Commonwealth v. Davis, 487 Mass. 448 (2021). Following conviction for armed assault with intent to murder and other charges, the defendant argued on appeal, among other things, that the GPS device evidence introduced at trial was not sufficiently reliable, that the maps of the GPS data violated his confrontation rights, and that the cell phone video introduced was not authenticated. Id. at 449-50. On the issue of authentication, the court held that there are a number of different ways that a video may be authenticated. Id. at 465-66. These include eyewitness testimony, testimony about the surveillance procedures and methods of storing and reproducing video, and circumstantial evidence. Id. Here, the Commonwealth properly authenticated the cell phone video using circumstantial evidence. Id. at 33.

- Commonwealth v. Castro, 99 Mass. App. Ct. 502 (2021). Cesar Castro was convicted of photographing an unsuspecting nude or partially nude person in violation of G.L. c.272, §105(b). Id. at 502. The Appeals Court affirmed the conviction. Cesar Castro argued that the judge abused his discretion in admitting the photograph within an Instagram message without sufficient authentication. Id. at 509. The court noted that proof that the defendant sent the photograph was not critical, since that was not at issue in the case; rather, the issue was whether the defendant took the photograph with the requisite intent. Id. at 509. But the court found sufficient evidence that the defendant sent the photo regardless. Id. The court emphasized that there is no requirement for direct evidence to support a determination that a digital communication was sent by a defendant for authentication purposes; the court may consider circumstantial evidence and look at "confirming circumstances." Id. at 510 (quoting Commonwealth v. Meola, 95 Mass. App. Ct. 303, 311 (2019)). Here, the court found extensive confirming circumstances, including the unique name on the Instagram account at issue, the defendant's photo in the Instagram icon, the defendant's cell phone number shown in screenshots, references to the victim's birthday, and escalating conduct consistent with the victim's prior relationship with the defendant ending on bad terms. 99 Mass. App. Ct. at 510-11.

- Commonwealth v. Leneski, 66 Mass. App. Ct. 291 (2006): A witness sufficiently authenticated a CD containing digital images created by a digital camera system at a convenience store where that witness testified he had "viewed the images on the computer and 'burned' the CD copy; [and] testified as to the procedure he used in the surveillance process, the copying process, and to the contents of the CD." Id. at 295.

Testimony about a photo or video that is not introduced in court, but instead is described to the jury by a witness, is subject to the admissibility conditions as the original photo or video: that is, the testimony is admissible upon establishing that the photo or video the witness saw was a fair and accurate representation of the events in question. Commonwealth v. Connolly, 91 Mass. App. Ct. at 586–87.

### 3. Digitally Enhanced Images and Video

The SJC has indicated that even digital photographs that have been enhanced have some use as a demonstrative aid, so long as they accurately illustrate what a witness testifies about. See Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing 2 McCormick, Evidence § 214 (6th ed. 2006)).

When offering digitally enhanced photographs or videos, the type of media and the manner of enhancement will be relevant. See Iacobucci v. Boulter, 193 F.3d 14, 20 (1st Cir. 1999). Objections to evidence on the grounds that it lacks a proper foundation are allowed at the discretion of the judge. Id. In Iacobucci, where the audio portion of a video was enhanced with a high quality play-back system to increase the volume, the trial judge decided that this did not destroy the video's integrity and the video was properly authenticated. Id. Several witnesses positively identified the defendants' voices on the recording, and the jury had the opportunity to evaluate the identification on their own. Id. at 20–21.

Alternatively, "[f]or digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007). In such a case, there will need to be proof that the digital enhancement process produces reliable and accurate results. Id.

- Commonwealth v. Robertson, 489 Mass. 226 (2022). In a first-degree-murder trial, the Commonwealth used digitally-enhanced photographs of the defendant on the night of the shooting and at the club near where the shooting occurred. Id. at 235. The defendant challenged the admission of the enhanced photographs. Id. The SJC noted that whether enhanced photographs "properly were admitted is an issue of authentication and the balancing of the probative value and prejudicial effect." Id. The court also noted that a party that seeks to use an enhanced image must elicit "testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer." Id. (quoting State v. Swinton, 268 Conn. 781, 813 (2004)). Here, "a witness explained that he enlarged each photograph and used computer software to lighten and sharpen shadowed areas" and "that these modifications did not alter the photograph's pixels other than to change their colors." Id. at 235-36. "The original photographs had been authenticated earlier in the trial by the individual who took them, and the direct and cross-examination of the individual who enhanced the photographs revealed that the images were not so altered as to make them unduly

prejudicial or misleading." Id. at 236. Thus, "[t]he judge did not abuse her discretion in admitting the enhanced photographs." Id. at 236.

#### 4. Transcripts of Recordings

A written transcript of a recorded conversation taken from an electronic transmitting device can be authenticated where a witness testifies that the transcript is a fair and accurate representation of the recording. See United States v. Anderson, 452 F.3d 66, 76–77 (1st Cir. 2006) (citing United States v. Ademaj, 170 F.3d 58, 65 (1st Cir. 1999)). That witness does not have to be the person who transcribed the recording. Id. at 77.

#### 5. Email

"While e-mails and other forms of electronic communication present their own opportunities for false claims of authorship, the basic principles of authentication are the same." Commonwealth v. Purdy, 459 Mass. 442, 450 (2011) (citing United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006)). Email authentication does not require expert testimony or evidence of exclusive access or password protection, although they are relevant to the jury's assessment of the weight of the evidence. See id. at 451. Where the relevance or admissibility of emails depends on whether the defendant authored the emails, the judge must "determine whether the evidence [is] sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the e-mails." Id. at 447 (citing Commonwealth v. Leonard, 428 Mass. 782, 785–86 (1999); Mass. G. Evid. § 104(b)(1)).

However, where the contents of an email do not sufficiently authenticate it, it may be properly authenticated through confirming circumstances. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011). Confirming circumstances imply that evidence is what the proponent represents it to be. Id. at 674. For example, the following confirming circumstances were sufficient to link a defendant to emails: (1) an email revealed that the sender would meet the email recipient at a certain place and time, and the defendant then appeared in that place at the time specified; (2) the sender of that email included his telephone number and a photograph of himself. Id. at 674–75. The defendant answered a call to that number, and emailed photograph depicted the defendant. Id.

Other confirming circumstances include: (1) emails originate from an account that bears the defendant's name and that the defendant admits having used; (2) emails are found on a computer hard drive that the defendant admits owning; (3) the defendant supplies all necessary passwords to access files on the computer; (4) emails contain an attached photograph of the defendant and/or describe the unusual circumstances or traits attributable to the defendant. Purdy, 459 Mass. 442, 450–51 (2011).

"Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking website such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant. There must be some confirming circumstances sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the emails." Id. at 450 (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)); see also Griffin v. State, 419 Md. 343, 357–58 (2011) (holding that authentication of a page printed from a social networking site

requires more than a showing that a picture, birth date, and location of the alleged creator exist on the profile from which the page was retrieved).

Embedded e-mails will not be excluded because of the mere possibility that they can be altered without any specific evidence showing alteration. In Safavian, when "the trustworthiness of the emails particularly those . . . . emails that are included in a chain-either as ones that have been forwarded or to which another has replied" were challenged, the district court held that the "*possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course any more than it can be the rationale for excluding paper documents (and copies of those documents)." 435 F. Supp. 2d at 41 (emphasis in original). The court added that the defendant would be entitled, however, to raise any issue of alteration with the jury. Id.

- Commonwealth v. Middleton, 100 Mass. App. Ct. 756 (2022). In an appeal from convictions for stalking and violating a restraining order, the defendant argued that the trial court erred in admitting into evidence thirty-three emails without proving that the defendant had sent the emails. Id. at 757. The defendant further argued that the trial court erred by admitting email records summonsed from Google, without expert testimony to explain "some dates and times and codes" contained in the records. Id. at 761. The Appeals Court rejected both arguments. Id. at 757.

  The court held that the trial judge appropriately determined that sufficient evidence existed "'for a reasonable jury to find by a preponderance of the evidence that the defendant authored' the communication." Id. at 760 (quoting Commonwealth v. Oppenheim, 86 Mass. App. Ct. 359, 366 (2014) and Commonwealth v. Purdy, 459 Mass. 442, 451 (2011)). The communication can be "authenticated by circumstantial evidence, including details of defendant's and victim's lives." Id. (citing Commonwealth v. Welch, 487 Mass. 425, 440-442 (2021)). Relevant factors included the presence of unique personal references and nicknames in the emails, references to prior conversations between the defendant and victim, and other personal identifying information. Id. at 758-59. The court further held that "expert testimony was not necessary for the jurors to understand the Google records." Id. at 761. More specifically, expert testimony was not necessary here because "understanding the dates of service for each account did not require any 'scientific, technical, or other specialized knowledge.'" Id. at 761 (quoting Commonwealth v. Canty, 466 Mass. 535, 541 (2013)). Moreover, no expert testimony about IP addresses was necessary, where "[t]he Google records did not contain any IP addresses." Id. at 762.

### 6. Chatrooms

Similar to the method of authentication by confirming circumstances allowed in the Commonwealth, "[c]ourts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. For example, in [the Pennsylvania case] In re F.P., the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert . . . . The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 556 (D. Md. 2007) (citing In re F.P., 878 A.2d 91, 93–94 (Pa. Super. Ct. 2005)).

### 7. Text Messages

- Commonwealth v. Welch, 487 Mass. 425 (2021). The defendant was convicted of first-degree murder for the death of his girlfriend. On appeal, he argued that text messages between him and the victim, which a state police trooper read aloud into the record at trial, were not authenticated. Id. at 440. The court disagreed, finding that "the Commonwealth presented more than an ample foundation for the judge to determine that a reasonable jury could find by a preponderance of the evidence that the defendant authored the text messages." Id. at 442. Text messages may be authenticated "by way of direct or circumstantial evidence, including its [a]ppearance, contents, substance, internal patterns, or other distinctive characteristics." Id. at 441 (quoting *Commonwealth v. Lopez*, 485 Mass. 471, 477 (2020)). In addition, "confirming circumstances" that may authenticate text messages include "acknowledgement that the defendant uses the cell phone, acknowledged ownership by a defendant of the cell phone containing the messages, and whether the defendant knows or supplies the passwords protecting the cell phone." Id. (citations omitted). Here, the court found "abundant confirming circumstances." Id. The phones were registered to the victim and the defendant; the phones were password protected such that police had to use specialized software to break into phone; the phones were found in the possession of the defendant and the victim on the night of the murder; the messages contained many details of the defendant's and victim's lives. Id. at 441-42. The court also concluded that the defendant's claim that another party may have authored the text messages is only relevant to their weight as evidence, not their admissibility. Id. at 442.

- Commonwealth v. Alden, 93 Mass. App. Ct. 438 (2018). The victim received threatening text messages from a "telephone number [she] had used to communicate with the defendant . . . every few days for over one year." Id. at 439. The trial court held that "the Commonwealth had established by a preponderance of the evidence that the text messages were authentic" - i.e., that the messages came from the defendant. Id. at 440. The Massachusetts Appeals Court affirmed because "for over one year, [the victim] had contacted the defendant multiple times each week using the telephone number from which the threatening messages originated. When she called that number, the defendant answered. When she sent a text message to that number to arrange a meeting with the defendant, he appeared." Id. at 440–41. Moreover:

  > [t]he content of the text messages reinforced their link to the defendant. It is undisputed that at the time she received the text messages, [the victim] was a witness in a pending case against the defendant. In this context, where there was evidence that the text messages directed her to "keep her [explicative] mouth shut" and "leave their personal stuff out of the courtroom" or "people [would] come after [her] if [she] went to court," it was reasonable to infer that the defendant was responsible for sending the messages.

  Id. at 441.

## 8. Information Available on Websites and Social Networks

Evidence available on websites presents its own problems. "Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007). "The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting." Id. (citing United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000)). In doing so, federal courts require the proponent of such evidence to show what was actually on the website, to show that the exhibit or testimony accurately reflects that content, and to show that the content can be attributed to the owner of the site. Id. (citations omitted).

In the courts of the Commonwealth, "[e]vidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant." Commonwealth v. Purdy, 459 Mass 442, 450 (2011) (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)).

Circumstantial evidence can authenticate a social network page:

- Commonwealth v. Meola, 95 Mass. App. Ct. 303 (2019). The Appeals Court affirmed the Superior Court's holding that sufficient evidence in the form of "confirming circumstances" established that the defendant attached an obscene video to a communication he sent to an underage victim. Following a jury waived trial, a Superior Court judge found the defendant guilty of disseminating obscene material to a minor in violation of G.L. c. 272, § 28. Id. at *1. The Appeals Court looked to the principles established by the SJC in Commonwealth v. Purdy, 459 Mass 442 (2011) regarding authenticating digital evidence (that is not self-authenticating). First, Purdy establishes that direct evidence is not necessary to determine that a defendant sent a digital communication. Rather, a judge "may consider circumstantial evidence and look to 'confirming circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored" the electronic communication. Meola, 2019 WL 2202909 at *5 (quoting Purdy, 459 Mass. at 450). Second, under Purdy, the "mere possibility that a digital communication was fraudulently sent by someone other than the person associated with a particular social media...account from which the communication originated is not a bar to its authentication." Meola, 2019 WL 2202909 at *5. Third, common-law principles concerning authenticity are applicable to digital communications. Id. In this matter, the trial judge's decision to exclude records proffered by the prosecutor, describing user information related to the Facebook account and the sender of the video, required the Commonwealth to rely on indirect evidence to authenticate the materials. Id. at *2. The Appeals Court concluded that the following facts offered sufficient indirect evidence of authenticity: the defendant's prior association with the victim (defendant had previously lived with her and her mother); the defendant's biological relation to the victim's half-sister; and the friend request the user of the account sent to the victim. Moreover, the court determined that the trial judge did not err in finding the

communications authentic because there was no evidence to suggest that the Facebook profile photo or the self-authored obscene video were publicly available. Id. at *6. Based on these facts, the court affirmed the trial judge's determination that the defendant "purposefully disseminated matter harmful to a minor to the victim" with full knowledge that she was a minor. Id. at *7.

- Other jurisdictions have taken a similar approach. For example, in the Texas case Tienda v. State, MySpace webpages were admissible because there was sufficient evidence on them indicating that they "were what they purported to be." 358 S.W.3d 633, 646 (Tex. Crim. App. 2012). The court stated that, "as with the authentication of any kind of proffered evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case." Id. at 639. The court held that there was "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the Myspace pages belonged to the appellant and that he created and maintained them." Id. at 645; see also Parker v. State, 85 A.3d 682 (Del. 2014) (holding that social media post was sufficiently authenticated by circumstantial evidence and by testimony explaining how the post was obtained); Simmons v. Commonwealth, No. 2012–SC–000064–MR, 2013 WL 674721 (Ky. Feb. 21, 2013) (holding that the print-outs of the defendant's Facebook messages were admissible because the messages were what they purported to be and the role of the judge, as a gatekeeper, was only to determine if an offering party has produced enough evidence for a reasonable jury to find authenticity).

### 9. Software Programs Used in Investigation

When a witness uses software to create information relevant to an investigation, that witness should testify in detail as to the nature of the tool, how the witness used it, and how it was created and maintained in order to authenticate the records. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 327 (2009) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)). In Whitlock, a police officer used a software program called ArcView, which is a computerized map that depicted the location and ownership of property within the city of Springfield. Id. at 325–26. The information provided by this software was used to show that the defendant was distributing a controlled substance within a school zone. Id. Where software provides information to a witness, for example software that measures and provides distances between real-world objects, it does not make a "statement," and therefore is not subject to the hearsay rule. Id. at 326–27.

### 10. GPS Records

The SJC has "recommend[ed] strongly" that GPS records offered in probation revocation proceedings "be properly attended and certified by an appropriate custodial officer" to avoid authenticity concerns. Commonwealth v. Thissell, 457 Mass. 191, 199 (2010).

- Commonwealth. v. Lehan, 100 Mass. App. Ct. 246 (2021). Defendant, who was convicted of criminal stalking and vandalism of property, claimed on appeal that his GPS records, as well as an officer's testimony about them, were improperly admitted. Id. at 247. At trial, the police officer who investigated the case testified about his conclusions after reviewing the GPS charts, but no one with personal knowledge testified about the

creation of the records. Id. The Appeals Court held that the GPS records were erroneously admitted, because without the proper foundation to demonstrate that they were business records, they were inadmissible hearsay. Id. at 254-57. For evidence to be admitted as a business record, a foundation must be established under G.L. c. 233, §78, by the party seeking admission. Id. at 255. More specifically, the court must find "that the entry, writing or record was made in good faith in the regular course of business and before the beginning of the civil or criminal proceeding . . . and that it was the regular course of such business to make such memorandum or record." Id. (quoting G.L. c. 233, §78). Without sufficient evidence on how the GPS records were generated or created, the records were not admissible as business records. Id. at 255-56. The court also rejected the Commonwealth's argument that the records could be admitted based on a keeper of the records certification under G.L. c. 233, §79J, because "[t]he statute does not overcome a hearsay objection." Id. at 256. In fact, the keeper of the records affidavit in these circumstances is itself "classic hearsay." Id. at 257. Unlike hospital and bank records, the admissibility of which are governed by other statutes, GPS records cannot be admitted without a testifying witness. Id. In addition, the police officer's testimony about the records should not have been admitted, both because the records themselves were not properly in evidence, and because the Commonwealth failed to establish a foundation for the officer to testify about the GPS charts based on his personal knowledge. Id. The court further held that the admission of the GPS charts and the officer's testimony about them was prejudicial because it was precisely this evidence that tied the defendant to vandalism. Id. at 258. Accordingly, the court overturned the defendant's convictions. Id.

## D. Technological evidence as the basis of criminal conviction

Evidence used as the basis of a conviction must be sufficient, viewed in the light most favorable to the government, for a rational trier of fact to find the essential elements of the crime beyond a reasonable doubt. Commonwealth v. Ayala, 481 Mass. 46, 51 (2018) (citing Commonwealth v. Latimore, 378 Mass. 671, 677-78 (1979). Thus, even evidence that meets the preponderance standard required to authenticate a piece of evidence, see § II.C, supra, may not be sufficient to support a conviction. The government bears the burden of explicit proof even for facts about technology that may be well known to the trier of fact, e.g., that a password is generally required to log in to and send messages from an Instagram account. Commonwealth v. McMann, 97 Mass. App. Ct. 558, 561 (2020). Such facts are not appropriate subjects of judicial notice. Id. at 561 n.4.

- Commonwealth v. Bustard, 106 Mass. App. Ct. 442 (2026). The defendant was convicted of violating an abuse prevention order that prohibited him from contacting the victim. Id. at 442, 444. Prior to the issuance of the order, the defendant and the victim had communicated via Snapchat, with the defendant messaging under the username "jayysworld25." Id. at 443. After the defendant and the victim separated, the victim blocked jayysworld25 on Snapchat. Id. at 443. After blocking jayysworld25 but prior to the issuance of the order, the victim received a Snapchat message reading "Miss me" from a user she did not recognize. Id. at 443, 449. The unknown user had the username "jesseman94" and the display name "Jesse Cunningham." Id. at 443. Jesseman94's bitmoji (a cartoon representation that is associated with a user's Snapchat profile) was similar to jayysworld's bitmoji: both had slicked-back hair with a beard, although the beards

differed. Id. at 443. On July 14, 2022, the defendant's girlfriend was in court "seeking an abuse prevention order against the victim's fiancée." Id. at 443. That same day, jesseman94 messaged the victim "You happy." Id. When the victim's sister looked up the jesseman94 account using her own Snapchat account, rather than "Jesse Cunningham," the display name was "Justin," which is the defendant's first name. Id. at 444. The victim "testif[ied] that different Snapchat users may see different names for one account" because the display name is frozen at the time of connection acceptance, regardless of whether "the user later changes the display name." Id. at 444. "The victim further testified that the defendant's brother's name is Jesse and that the defendant's old family friends were the Cunninghams." Id.

On appeal, the defendant argued that there was insufficient evidence at trial to support his conviction. Id. at 445. The MAC reversed the judgment and found that defendant's motion for a required finding of not guilty should have been granted for the following reasons: (1) "[t]he solitary message of 'You happy' could not reasonably guide the fact finder to the defendant" because it "does not refer to any prior conversations between the victim and the defendant, contains no personal references, and reads without a singular or familiar tone," Id. at 447, see Commonwealth v. Oppenheim, 86 Mass. App. Ct. 359, 364 (2014); (2) the message did not display knowledge of the July 14, 2022, restraining order hearing, and even if it had, "the hearing was not an event about which the victim and the defendant only would have knowledge of or motive to discuss," Bustard, 106 Mass. App. Ct. at 447, see Commonwealth v. Gilman, 89 Mass. App. Ct. 752, 759 (2016); (3) "the evidence failed to establish that jesseman94 was the defendant's account or that the defendant even had access to the account" because (a) the bitmoji similarities were not supported by "evidence demonstrating how many options a user has when building a bitmoji or how the two bitmojis were evocations of the defendant," Bustard, 106 Mass. App. Ct. at 448, and (b) "the conclusion that the defendant was using his brother's name and his family friend's last name required that the fact finder take too great an inferential leap" because "[t]he evidence did not show that the defendant ever went by the name 'Jesse Cunningham' or that the defendant had previously reached out to the victim through this account," Bustard, 106 Mass. App. Ct. at 448, see Commonwealth v. Lopez, 484 Mass. 211, 216 (2020); and (4) "even if the piling of inferences were permissible (which it is not), evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site ... that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant," Bustard, 106 Mass. App. Ct. at 448, citing Commonwealth v. McMann, 97 Mass. App. Ct. 558, 559 (2020) (citation modified).

- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020). Defendant was convicted of violating an abuse prevention order that prohibited him from contacting his ex-girlfriend. Id. While the order was in effect, the ex-girlfriend received an Instagram message from user "bigm617" that said "Yoooo." Id. at 559. She testified that she knew that "bigm617" was the defendant's account "because the associated account displayed pictures of the defendant, including one of him with the victim, and the victim and the defendant had previously 'liked' and commented on each other's Instagram posts." Id. The victim showed this Instagram message to a police officer, who

met with the defendant later that day. Id. The defendant denied sending any message to the victim, 'wanted to show [the officer] that he never did[,]' and entered a passcode to unlock his cell phone. He then opened the Instagram application on his cell phone, and the 'Yoooo' message to the victim appeared on the screen. The officer observed that the defendant looked '[s]urprised.' Id. The Appeals Court held that "even assuming without deciding that the Instagram message was properly authenticated, the Commonwealth failed to… prov[e] beyond a reasonable doubt that the defendant was the person who wrote or sent the message to the victim. Although the evidence was sufficient to show that the Instagram account was the defendant's and that he could access it, there was no circumstantial evidence establishing authorship." Id. at 560. The court suggested the burden could have been met by "evidence that the message itself contained characteristics showing that the defendant wrote it, or through evidence establishing how secure Instagram accounts are and how the Instagram cell phone application works." Id. at 562.

## E. Best Evidence Rule

### 1. Best Evidence Rule - Generally

"The best evidence rule provides that, where the contents of a document are to be proved, the party must either produce the original or show a sufficient excuse for its nonproduction." Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001); see also Mass. G. Evid. § 1002. However, what constitutes a "document" has been narrowly construed such that "[t]he best evidence rule is applicable only to those situations where the contents of a *writing* are sought to be proved." Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970) (emphasis added). Most photographs and videos depict objects rather than writings. Consequently, the best evidence rule does not typically apply, *inter alia*, to photographs or videotapes. See also Commonwealth v. Weichell, 390 Mass. 62, 77 (1983) (holding that the "enlarged photograph was a fair and accurate representation of the defendant at the time of his arrest"); Commonwealth v Leneski, 66 Mass. App. Ct. 291, 294 (2006) ("Videotapes, like photographs, are not subject to the best evidence rule."). Additionally, "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes." Leneski, 66 Mass. App. Ct. at 294.

### 2. Digital Images

Digital image evidence is not subject to the best evidence rule in Massachusetts because these images are not writings. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006) (citing Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970)). The Leneski court held that digital images from a computer copied to a compact disk ("CD") would be considered as originals. Id. Testimony about authenticity, including how the disc was generated, the procedure used in the surveillance process, the copying process, and the contents of the CD, was deemed sufficient. Id. The court noted that there was opportunity for cross-examination that went to the weight of the evidence on the subject of surveillance procedure and the method of storing and reproducing the data. Id.

This exception to the best evidence rule extends to images that have been transferred from a hard drive to other media such as CDs and DVDs. See id. at 294 (holding that "digital images placed and

stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes").

### 3. Admission of Duplicate Evidence

> [W]here the original [of a document] has been lost, destroyed, or otherwise made unavailable, its production may be excused and other evidence of its contents will be admissible, provided that certain findings are made.
>
> As a threshold matter, the proponent must offer evidence sufficient to warrant a finding that the original once existed. . . . If the evidence warrants such a finding, the judge must assume its existence, and then determine if the original had become unavailable, otherwise than through the serious fault of the proponent . . . and that reasonable search had been made for it. . . . If the judge makes these findings in favor of the proponent, the judge must allow secondary evidence to establish the contents of the lost writing.

Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001) (quoting Fauci v. Mulready, 337 Mass. 532, 540–43 (1958) (internal citations and quotation marks omitted)).

### 4. Videos

The best evidence rule does not apply to digital videos. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006). "Our courts have held that videos are 'on balance, a reliable evidentiary resource . . . .'" Id. (quoting Commonwealth v. Harvey, 397 Mass. 351, 359 (1986)). "[Videos] 'should be admissible as evidence if they are relevant, they provide a fair representation of that which they purport to depict, and they are not otherwise barred by an exclusionary rule.'" Id. (quoting Commonwealth v. Mahoney, 400 Mass. 524, 527 (1987)).

### 5. Email

It is unlikely that printed email communications are subject to the best evidence rule so long as their authenticity can be proven through circumstantial evidence. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 675–76 (2011). In Amaral, the court reasoned that the email server, or the computer itself, is not better evidence than directly printed emails, and that "[t]he significance of the best evidence rule has declined appreciably in recent decades." Id. at 675 (internal quotation marks omitted).

### 6. Summaries

Large volumes of digital evidence may be summarized and shown to a jury without running afoul of the best evidence rule.

In the Commonwealth, voluminous evidence that would be difficult for a jury to understand due to volume or complexity may be presented in the form of a written or testimonial summary or a chart, shown by testimony to accurately reflect the contents of the underlying documents, so long as the proponent does not unfairly emphasize portions of the summarized evidence. See Mass. G. Evid. § 1006; Commonwealth v. Mimless, 53 Mass. App. Ct. 534, 538 (2002) (quoting Welch v. Keene Corp. 31 Mass.

App. Ct. 157, 165–66 (1991)) ("[C]are must be taken to insure that summaries accurately reflect the contents of the underlying documents and do not function as pedagogical devices that unfairly emphasize part of the proponent's proof.") (internal quotation marks omitted); Commonwealth v. Greenberg, 339 Mass. 557, 582 (1959) ("The witness was not allowed to state deductions and inferences of his own but could state only the results of his computations from the admitted evidence."). The summarized evidence should be made available to other parties in advance of trial, and the court may order that the originals be produced in court. See Mass. Guide to Evid. § 1006.

- Commonwealth v. Shepherd, 493 Mass. 512 (2024). The defendant claimed that counsel was ineffective for failing to object to two map exhibits derived from the CSLI data. Id. at 534-36. The Court rejected the defendant's argument. Id. at 536. The Court held that trial counsel's lack of objection was not "manifestly unreasonable." Id. at 536. Under Commonwealth v. Bin, 480 Mass. 665, 679-80 (2018), the maps were admissible because they were derived from CSLI data for which a proper foundation had already been established. Id.

- Commonwealth v. Sosa, 493 Mass. 104 (2023). The SJC affirmed the defendant's convictions of murder in the first degree and armed assault with intent to rob. Id. at 124. The defendant challenged the use of a compilation video made to show the relevant parts of surveillance footage from the apartment building where the shooting occurred. Id. at 114. The defendant argued it was not properly authenticated nor properly admitted, while the Commonwealth contended that because the complete surveillance footage from which the compilation originated was properly admitted, using a subset of the footage did not impact the case significantly. Id. at 114. The court held that even if admitting the compilation video was erroneous, that admission did not prejudice the defendant, because the complete footage, which was authenticated and admitted, provided the necessary context, and the compilation video did not significantly alter the case's presentation. Id. at 115. The court stated that the better practice is to authenticate excerpts copied from an exhibit even if the complete exhibit has been authenticated and submitted into evidence. Id. at 115. The court also noted that when a jury may have issues handling the full video, "Parties should explore the viability of admitting excerpts of voluminous video recording pursuant to Mass. G. Evid. § 1006 (2023)." Id., quoting Commonwealth v. Suarez, 95 Mass. App. Ct. 562, 571-72 (2019).

- Commonwealth v. Suarez, 95 Mass. App. Ct. 562 (2019). The defendant, who was convicted of assault with intent to rape and other charges, challenged on appeal the introduction at trial of a six-minute compilation of video surveillance footage from before, during and after the attack, and a timeline describing parts of the videos. Id. at 566-67, 570. Since the defendant did not object at trial, the Appeals Court "examine[d] whether any abuse of discretion in admitting the exhibits created a substantial risk of a miscarriage of justice." Id. at 570-71. The court found the individual underlying videos could not 'be conveniently examined in court.'" Id. at 571 (quoting Mass. G. Evid. § 1006). Though the Commonwealth played portions of the videos in the courtroom, "a deliberating jury would have found it difficult to master the technology necessary to find and view the relevant parts of the videos in the jury room." Id. at 571-72. Furthermore, the court rejected the defendant's claim that the compilation was unfairly edited. Id. at 572. However, the court did find certain improprieties in the compilation and timeline. In particular, it

ruled that still photos, taken from a 7-Eleven store four hours after the attack, should not have been included in the compilation because the photos taken hours after the assault were not relevant to the crime itself. Id. The court also ruled that the timeline describing the digital compilation "could and should have used a neutral heading" for a set of video clips. Id. at 574. The court criticized the Commonwealth's use of the term "suspect" in the timeline to refer both to a person the defendant admitted was him, in certain video clips, and to the attacker, in other video clips, since use of that term suggested that they were the same person. Id at 573. The court ruled, however, that these "limited errors in the compilation and the timeline" did not create a substantial risk of a miscarriage of justice because they had little, if any, impact on the case. Id. at 574.

## F. Hearsay

"Whether a computer record contains a statement depends on whether the record is 'computer-generated,' 'computer-stored,' or a hybrid of both." Commonwealth v. Davis, 487 Mass. 448, 465 (2021). Because computer-generated records "are created solely by the mechanical operation of a computer and do not require human participation," they cannot be hearsay. Id.; see also id. at 464-65 (maps depicting defendant's location based on data from GPS devise were not hearsay and did not violate confrontation clause).

See also Commonwealth v. Thissell, 457 Mass. 191, 197 n.13 (2010) (discussing the difference between computer-generated and computer-stored records in the context of the rule against hearsay); Commonwealth v. Royal, 89 Mass. App. Ct. 168, 171–72 (2016) (treating "computer-stored" records as hearsay, but treating "computer-generated" records as not hearsay); Commonwealth v. Woollam, 478 Mass. 493, 498 (2017) (holding that call logs are computer-generated records that do not raise hearsay concerns; admissibility thus only depends on authentication) (Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326-27 (2009) (use of software that determined distance between point of sale and school did not raise hearsay concerns).

- Commonwealth v. Ubeda, 99 Mass. App. Ct. 587, 2021 WL 1974182 (2021). The defendant was convicted on multiple charges, including "aggravated rape and abuse of a child, posing or exhibiting a child in a state of nudity, disseminating child pornography, trafficking of a person for sexual servitude, extortion by threat of injury, larceny over $250, assault and battery, and trafficking of a person under eighteen years of age for sexual servitude." Id. at *1. Among other issues raised on appeal, the defendant argued that a police officer's testimony about the content of the defendant's and a victim's phones was inadmissible hearsay. Specifically, the defendant asserted that the police officer's testimony that the extraction reports contained photographs and a video of the victim and collages of nude images of the victim should have been suppressed as inadmissible hearsay. Id. at *4. The court found that "the extraction reports [were] 'computer-generated records,' which [did] not implicate the rule against hearsay." Id. at 5. The extraction reports were produced by a machine and required minimal human input to be created; thus, they were "not statements for purposes of the hearsay rule." Id.

## G. Business Records Exception

### 1. Email

A document from an email service provider that indicates that a specific login name is connected to a defendant's email address is admissible as a business record as long as it is supported by an affidavit from the service provider's custodian of records. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 673–74 (2011).

### 2. Computer Records

"[C]omputer records . . . are admissible under the business records exception to the hearsay rule, [Mass. Gen. Laws ch.] 233, § 78, if they were (1) made in good faith; (2) made in the regular course of business; (3) made before the action began; and (4) [it was] the regular course of business to make the record at or about the time of the transaction or occurrences recorded." McLaughlin v. CGU Ins. Co., 445 Mass. 815, 819 (2006) (quoting Beal Bank, SSB v. Eurich, 444 Mass. 813, 815 (2005) (internal quotation marks omitted)).

A lack of personal knowledge on behalf of the affiant, the maker, or custodian of records goes to the weight and not the admissibility of the business records. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674 (2011) ("[T]he personal knowledge of the entrant or maker affects only the weight of the record, not its admissibility.") (quoting and citing Note to Mass. Guide to Evid. § 803); see also McLaughlin, 445 Mass. at 819 (2006) ("[P]ersonal knowledge of the entrant or maker of a record is a matter affecting the weight rather than the admissibility of the record.").

A print-out of an electronic document is admissible as a business record as long as it is supported by an affidavit from the provider's custodian of record establishing that the requirements of the business records exception are met. Amaral, 78 Mass. App. Ct. at 673–74 n.4; McLaughlin, 445 Mass. at 8199 ("The affidavits plainly establish that the records satisfy these foundational requirements.").

### 3. GPS Records

GPS records cannot be admitted under the business records exception without witness testimony about the way they were generated or created.

- Commonwealth. v. Lehan, 100 Mass. App. Ct. 246 (2021). Defendant, who was convicted of criminal stalking and vandalism of property, claimed on appeal that his GPS records, as well as an officer's testimony about them, were improperly admitted. Id. at 247. At trial, the police officer who investigated the case testified about his conclusions after reviewing the GPS charts, but no one with personal knowledge testified about the creation of the records. Id. The Appeals Court held that the GPS records were erroneously admitted, because without the proper foundation to demonstrate that they were business records, they were inadmissible hearsay. Id. at 254-57. For evidence to be admitted as a business record, a foundation must be established under G.L. c. 233, §78, by the party seeking admission. Id. at 255. More specifically, the court must find "that the entry, writing or record was made in good faith in the regular course of business

and before the beginning of the civil or criminal proceeding . . . and that it was the regular course of such business to make such memorandum or record." Id. (quoting G.L. c. 233, §78). Without sufficient evidence on how the GPS records were generated or created, the records were not admissible as business records. Id. at 255-56. The court also rejected the Commonwealth's argument that the records could be admitted based on a keeper of the records certification under G.L. c. 233, §79J, because "[t]he statute does not overcome a hearsay objection." Id. at 256. In fact, the keeper of the records affidavit in these circumstances is itself "classic hearsay." Id. at 257. Unlike hospital and bank records, the admissibility of which are governed by other statutes, GPS records cannot be admitted without a testifying witness. Id. In addition, the police officer's testimony about the records should not have been admitted, both because the records themselves were not properly in evidence, and because the Commonwealth failed to establish a foundation for the officer to testify about the GPS charts based on his personal knowledge. Id. The court further held that the admission of the GPS charts and the officer's testimony about them was prejudicial because it was precisely this evidence that tied the defendant to vandalism. Id. at 258. Accordingly, the court overturned the defendant's convictions. Id.

## H. Confrontation Clause

### 1. Software-generated information

"The confrontation clause bars the admission of testimonial out-of-court statements by a declarant who does not appear at trial unless the declarant is unavailable to testify and the defendant had an earlier opportunity to cross-examine him." Commonwealth v. Wilson, 94 Mass. App. Ct. 416, 417 n.1 (2018), (quoting Commonwealth v. Simon, 456 Mass. 280, 296 (2010)).

When introducing software-generated information that is not hearsay as evidence, see § II.E, supra, the Confrontation Clause is not implicated. See Commonwealth v. Hurley, 455 Mass. 53, 65 n. 12 (2009) ("admission of a testimonial statement without an adequate prior opportunity to cross-examine the declarant… violates the confrontation clause only if the statement is hearsay…") (citing Crawford v. Washington, 541 U.S. 36, 59-60 & n. 9 (2004)); Commonwealth v. Davis, 487 Mass. 448, 464-65 (maps depicting GPS evidence were computer generated, and therefore were not hearsay and did not violate the confrontation clause).

### 2. Secondary Examiners

The Sixth Amendment's bar on the testimonial statements of a witness who does not appear at trial applies to forensic examiners because their explanation of the process and results of specific forensic examinations are testimonial statements. See United States v. Soto, 720 F.3d 51, 58–60 (1st Cir. 2013) (summarizing relevant Supreme Court cases).

A "surrogate" witness who is familiar with a lab's practices, but who has formed no independent opinion of the results is insufficient to satisfy the Sixth Amendment. Id. at 58 (citing Bullcoming v. New Mexico, 564 U.S. 647, 662–63 (2011)).

However, "[t]he government may ask an agent to replicate a forensic examination if the agent who did the initial examination is unable to testify at trial, so long as the [testifying] agent . . . conducts an independent examination and testifies [as] to his own results." Id. at 59; see, e.g., Commonwealth v. Chappell, 473 Mass. 191, 199–200 (2015) (substitute DNA expert testimony allowed because, as the second reader, she independently read all the raw data and the reports produced by the original analyst, made interpretations, and ensured that there was agreement between her findings and those the analyst, and therefore testified to her opinions or conclusions concerning the DNA).

- Commonwealth v. Seino, 479 Mass. 463 (2018). Defendant was convicted of first-degree murder. Id. at 464. On appeal, he asserted several confrontation claims. Id. at 466, 469–72. First, the defendant argued that it was improper for a doctor who did not perform the autopsy to refer during his trial testimony to statements in the autopsy report and death certificate, neither of which the testifying doctor authored. Id. at 466. The SJC held that it was appropriate for the testifying doctor to offer his opinion on the cause of death based on the case file and his own examination, but agreed with the defendant that the doctor should not have testified about statements in the autopsy report and death certificate. Id. at 466–67. The SJC found that the error was harmless beyond a reasonable doubt, however, because the improper testimony was cumulative, did not incriminate the defendant, and "did not contribute to the guilty verdicts." Id. at 467–68. Second, the defendant argued that his confrontation right was violated when two experts, as part of their trial testimony, used charts showing DNA testing data obtained by other analysts (who did not testify). Id. at 469–70. The SJC held that the data should not have been shown to the jury. Id. at 470. The court also concluded, however, that there was no substantial likelihood of a miscarriage of justice "because the charts did not taint the analysts' independent opinions, which . . . were properly admitted." Id. at 471. [Note: The court applied a miscarriage of justice standard because the defendant did not preserve an objection to the charts at trial. Id. at 470.] The SJC noted that the charts "merely displayed genetic locations, not any information regarding a match or the statistical probability thereof." Id. at 471. Third, the defendant argued that it was reversible error for an analyst to testify that the defendant's DNA profile matched a DNA profile developed by a different analyst from the victim's jeans. Id. The SJC rejected this claim, finding that the defendant had had the opportunity at trial to cross-examine the analyst who developed the defendant's DNA profile, the supervisor of the laboratory that developed the DNA profile from the jeans, and the analyst who compared the two profiles. Id. at 471–72.

- Commonwealth v. Scesny, 472 Mass. 185 (2015). An autopsy report and photographs from the victim's autopsy were introduced in evidence and a substitute medical examiner testified regarding findings in the report. Id. at 196–97. The SJC held the autopsy report was "'inadmissible hearsay whose admission violate[s] the defendant's right of confrontation under the Sixth Amendment to the United States Constitution,'" id. at 197 (quoting Commonwealth v. Emeny, 463 Mass. 138, 145 (2012)), and that a substitute medical examiner cannot testify about the facts and findings of the report on direct examination. Id. The autopsy photographs were properly admitted through a State police trooper who attended the autopsy. Id. at 198 n.25.

- Commonwealth v. Jones, 472 Mass. 707 (2015). At defendant's trial for rape, a chemist at the State police crime laboratory, who was not present during the "rape kit" examination and had no apparent connection to the hospital at which the swabs were taken, was allowed to testify on direct examination to her "understanding" of how the swabs had been collected. Id. at 711–12. The SJC held that allowing an expert witness who had not been present during the examination and had no apparent connection to the hospital where the examination occurred, to testify on direct examination to her "understanding" of how the swabs had been collected violated the defendant's confrontation right. Id. at 708. The SJC found that the "surrogate" expert's statements were testimonial for two main reasons: (a) in labeling the various swabs and completing the "rape kit" inventory list, the initial examiner made factual statements concerning how the swabs were collected, and (b) the purpose of a "rape kit" is to gather forensic evidence for use in a criminal prosecution,. Id. at 714. These statements would therefore only be admissible if they complied with the test established by Commonwealth v. Greineder, 464 Mass. 580, 593 (2013). Id. at 715. The Jones court summarized the holding of Greineder as follows: "'[e]xpert opinion testimony, even if based on facts and data not in evidence, does not violate the right of confrontation, provided that the facts and data 'are independently admissible and are a permissible basis for an expert to consider in formulating an opinion,' and that two further conditions are met. First, the expert must 'not present on direct examination the specific information on which he or she relied'; second, the expert witness must have the capacity to 'be meaningfully cross-examined about the reliability of the underlying data.'" Id. at 713 (quoting Greineder, 464 Mass. 580) (other citations omitted). The statements in Jones did not meet either of these requirements in Greinder: (1) the underlying hearsay facts of how the swabs were collected came in on direct examination and (2) the expert could not meaningfully be cross-examined about the reliability of the representations of the "rape kit" examiner concerning the origins of the swabs and lacked the capacity to address chain of custody and evidence-handling protocols relevant to the process by which the swabs were collected. Id. at 715–16. The testimony thus failed to comply with Greineder and was therefore inadmissible. Id. at 715.

## I. Discussing Digital Evidence in Closing Arguments

This section discusses cases in which courts consider whether statements about digital evidence made by prosecutors in closing arguments are permissible.

- Commonwealth v. Ferguson, 497 Mass. 199 (2026). In a first-degree murder case, the defendant argued on appeal that the prosecutor misstated the evidence at trial by claiming that the defendant's cell phone records placed him at a witness's house in Quincy, which "significantly bolster[ed] [the witness's] credibility." Id. at 214. The prosecutor said that the cell phone records placed "[the defendant] [] in Quincy right at the time [the witness] says so." Id. at 214. The SJC held that the prosecutor was not claiming that the defendant was at the witness's house, but rather was making a more general assertion that the defendant was in the bounds of Quincy, which "[was] a permissible inference drawn from the cell phone records that show that [the defendant's] cell phone connected to a cell tower located in Quincy." Id. at 215. See Commonwealth v. Hobbs, 482 Mass. 583, 547 (2019) (holding that "the location of a suspect's cell phone at the time of the criminal activity … can reasonably be expected to be found in the CSLI records requested."); see

also Commonwealth v. Parker, 481 Mass. 69, 74 (2018) (stating inferences suggested by prosecutors in closing arguments "need only be reasonable and possible based on the evidence before the jury").

- Commonwealth v. Phillips, 495 Mass. 491 (2025). Defendant was convicted of murder in the first degree and of possessing a firearm without a license. Id. Among other issues raised on appeal, the defendant argued that the prosecutor misstated evidence with respect to a photograph of the defendant during closing arguments. Id. at 502. The photograph was found on the codefendant's cell phone. Id. at 502. The photograph depicted the defendant outside an apartment building. Id. at 495. The cell phone's metadata showed the photograph was taken at approximately the same address where a vehicle was parked after the shooting in question. Id. at 494-95. The prosecutor told jurors that the codefendant "took" the picture of the defendant. Id. at 502. There was no direct evidence to support this claim. Id. at 502. The SJC held that the prosecutor did not necessarily misstate the evidence. Id. at 502. The court determined that it "need not decide whether the cell phone's metadata was sufficient to support an inference that the photograph was taken with that particular cell phone, or by whom[,]" because any error by the prosecutor did not rise to the level of a substantial risk of a miscarriage of justice. Id. at 502.

## J. Special Matters Related to the Use of Digital Evidence in Court

This section covers additional evidentiary matters related to digital evidence, which are not included in other subsections of Chapter II.

- Commonwealth v. Rios, 496 Mass. 11 (2025). Defendant was convicted of murder in the first degree involving a network of co-conspirators. Id. at 12. One of the co-conspirators, Medina, secretly recorded the defendant in the days following the murder on her cell phone. Id. at 17-18. Police learned of these recordings in their initial interview with Medina. Id. at 19. Police "manually transferred" the files from Medina's cell phone to a police department computer. Id. at 30. Police did not conduct a "forensic extraction" using the department's Cellebrite software. Id. at 19. The defendant argued on appeal that the "negligent" handling of the cell phone and extraction of the recordings was a due process violation under the Fifth and Fourteenth Amendments. Id. at 30. The court acknowledged that "the data captured by the file transfer process was not equivalent to the data that would have been captured via forensic extraction." Id. at 30. However, the court held that the defendant's rights were not violated by the failure to conduct a proper forensic extraction and to retain all possible metadata. Id. at 31. The court agreed with the trial judge's conclusion under Commonwealth v. Neal, 392 Mass 1 (1984), that there was no "reasonable possibility" that the forensic extraction would have produced evidence "favorable to [defendant's] cause." Id. at 31. The court reasoned that there was "no concrete evidence" that "defendant's inculpatory statements were somehow derived from exculpatory statements" via another's manipulation of the recordings. Id. at 31-32. The court also noted that any discrepancies in the date and time stamps were addressed at trial. Id. at 32.

- Commonwealth v. Shakespeare, 493 Mass. 67 (2023). Police recovered video surveillance from multiple cameras at several locations including (1) a bus, (2) an ice cream shop and a liquor store that were close to the scene of the crime, (3) a private residence, and (4) United States Department of Homeland Security (DHS) cameras. Id. at 73-74. None of the footage depicted the shooting, but it did place the defendant in proximity to the shooting and suggested motive. Id. at 74-75. At trial, a detective testified about his observations of several videos. Id. at 98. He pointed out the movements of a particular car, which he believed to be a black Toyota Camry. He testified that, on the video, "he saw a man get out of the car, walk toward the area of the back of the shop [where the shooting occurred] minutes before the shooting, and return to the car and drive away after the shooting." Id. at 98. "He testified at several points that one can observe the defendant walking in and out of view in the shop video. He also testified that before he saw the defendant walk into the shop for the first time, he identified him on the ice cream shop video." Id. at 98.

  The SJC held that the detective's "testimony regarding the movements of the black car was properly admitted to assist the jury in focusing their attention to relevant areas in the video, and to orient the jury to the streets and the areas in which the car was traveling." Id. at 99-100. Additionally, the SJC held that the detective's identification of the driver of the black car as wearing a particular color shirt as "'consistent in color to the one that [the defendant] was wearing' was properly admitted to explain why police focused on the defendant in the investigation . . . ." Id. at 100. And the SJC held that the detective's repeated identification of the defendant in one of the videos was not error because (1) the identifications "became pervasive only once counsel began to ask [the detective] on cross-examination what exactly he saw in the video[,]" (2) "the defendant meaningfully raised not only a Bowden argument, but also a third-party culprit argument[,]" and (3) "the judge gave a forceful instruction to the jury during the testimony, which emphasized that [the detective's] testimony was for the purpose of helping the jury understand why police made certain investigatory decisions and that it was the jury's job to decide what they saw in the video." Id. at 100-101.

- Commonwealth v. Moore, 489 Mass. 735 (2022). The defendant was convicted of first-degree murder for the shooting deaths of four victims in the so-called 2010 "Mattapan Massacre." Id. at 736. He moved for a new trial based on, *inter alia*, ineffective assistance of counsel for failure to use the defendant's cell site location information (CSLI) to cast doubt on a witness's "testimony that the defendant was present for the killings." Id. at 747. More specifically, the defendant argued that the location of the towers to which his phone calls connected around the time of the murder show that he was not present for the killings. Id. The SJC found that trial counsel was not ineffective. Id. First, counsel moved "to exclude CSLI data from the trial, arguing that it was unreliable." Id. at 748. This data showed which towers Moore's phone was connected to for each call. Id. At trial, multiple witnesses testified that calls "usually but not necessarily" connect to "the geographically closest tower." Id. Second, after the motion to exclude CSLI data was denied, counsel cross-examined witnesses about this data and argued in closing that the CSLI data did not support the defendant's guilt. Id. Finally, the court concluded that counsel was not ineffective for failing to highlight CSLI records because they were "arguably inculpatory." Id.

- Commonwealth v. Kostka, 489 Mass. 399 (2022). Timothy Kostka was convicted of murder in the first degree and home invasion in connection with the death of Barbara Coyne. 489 Mass. 399. He challenged as a discovery violation the Commonwealth's failure to provide the complete CSLI data regarding the location of his cell phone in the time periods immediately before and after the murder. Id. at 413. The SJC held that there was no Brady violation in the failure to disclose the CSLI data, because that data was not exculpatory. Id. at 414. The data was not exculpatory because "the connection of the defendant's telephone to towers in multiple areas of Boston and a neighboring city, within minutes, tended to call into question the reliability of the CSLI data . . . ." Id. The SJC cautioned that the result of the detective's investigation likely fell "within the ambit of the allowed motion for nonmandatory discovery of the results of investigations and scientific tests and should have been provided." Id. But, the failure to provide that evidence did not require reversal because production of that information "would have made no difference," given other, reliable evidence of the defendant's location shortly after the time of the murder. Id. at 415.

## K. Digital Evidence Management and Disposition

- Commonwealth v. James, 493 Mass. 828 (2024). The SJC held that proceedings consistent with the requirements of G. L. c. 276, §§ 4-8, were necessary to determine whether hard drives that potentially contained child pornography could be forfeited and that a judge's determination that forfeiture would be in the "public interest" was not sufficient. Id. at 829. After police seized from the defendant's home items including an external hard drive, a cell phone, and a computer tower holding five internal hard drives, those items were examined by both a forensic examiner and a state trooper with experience related to child pornography investigations. Id. at 830-31. On one hard drive, the examiner found photos of the juvenile victim and of the victim and the defendant together. Other photos of nude or partially nude unidentified people and pornography were found on some of the other drives, but the trooper could not determine the age of the people in those photos. Id. at 831. The defendant moved for the return of the items after pleading guilty and subsequently appealed from the partial denial of that motion. Id. at 832. On appeal, the Commonwealth argued that forfeiture was in the "public interest" because of the odious nature of the crimes for which the defendant was convicted and because the disputed hard drives may contain child pornography. Id. at 839. The court disagreed, stating, "the defendant's property may not be forfeited based merely on the speculative concern that harm could occur if the disputed property were to be returned." Id. at 840. The court instead held that the required procedure under G. L. c. 276, §§ 4-8, must be followed, including notice and a trial, at which a judge may evaluate the merits of the competing arguments. Id. at 840. The case was remanded to the Superior Court for further proceedings consistent with the SJC's opinion. Id. at 840-841.

# III. Cybercrimes

## A. Possession of Child Pornography

### 1. Multiple Convictions Require Multiple "Caches"

In prosecuting possession of child pornography, each "cache" of pornography counts as one unit of prosecution. See Commonwealth v. Rollins, 470 Mass. 66, 73–75. That is, "a defendant's possession of a single cache of one hundred offending photographs in the same place at the same time gives rise to a single unit of prosecution pursuant to [Mass. Gen. Laws ch. 272,] § 29C" rather than one-hundred separate charges and convictions. Id. at 74. To support multiple prosecutions for possession of child pornography in compliance with the Double Jeopardy Clause, that possession must be "'sufficiently differentiated by time, location, or intended purpose.'" Id. at 73 (quoting Commonwealth v. Rabb, 431 Mass. 123, 130 (2000) (with internal quotation marks omitted)).

- Commonwealth v. Wassilie, 482 Mass. 562 (2019). The defendant, who was convicted on 15 separate indictments relating to secretly videotaping nude or partially nude adults and children, appealed, arguing that the judge erred in ruling that the proper units of prosecution were the individual victims rather than the individual episodes of surveillance. Id. at 563. The defendant concealed his cell phone in a unisex, one room bathroom without stalls at an angle that gave a clear view of the toilet. Id. at 563-564. He recorded two videos on the same day, and these videos captured "genitalia of children and adults, male and female"—a total of seventeen adults and five juveniles. Id. On appeal, the court cited precedent that, for the purpose of determining whether particular conduct constitutes a single offense or multiple offenses, there are two categories of statutes. Id. at 567. "One category is focused upon the prevention of violence or physical injury to others." Id. In this category, a single incident can give rise to multiple indictments, based on the number of victims. Id. The other category is directed at "punishing the defendant for conduct offensive to society." Id. For this second category, separate indictments for separate victims are not appropriate. Id. at 568. Some crimes, like the one at issue here, do not fit neatly into either category. Id. The defendant argued that the statute reflects an intent to punish the physical act of recording, but the court read the statute as punishing criminal acts that invade an individual's privacy. Id. The court also rejected the defendant's reasoning on the grounds that his statutory interpretation would produce the "absurd result" of allowing people who take illicit photos of multiple people to be tried as if they had one victim. Id. at 571. Based on this statutory analysis, the court upheld the lower court's decision to use a per victim unit of prosecution. Id. at 578.

### 2. Brief Possession is Sufficient

Brief possession of offending images is sufficient to sustain a violation of Mass. Gen. Laws ch. 272, § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 329–30 (2011). Evidence of prolonged or continued control is not needed. Id. (citing Commonwealth v. Harvard, 365 Mass. 452, 458 (1969)). In Hall, although the defendant's cell phone no longer contained child pornography and though there was no confirmation that the defendant had viewed the pictures sent to him by the victim, the defendant was

found guilty of possession of child pornography because the fact that he had enticed and encouraged the victim combined with the fact that he received the images allowed a jury to find that he had possessed them. Id. at 327–29.

### 3. Receipt by Cell Phone is Sufficient

Confirmation that defendant's cell phone received picture messages from the victim, where the defendant enticed the victim to take and send the picture messages, is sufficient to show control and possession of such photos in violation of Mass. Gen. Laws ch. 272 § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 327–29 (2011).

### 4. Malware and Computer Viruses Defense

The First Circuit notes that "we must be cognizant of 'the prevalence and sophistication of some computer viruses and hackers that can prey upon innocent computer users' by placing child pornography on their machines, but 'the specter of spam, viruses, and hackers must not prevent the conviction of the truly guilty.'" United States v. Rogers, 714 F.3d 82, 87 (1st Cir. 2013) (quoting United States v. Pruitt, 638 F.3d 763, 766–67 (11th Cir. 2011)). In Rogers, the possibility that the child pornography found on the defendant's computer was a result of malware was ruled out by forensic analysis (where an analyst installed the same malware on another computer and no child pornography was found) and corroborating evidence (child pornography found on another computer, browsing history matching an interest in child pornography, and evidence that some of the pornography had been deleted by the defendant). Id.

### 5. Probable cause / Staleness in Child Pornography Cases

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that the probable cause in the affidavit in support of the warrant to search his home was stale. Id. In Guastucci, police were investigating the upload of a single image of child pornography from the defendant's home to Skype seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time, the court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the court separately identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant

affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]", an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

## B. Statutory Terms of General Laws Chapter 272

### 1. "Dissemination"

"The definition of 'disseminate' includes 'publish, produce, print, manufacture, distribute, . . . exhibit or display.' The statutory emphasis is on the content of the material and the intent of the person disseminating such material; the draftsmen were not so much concerned with the manner in which the image was distributed, exhibited, or displayed. The statutes criminalize such dissemination whether accomplished by way of hand, mail, facsimile, or through the use of e-mail. The judiciary ought, absent constitutional inhibitions, give effect to the purpose of the law gleaned from the Legislature's choice of language." Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *2 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 31 (internal citation marks omitted)).

"Possession" is not an element of the crime of "dissemination." Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *4 (Sep. 22, 2016) (unpublished). To "disseminate" is defined as 'to import, publish, produce, print, manufacture, distribute, sell, lease, exhibit or display." Id. at *5 (quoting Mass. Gen. Laws ch. 272, § 31). In Moore, the Appeals Court held that "[t]o infer a requirement of possession would be to add a requirement not expressed by the Legislature." Id. The term "dissemination" also connotes some form of distributive act beyond showing something to another. Id. Consider Commonwealth v. McDonagh, 480 Mass. 131 (2018), where the defendant showed nude pictures on his computer to his minor son. The Commonwealth charged the defendant with various offenses, including dissemination of obscene matter (in violation of Mass. Gen. Laws ch. 272, § 29). Id. at 132. On appeal, the Commonwealth conceded that the evidence was insufficient to prove "dissemination." Id. at 144–45.

- Commonwealth v. Ubeda, 99 Mass. App. Ct. 587, 2021 WL 1974182 (2021). The defendant was convicted on multiple charges, including "aggravated rape and abuse of a child, posing or exhibiting a child in a state of nudity, disseminating child pornography, trafficking of a person for sexual servitude, extortion by threat of injury, larceny over $250, assault and battery, and trafficking of a person under eighteen years of age for sexual servitude." Id. at *1.On appeal, he argued that there was insufficient evidence of dissemination because the defendant only sent the collages with nude images of the victim to the victim herself. The court found that evidence was sufficient "to prove the element of dissemination" because dissemination, as defined by statute, requires neither "publication to a broad audience," nor "receipt by a third party." Id. at 5 (citing G.L. c. 272, § 31, which defines "disseminate" as "to import, publish, produce, print, manufacture, distribute, sell, lease, exhibit or display."). Further, the victim's willing participation in taking the photos was irrelevant because G.L. c. 272, § 29B (d) specifically provides that a minor is incapable of consenting in a prosecution for dissemination of child pornography.

### 2. Computer "Depictions"

"The Legislature was unconcerned with how the photographically created image is stored or communicated." Commonwealth v. Hall, 80 Mass. App. Ct. 317, 326 (2011). "[T]he Legislature's creation of a separate and distinct category for 'depiction by computer' manifests an intent to give special treatment to the unique issues presented by computers, including the fact that stored data, although intangible in their unprocessed form, are readily transferrable to a graphic image." Id. at 327 (quoting Mass. Gen. Laws ch. 272, § 29C).

"Depiction by computer," as that phrase is used in § 29C, includes an unopened file on a hard drive—not only a file that is reduced to a hard copy, or one that is disseminated. Commonwealth v. Hinds, 437 Mass. 54, 63–64 (2002).

### 3. Child Enticement

"[I]n order to constitute enticement of a victim, the defendant need not physically meet the victim at the same place to which he entices the victim to go" given modern and electronic digital technology. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 323 (2011). In Hall, the Appeals Court noted that the defendant's enticement of the victim via cell phone text messages to go to a private place and take naked photographs to send to him can qualify as enticement. Id. However, given the potentially duplicative offense of posing a child in a state of nudity, the court held that the defendant must lure the child to a place of his/her choosing, not the victim's choosing. Id at 324–25. As this element was missing in Hall, the defendant's enticement charge was set aside. Id. at 325.

### 4. "Visual Material"

"The Legislature's objective of including a broad range of 'visual material' in its proscription is further demonstrated by Section 31's second sentence which provides: '[u]ndeveloped photographs, pictures . . . and similar visual representations or reproductions may be visual materials notwithstanding that processing, development or similar acts may be required to make the contents thereof apparent.' Thus, in determining whether an image is a 'visual material' within Mass. Gen. Laws ch. 272, the manner of its dissemination is insignificant. Whether further acts are required to make the image apparent to the naked eye, by, for example, keying a computer board, does not render the image any less a 'visual material.'" Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *3 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 29C).

### 5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31

The SJC examined the definition of "nudity" under §31 in Commonwealth v. Provost, 418 Mass. 416 (1994). In this case, the defendant took photographs of children in the pool and boys in the locker room. Id. at 417–18. One child struck different poses and his partially covered scrotal area was visible in two photographs. Several others showed the child displaying his bare buttocks ("mooning" the defendant). Id. at 418. The SJC provided the following analysis of the statutory meaning of "nudity": "The defendant claims that his activities do not fall within the ambit of § 29A(a). He first contends that the photographs do not depict a minor in a state of nudity within the meaning of, which defines 'nudity'

as: 'uncovered or less than opaquely covered human genitals, pubic areas, . . . or the covered male genitals in a discernibly turgid state.' Although [the child] had his underwear on, in two of the photographs portions of his pubic and genital area are clearly visible. The statute does not require that the areas be completely uncovered. It is enough that a portion of the genital area is visible." Id. at 418 (quoting Mass. Gen. Laws ch. 272, § 31).

### 6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A

A "performance" under Mass. Gen. Laws ch. 272, § 29A "does not expressly or implicitly require the physical presence of 'one or more persons.' In view of the advances in technology, a violation of the statute may occur without the defendant's physical presence." Commonwealth. v. Bundy, 465 Mass. 538, 545 (2013) (finding the statutory definition of performance satisfied by victim masturbating facing a camera attached to a device that, through an Internet connection, resulted in the image being broadcast to the defendant for him to view).

A "performance" occurs "before one or more persons" even when the only audience member is the person who enticed or encouraged the performance because to hold otherwise would circumvent the plain meaning of "one." Id. at 544.

### 7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A

Mass. Gen. Laws ch. 272, § 29A(b), provides in relevant part: "Whoever . . . hires, coerces, solicits or entices, employs, procures, uses, causes, encourages, or knowingly permits such child to participate or engage in any act that depicts, describes, or represents sexual conduct for the purpose of representation or reproduction in any visual material, or to engage in any live performance involving sexual conduct, shall be punished . . . ." (quoted in Com. v. Bundy, 465 Mass. 538, 539 n.2 (2013)). In Bundy, the jury was instructed as follows on a charge under this statute:

> [I]n proving [the element of live performance], the Commonwealth must establish beyond a reasonable doubt that it was [the defendant's] specific intent to solicit, entice, cause, or encourage [the victim] to engage in a live performance involving sexual conduct. In determining whether the defendant possessed such a specific intent, [the jury] may consider all facts and circumstances, including the defendant's acts and statements. The statute also permits the Commonwealth to establish alternatively that the defendant knowingly permitted [the victim] to engage in a live performance involving sexual conduct.

Id. at 542.

The meaning of "knowingly permit" was at issue in Commonwealth. v. Provost, 418 Mass 416 (1994). The defendant in Provost asserted that "the depiction of [a victim's] pubic area was unintentional and that, since [the victim] voluntarily struck the various poses without instruction, [defendant] did not 'knowingly permit' him to pose in a state of nudity." Id. at 419. The court rejected this argument and held that:

> The photographs themselves suggest that the defendant knowingly permitted [the victim] to pose with a portion of his pubic region and genitals exposed. He took a series of well-focused photographs at various points in the process of [the victim's] dressing. [The victim's] genital area is prominent in many of the photographs. The defendant admitted that he sometimes took photographs of nude boys for sexual gratification. There was sufficient evidence, therefore, for the judge to conclude that the defendant knowingly permitted [the victim] to pose in a state of nudity. Furthermore, the fact that the defendant continued to take the photographs as [the victim] struck different poses certainly supports the inference that he "encouraged" [the victim] to pose in a state of nudity.

Id. at 419.

#### 8. Lewdness

In Commonwealth v. Rex, 469 Mass. 36 (2014), during a standard cell inspection prisoner Rex was found in possession of seven photographs of naked children. Id. at 37. The photos were from National Geographic, a sociology textbook, and a naturist catalogue. Id. The court held that the indictment for possession of child pornography was properly dismissed because the children depicted were not in unnatural poses and their genitals were not the focus of the photo. Id. at 47. Thus the photos did not depict lewdness—just nakedness. Id. at 47–48. "It is well settled that nudity alone is not enough to render a photograph lewd." Id. at 44 (quotation omitted).

#### 9. "Lascivious Intent" as defined by General Laws Chapter 272, Section 29B

- Commonwealth v. Ubeda, 99 Mass. App. Ct. 587, 2021 WL 1974182 (2021). The defendant was convicted on multiple charges, including "aggravated rape and abuse of a child, posing or exhibiting a child in a state of nudity, disseminating child pornography, trafficking of a person for sexual servitude, extortion by threat of injury, larceny over $250, assault and battery, and trafficking of a person under eighteen years of age for sexual servitude." Id. at *1. On appeal, he argued that there was insufficient evidence "to prove the element of lascivious intent" in his conviction for disseminating child pornography. Id. at *6. The court disagreed, noting that there are several ways to show that the defendant had "lascivious intent," which is defined by statute as "a state of mind in which the sexual gratification or arousal of any person is an objective." Id. Here, the photographs were of a "graphic sexual nature," and "included photographs of [the victim] engaging in masturbation and lewd exhibition of the genitals." Id. Thus, "the jury could have found that the defendant had his own sexual gratification as an objective in creating and sending the collages to [the victim]. Id. (quotations omitted).

## C. Special Conditions of Probation

Special conditions of probation can be unconstitutionally vague — facially or as applied — if they do not give fair notice to a defendant of the scope of prohibited activity. Commonwealth v. Ruiz, 453 Mass. 474, 479 (2009). A defendant "cannot be found in violation of probationary conditions that might have been intended or would have made sense, only of those that are unambiguous and of which he has

notice," Commonwealth v. King, 96 Mass. App. Ct. 703, 710(2019) (citing Commonwealth v. Lally, 55 Mass. App. Ct. 601, 603 (2002)), and "ambiguities in probation conditions are construed in favor of the defendant." Lally, 55 Mass. App. Ct. at 603 (citing Commonwealth v. Power, 420 Mass. 410, 421 (1995)).

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography." Id. at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. The court found this sufficed to put the defendant on fair notice that possession of "explicit stories describing the rapes of young children" would violate his probation. Id. at 786-87. However, the court found that a reasonable person would not consider photographs of adults in their underwear or with their hands covering their genitals to be pornographic. Id. Therefore, they were not "so inarguably pornographic as to put the defendant on fair notice that he was violating probation by possessing them," where the photographs "depicted no sexual activity or nudity, and it [was] unclear whether the intent behind them was to arouse sexual excitement." Id. at 786.

- Commonwealth v. King, 96 Mass. App. Ct. 703 (2019). Defendant, who had pled guilty to possession of child pornography, was subject to special probation conditions which provided, in relevant part, that: "(3) The probationer shall not access any internet services from any handheld device (e.g., Palm Pilots, Blackberries, and mobile telephones)"; and "(4) The probationer shall not use, enter, visit, participate in, or remain in any online chat room, bulletin board service, message board service, social networking site or service (for example, Facebook.com, Twitter.com, Instagram.com), or any other online communication service, with the sole exception of electronic mail." Id. at 704. The discussion during the plea colloquy clarified the scope of these two conditions such that, in summary, the third condition prohibited any Internet access from handheld devices, and the fourth condition prohibited the use of social media on any device (except email). Id. at 705. When read together, the two conditions appeared to permit non-social-media Internet access (including email) from non-handheld devices. Id. While on probation, the defendant accessed "images of young girls wearing scanty dance costumes in provocative poses" and annotated print-outs of these materials by hand with the girls' names, ages, information about their siblings, and smiley faces in some cases. Id. at 706. He accessed these and similar materials using search engines (e.g., Google) and Wikipedia on computers, and emailed some of them to himself. Id. at 705. While acknowledging that the defendant's conduct was "troubling," the Appeals Court held that "the evidence was insufficient to permit the judge to find that he violated special condition four," because "[s]pecial condition four did not prohibit the defendant from using the Internet generally, or downloading information from it." Id. at 710 ("the defendant cannot be found in violation of probationary conditions that might have been intended or would have made sense, only those that are unambiguous and of which he has notice.").

  In dicta, the King court wrote: "with the benefit of appellate hindsight, one cannot help but ask whether special condition four should not have been written differently and, in particular, whether

it should have expressly prohibited the defendant from using a computer to access images or information about children, whether via the Internet or otherwise." Id. at 710. Further, "recogniz[ing] both the importance and difficulty of drafting clear special conditions of probation, especially when they involve technology," the court suggested it would "be helpful to supplement existing sources with a set of model, nonbinding special conditions" "for sex offenders and those who use technology to commit crimes," among others. Id. at 711.

Special conditions of probation that refer to pornography may use the "common meaning" of pornography and may prohibit constitutionally protected activity that may not be the basis of an independent criminal conviction. Hamilton, 95 Mass. App. Ct. at 787.

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography,." Id. at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. Defendant argued that under Free Speech Coalition, which held facially unconstitutional a statute that criminalized possession of "sexually explicit images that appear[ed] to depict minors" but were actually "created by using adults who look like minors or by using computer imaging," Ashcroft v. Free Speech Coalition, 535 U.S. 234, 239–40 (2002), the explicit stories he posessed were not pornography because they were "'fantas[ies]' that [did] not involve actual children." Hamilton, 95 Mass. App. Ct. at 787. The court rejected defendant's argument, noting "that a probation condition is enforceable, even if it infringes on a defendant's ability to exercise constitutionally protected rights, so long as the condition is 'reasonably related' to the goals of sentencing and probation." Id. (quoting Commonwealth v. Lapointe, 435 Mass. 455, 459 (2001)). The court was not considering a facial challenge to a criminal statute, but rather had to decide the question of "whether a reasonable person in the defendant's circumstances would have known that the stories constitute pornography in violation of his probation conditions." Id. Thus, "[t]he discussion in Free Speech Coalition [was] not germane to that question because the common meaning of pornography is not limited to materials depicting actual people. For example, had the defendant been found in possession of computer-generated images of what appeared to be children engaging in sexual activity, he indisputably would have been in violation of his probation, even though Free Speech Coalition says that those same images cannot be the basis of a criminal conviction." Hamilton, 95 Mass. App. Ct. at 787.

# IV. Expert Testimony About Technology

Expert testimony is ordinarily required when the subject of the testimony "is beyond the common knowledge or understanding of the lay juror." Commonwealth v. Sands, 424 Mass. 184, 186 (1997). Even if a juror does not have personal experience of a technology, a lay juror, from common experience and knowledge, may understand the required concepts when provided sufficient non-expert testimony and evidence. Commonwealth v. Bundy, 465 Mass. 538, 546 (2013) (finding the victim's testimony and photographic evidence sufficient to keep jurors from engaging in conjecture about an Xbox and its accessories) (citing Commonwealth v. Sands, 424 Mass. 184, 186 (1997)).

- Commonwealth v. Cronin, 495 Mass. 170 (2025). The Supreme Judicial Court affirmed the convictions of possession of child pornography. On appeal, the defendant challenged the lay testimony about Cellebrite extractions. When a lay witness—here a police officer—testifies and answers questions regarding technical systems (i.e., Cellebrite), the inquiry is whether that testimony "required any specialized knowledge." Commonwealth v. Mason, 485 Mass. 520, 538 (2020). In Cronin, the lay witness testified that they were not an expert and that their testimony was based on personal knowledge of the system (i.e., general extraction procedure and specific procedure on defendant's phone). The Court noted that the witness's explanation of the contents of the extraction report required no scientific, technical, or specialized knowledge and that the report itself was properly admitted. However, the lay witness's testimony crossed the line into expert testimony when the witness testified about Cellebrite's accuracy or reliability.

- Commonwealth v. Arrington, 493 Mass. 478 (2024). The Commonwealth filed a motion in limine to permit expert testimony regarding frequent location history ("FLH") data retrieved from a full-file system extraction of an iPhone to establish that the defendant's device was in the immediate vicinity of the crime scene at the time the crime was committed. Id. at 479. The SJC noted that no court in the Commonwealth, "or apparently in any other jurisdiction in the country," had admitted FLH data. Id. at 479. The trial judge denied the motion because the testimony did not meet the requirements of the Daubert-Lanigan standard; specifically, the Commonwealth failed to meet its burden of showing that the proffered expert testimony established the reliability of the FLH data in the case. Id. at 479.

  As of 2015, FLH data referred to the amalgamation of location data points generated by the device from various sources such as "global positioning system (GPS) data, nearby wireless computer network (Wi-Fi) access points, short-range wireless Bluetooth connections, and cell site location information (CSLI)." Id. at 481. The output of the aggregated location data points created "a longitude and latitude coordinate point and a circle around it," which represents the device's approximate movement over time, the radius of the circle being the "uncertainty" in the FLH data. Id. at 481. FLH data also produced estimated time stamps of when the device entered and left a particular location. Id. at 482. Apple's algorithm that produced FLH data is proprietary, and "the Commonwealth's expert did not have access to the algorithm itself during his testing of FLH data reliability." Id. at 482.

The SJC determined that the trial judge did not abuse his discretion in denying a motion to permit expert testimony on FLH data. Id. at 490. The court concluded that the trial judge did not abuse his discretion in deciding that the Commonwealth failed to meet its burden of showing "that FLH data have been generally accepted as reliable by the scientific community." Id. at 492. Additionally, "the trial judge did not abuse his discretion in holding that there was not sufficient testing to establish the reliability of FLH data." Id. at 493. Nor did the trial judge "abuse his discretion in holding that the Commonwealth had failed to show evidence that FLH data have been subjected to peer review or publication." Id. at 496-97. And, finally, the trial judge did not abuse his discretion in deciding that the Commonwealth failed to meet its burden of establishing that FLH data do not have an unacceptably high known or potential rate of error. Id. at 496-97.

In April of 2026, the Superior Court, Ames, J., allowed the Commonwealth's motion for reconsideration and found, after further evidentiary hearings, that FLH was sufficiently reliable to be admitted at trial. Judge Ames found that (1) FLH data is generally accepted as reliable in the relevant scientific community; (2) FLH data has been and can be subjected to objective testing; (3) that while there is one scholarly article, the absence of scholarly writing on FLH data is not indicative of an absence of examination of it; (4) that the precision of FLH data, does not have an unacceptably high known or potential error rate; and (5) that there is some regulation of underlying location data points but the regulations do not govern FLH data itself.

The court, in its Daubert-Lanigan analysis, made two conclusions. First, while the court found that FLH data has "not been subject to significant formal testing or scholarly analysis," it noted that scholarly review and publication are "not a sine qua non of admissibility." Ready v. Commonwealth, No. Civ. A. 00-10390 SDP, 2002 WL 1255800, at *16 (Mass. Super May 17, 2002) (Muse, J.,), aff'd sub nom, In Re Ready, 63 Mass. App. Ct. 171 (2005), quoting Daubert, 509 U.S. at 593.

Second, the court held that despite a dearth of scholarship and a lack of access to the underlying FLH code, the record established that FLH data is sufficiently reliable for the purposes for which it is offered in trial. "Foremost, the Commonwealth has demonstrated, through the testimony of two established experts, that FLH data is generally accepted as reliable by the digital forensics community." The "Commonwealth has now performed testing of FLH data consistent with industry standards and best practices, the results of which are consistent with both the testimony of Whiffin and Hyde[.]" The court noted that, any "limitations of FLH data, once explained, are within the ken of a lay jury, and they are all proper fodder for cross-examination and rebuttal evidence." "The Commonwealth has demonstrated that 'FLH data can reliably establish that an iPhone was in an approximate area at an estimate time' sufficient to satisfy gatekeeper reliability. See Arrington, 493 Mass. at 498 (Lowy, J., concurring).

- Commonwealth v. Hinds, 494 Mass. 681 (2024). The Supreme Judicial Court affirmed the defendant's convictions of assault and battery by means of a dangerous weapon. On appeal, the defendant challenged the admission of certain text messages and social media posts and the exclusion of a social media expert on surrebuttal. The Court held that the text messages and social media posts, containing threats and racial epithets that establish prior bad acts, intent, and

disproved a claim of self-defense, had probative value and were admissible so long as the probative value outweighed the risks of unfair prejudice to the defendant, "even if not substantially outweighed by that risk." Commonwealth v. Correia, 492 Mass. 220, 228-29 (2023). Additionally, the trial judge did not abuse his discretion in excluding an alleged social media expert witness when applying the Durning factors and finding that the late disclosure prejudiced the Commonwealth. See Commonwealth v. Durning, 406 Mass. 485, 494-95 (1990). The expert's identity, though known to the Commonwealth, was disclosed relative to an entirely different subject matter than her proposed surrebuttal testimony. Under those circumstances, the Commonwealth would have been unable to investigate the expert's opinions and statements.

- Commonwealth v. Shepherd, 493 Mass. 512 (2024). The defendant was convicted of felony murder for shooting an acquaintance who unexpectedly fought back during a botched larceny at the acquaintance's home. Id. at 513-18. The Commonwealth used CSLI evidence to show that the defendant's phone had been used to make a call around the time of the incident and in the vicinity of the victim's home. Id. at 518. On appeal, the defendant claimed that trial counsel was ineffective for failing to retain an expert to challenge the Commonwealth's CSLI evidence and failing to object to the CSLI records custodian's qualifications to testify to how cell towers work. Id. at 534-36. The Court rejected each argument. Id. at 534-36.

  As to the first claim, the SJC held that trial counsel's strategic decision to rely on the cross-examination of the Commonwealth's CSLI witness was not unreasonable. Id. at 534-35. At trial, counsel elicited several concessions from the Commonwealth's CSLI witness to highlight the limitations of CSLI. Id. at 535. The Court reasoned that there is no categorical requirement to present expert or documentary evidence to support an argument, especially where other evidence is presented to support it. Id. The Court noted that the defendant's post-trial expert even opined that the coverage area for the call was somewhat larger than the Commonwealth's witness testified but still encompassed the victim's home. Id. at 535 n.37.

  The Court then went on to reject the defendant's second claim that trial counsel was ineffective for failing to object to the CSLI records custodian's qualifications to testify to how cell towers function. Id. at 535-36. The Court held that even if the defendant was correct in his assertion, the error did not "raise a substantial likelihood of a miscarriage of justice" because the data only served to corroborate a strong case against the defendant. Id.

- Commonwealth v. Corey, 493 Mass. 674 (2024). In a first-degree murder case, the defendant argued that her trial counsel was ineffective for failing to call a CSLI expert to testify about her location on the night of the murder. Id. at 675. In support of her motion for a new trial, the defendant submitted an affidavit by a CSLI expert that allegedly revealed significant gaps in cell phone activity during the "critical hours of the night" of the murder, with the only connections being to a distant cell tower at 10:42 p.m. and 4:06 a.m. Id. at 682, 685. The Commonwealth submitted its own expert's opinion regarding the defendant's CSLI data, which noted that "a cell phone does not always connect to the closest cell tower, meaning that the distance of a cell tower is not always determinative of the cell phone's location." Id. at 683. The SJC, agreeing with the

Commonwealth's expert, found that evidence of the defendant's CSLI "could not have conclusively placed her far from [the crime scene] on the night of the killing." Id. at 685. The SJC held that trial counsel's decision not to call a CSLI expert was not ineffective assistance, because the decision was not manifestly unreasonable at the time it was made; the CSLI weakly supported the defendant's case, and corroborated part of the Commonwealth's case. Id. at 686.

- Commonwealth v. Middleton, 100 Mass. App. Ct. 756 (2022). In an appeal from convictions for stalking and violating a restraining order, the defendant argued that the trial court erred in admitting into evidence thirty-three emails without proving that the defendant had sent the emails. Id. at 757. The defendant further argued that the trial court erred by admitting email records summonsed from Google, without expert testimony to explain "some dates and times and codes" contained in the records. Id. at 761. The Appeals Court rejected both arguments. Id. at 757.

  The court held that the trial judge appropriately determined that sufficient evidence existed "'for a reasonable jury to find by a preponderance of the evidence that the defendant authored' the communication." Id. at 760 (quoting Commonwealth v. Oppenheim, 86 Mass. App. Ct. 359, 366 (2014) and Commonwealth v. Purdy, 459 Mass. 442, 451 (2011)). The communication can be "authenticated by circumstantial evidence, including details of defendant's and victim's lives." Id. (citing Commonwealth v. Welch, 487 Mass. 425, 440-442 (2021)). Relevant factors included the presence of unique personal references and nicknames in the emails, references to prior conversations between the defendant and victim, and other personal identifying information. Id. at 758-59. The court further held that "expert testimony was not necessary for the jurors to understand the Google records." Id. at 761. More specifically, expert testimony was not necessary here because "understanding the dates of service for each account did not require any 'scientific, technical, or other specialized knowledge.'" Id. at 761 (quoting Commonwealth v. Canty, 466 Mass. 535, 541 (2013)). Moreover, no expert testimony about IP addresses was necessary, where "[t]he Google records did not contain any IP addresses." Id. at 762.

- Commonwealth v. Davis, 487 Mass. 448 (2021). Following his conviction for armed assault with intent to murder and other charges, the defendant argued on appeal, among other things, that the GPS device evidence introduced at trial was not sufficiently reliable, that the maps of the GPS data violated his confrontation rights, and that the cell phone video introduced was not authenticated. Id. at 449-50. The GPS device at issue was an ankle monitor called an "ExactuTrack 1" (ET1). Id. at 449. At trial, the Commonwealth introduced expert testimony from a manager at the manufacturing company of the ankle monitors. Id. at 452. During *voir dire*, the expert testified that location and speed determinations work differently, and that the manufacturer formally tested the ankle monitor's ability to determine location but not speed. Id. at 453. The court held that the Commonwealth failed to lay the proper foundation to admit the ET1's speed measurements, and that the trial judge therefore erred in admitting the speed evidence. Id. at 456. (There was no error in admitting the location data, however. Id. at 460.) The court emphasized that GPS technology is generally accepted as reliable but held that this showing was not sufficient because ET1 is a new type of GPS device. Id. at 456-57. Where a new type of device is at issue, the court found that the Commonwealth could meet its reliability burden by, for example,

showing that the device has "been tested or peer reviewed," or that the new model applies the same methodology as the prior one. Id. at 457. Here, the Commonwealth failed to make either showing with respect to ET1's speed data. Id. Because the error was prejudicial, the court reversed the defendant's convictions. Id. at 450, 461.

The defendant also argued that maps depicting his location based on data from ET1 were hearsay that violated his confrontation clause rights. Id. at 464. The court rejected this argument because all of the information in the maps was computer-generated. Id. at 465. "Whether a computer record contains a statement depends on whether the record is 'computer-generated,' 'computer-stored,' or a hybrid of both." Because computer-generated records "are created solely by the mechanical operation of a computer and do not require human participation," they cannot be hearsay. Id.

- Commonwealth v. Javier, 481 Mass. 268 (2019). In this first-degree murder case, the defendant argued, among other things, that the trial judge erred in admitting opinion testimony by a cell phone company employee interpreting CSLI information. Id. at 269. The defendant argued that the employee, who was not an engineer, should not have been permitted to testify about how cell sites operate and how to locate a cell phone based on historical cell site information. Id. at 277, 285. The SJC noted that it had previously expressed some doubt—in an appeal by the defendant's co-venturer, see Commonwealth v. Gonzalez, 475 Mass. 396 (2016)—about the propriety of the phone employee's testimony in two respects. Javier, 481 Mass. at 286. In particular, the SJC explained in Gonzalez that the employee's testimony "'that calls are 'typically' transmitted through the closest cellular site, and that a call from [a particular] address was unlikely to have been transmitted through [a particular cell site] . . . may well have required a witness with greater technical expertise.'" Id. (quoting Gonzalez, 475 Mass. at 412 n.37). The Javier court also noted, however, that the employee "properly qualified his testimony and explained that, even where a particular cellular telephone was most likely to connect to the nearest tower, there were many reasons why that might not happen," and therefore "the fact that he did not know or investigate the reasons why particular calls had connected to particular towers did not prejudice the defendant." Id. at 286. The SJC concluded that, "while it might have been better practice to exclude evidence that was of little assistance to the jury and that possibly could have been confusing, the judge did not abuse her discretion in allowing [the phone employee's] testimony about certain aspects of the CSLI." Id. at 286–87. Moreover, the portion of the employee's testimony "concerning the reasons that cellular telephones connect to cell towers, and what he 'expected' a particular telephone would be most likely to do here, would not have had any impact on the jury's verdict." Id. at 287.

- Commonwealth v. Lavin, 101 Mass. App. Ct. 278 (2022). In this armed home invasion case, the defendants argued on appeal that "the State trooper who testified regarding the CSLI overstated its accuracy or attached too much certainty to its precision." Id. at 295. The defendants also claimed that the expert's testimony that the cell phone "moved somewhere along the Route 9 corridor," id. at 297, should not have been allowed and that the trooper's use of chalks to diagram movements of cell phones was improper. The court concluded that the trial judge properly

allowed the expert's testimony about CSLI. Id. at 296-97. Citing Commonwealth v. Javier, 481 Mass. 268, 286 (2019), the court acknowledged that an expert should not claim "that a cell phone must have been near a particular tower when it connected to that tower." Id. (quotation omitted). The expert should explain that there are many reasons why a cell phone might not connect to the nearest tower, and the trooper did provide such a qualification in this case. Id. In addition, the trooper properly qualified his use of chalks (which were not admitted into evidence) to portray circles corresponding to cell phone locations during various calls. Id. "The trooper explained that the circles merely reflected '[seventy] percent of the way to the next available tower,' and he was 'not saying the phone was within that circle.' Rather, the circles were 'an estimation' or 'just an approximation of the area that that cellphone tower may cover.'" Id. In sum, the court found no error, "where the trooper did not overstate his ability to predict the location of the defendant's cell phone based on CSLI data." Id. at 297.

- Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *3 (2016) (unpublished). In an appeal from convictions for possession and dissemination of child pornography claiming ineffectiveness of counsel for failure to object to the testimony of the Commonwealth's digital evidence analyst and to request a Daubert-Lanigan hearing to challenge the reliability and the admissibility of his testimony, the Appeals Court found the claim unfounded. Id. at *3. The prosecution's case was based on evidence found on the defendant's laptop. Id. at *1. The AGO analyst connected the laptop's hard drive to a "write blocker"—thus preventing any data additions or removals—and then created a duplicate image of the drive with a program called Encase. Id. A search of the duplicate image resulted in the discovery of three (3) peer-to-peer file sharing programs: "(1) LimeWire (containing more than 900 videos and images of child pornography); (2) eMule (containing more than 400 videos of child pornography); and (3) Ares (containing several search terms consistent with child pornography)." Id. at *1 The AGO analyst also examined the browsing history, text messages, and photographs on the laptop and the defendant's cell phone to corroborate his ownership and exclusive use of the two items. Id. The court found that the Commonwealth presented a strong case at trial and that "the defendant [did] little more than offer [u]nsupported speculation that further examination of the reliability and the admissibility of the prosecution's expert testimony would have undermined the prosecution's case." Id. at *3 (quotation and citation omitted).