THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

MASSACHUSETTS DIGITAL EVIDENCE GUIDE

Office of the Attorney General, Maura Healey
Cyber Crime Division - Thomas Ralph, Division Chief

June 9, 2015

Massachusetts Digital Evidence Guide

Office of the Attorney General, Maura Healey
Cyber Crime Division - Thomas Ralph, Division Chief

Contents

Contents 2

I. Investigation 6

A. The Search and Seizure of Digital Evidence 6

1. Was there a search or seizure? 6

a) Searches and the Reasonable Expectation of Privacy 7

(1) The Third-Party Doctrine 8

b) Seizures and Interference with Possessory Interest 10

c) Private Party Searches 11

(1) Initial Search Made by Private Party 11

(2) Warrantless Search: Private Citizen or State Actor 11

(3) An ISP's Reporting Obligation Does Not Make it a State Agent 12

2. Was a search or seizure reasonable? 12

a) Warrants 12

(1) Probable Cause / Affidavit 13

(2) Particularity / Scope 15

(3) Staleness of Information Supporting Probable Cause 16

(4) Timely Execution of the Warrant 17

(5) Manner of Executing the Warrant 18

b) Exceptions to the Warrant Requirement 19

(1) Search Incident to Arrest 19
(2) The Plain View Doctrine 20
(3) Exigent Circumstances 21
3. The Exclusionary Rule 22
a) Good Faith / Substantial and Prejudicial 22
b) Inevitable Discovery 22
B. Cases Relating to Specific Digital Devices 23
1. Cell Phone Searches 23
2. Cell Site Location Information 23
3. Search of Computer Files 24
4. Email 25
C. Search of Electronic Service Providers 26
1. General Overview of Stored Communications Act 26
2. Search warrants served on out-of-state Internet service providers 26
D. Encryption and Self Incrimination 26
1. The Fifth Amendment and the Foregone Conclusion Doctrine 26
2. Massachusetts Declaration of Rights Article Twelve 27
3. Encryption 27
4. Model Decryption Protocol 28
E. Searches Implicating Attorney-Client Privilege 29
1. Post-Indictment Email and File Searches 30
2. Taint Teams 30
3. Third Parties and Attorney-Client Privilege (e.g., CC'd emails) 31
II. Evidentiary Matters 32
A. Judicial Discretion 32
1. Trial Judge's Discretion 32
2. Demonstrative Photographs 32
B. Discovery 32
1. Pornographic Images in Child Pornography Cases 32

C. Authentication 32
1. Generally 32
2. Photographs and Digital Images, Videos, and CDs 33
3. Digitally Enhanced Images and Video 33
4. Transcripts of Recordings 33
5. Email 34
6. Chatrooms 35
7. Information Available on Websites and Social Networks 35
8. Software Programs Used in Investigation 36
9. GPS and Probation 36
D. Best Evidence Rule 36
1. Best Evidence Rule - Generally 36
2. Digital Images 37
3. Admission of Duplicate Evidence 37
4. Videos 37
5. Email 38
6. Summaries 38
E. Hearsay 38
1. Software Programs 38
2. Social Networking Sites 38
F. Business Records Exception 39
1. Email 39
2. Computer Records 39
G. Confrontation Clause 39
1. Secondary Examiners 39
H. Encryption 40
III. Crimes 41
A. Possession of Child Pornography 41
1. Multiple Convictions Require Multiple “Caches” 41
2. Brief Possession is Sufficient 41
3. Receipt by Cell Phone is Sufficient 41

4. Malware and Computer Viruses Defense 41
B. Statutory Terms of M.G.L. c. 272 (Knowing Purchase, Possession, or Dissemination) 42
1. "Dissemination" 42
2. Computer "Depictions" 42
3. Child Enticement 42
4. "Visual Material" 42
5. "Nudity" under M.G.L. c. 272 §31 43
6. "Performance" under M.G.L. c. 272 § 29A 43
7. "Knowingly Permit" under M.G.L. c. 272 § 29A 43
8. Lewdness 44
IV. Expert Testimony about Technology 45

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 has interpreted it as providing broader protections than its federal counterpart. See Commonwealth v. Upton, 394 Mass. 363 (1985) ("We conclude that art. 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause."). This guide will generally reference the Fourth Amendment. Where applicable, however, it will note Article Fourteen's higher standards.

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? See, 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 of a GPS tracking device on a car to be a seizure under Massachusetts art. 14 because it required entering 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 (citations omitted).

Individuals generally have a reasonable expectation of privacy in their personal computers and files. See id. (listing cases to that effect). "The salient question is whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated" by some other circumstance. Id. The cases below explore some of these circumstances. There is also a separate section for searches falling under the third-party doctrine.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder 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 defendant's 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. Defendant did not dispute that he had no reasonable expectation of privacy in files shared with the network. Id. at 107. Instead, defendant argued that he did have a reasonable expectation of privacy in his *private* files and that there was not 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 defendant's computer. The facts, even considered together, did not provide a substantial basis to conclude that child pornography would be found on the computer. Id. at 111.

- 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. 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 defendant's argument that the special forensic software used by investigators constituted a search. They 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 hard drive shared across a military network. See id. at 1342. He took several steps—ultimately unsuccessful—that he believed shielded this hard drive from access by others. See 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. See id. at *1. He allowed downloads by a private user who then turned his account over to the Royal Canadian Mounted Police. See id. at *1. The court held that even though he 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 defendants by using automated scanning tools designed to detect child pornography shared on peer-to-peer networks. Id. After lengthy explanations of what these tools do, see 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 Borowy, see discussion supra, along with other circuit cases to that effect, see Thomas, 2013 WL 6000404, at *19. 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 *18. [Note: This case contains clear and thorough explanations of peer-to-peer networks, hash values, and TLO's CPS suite of tools.]

(1) 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).

The third-party doctrine is increasingly controversial, however, as highlighted by Justice Sotomayor's concurrence in United States v. Jones, 132 S. Ct. 945, 954–55 (2012) (Sotomayor, J., concurring) ("[I]t 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 . . . ." (citations omitted)). More importantly, the Supreme Judicial Court recently ruled that—regardless of Fourth Amendment jurisprudence—art. 14 of the Massachusetts Declaration of Rights protects some information held by third parties. See Commonwealth v. Augustine, 467 Mass. 230, 244–55 (2014) (examined below). Though the third-party doctrine still applies to most information held by third parties, the cases below highlight the growing list of exceptions.

- Commonwealth v. Augustine, 467 Mass. 230 (2014). Police investigating a murder obtained the defendant's Cellular Site Location Information (CSLI) from his service provider pursuant to a § 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 Augustine, 467 Mass. 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 that the provision 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, requires a warrant to overcome. Id. at 252–55.

- 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). The defendant challenged such access to his email on Fourth Amendment grounds. 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 this reasonable expectation of privacy, the Sixth Circuit analogized 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.

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, "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 . . . ." Texas v. Brown, 460 U.S. 730, 747–48 (1983) (Stevens, J., concurring). Relying on ample precedent from other courts, the Supreme Judicial Court has found the entire computer analogous to such closed containers 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.

- Commonwealth v. Connolly, 454 Mass. 808 (2009). Investigating a suspected drug dealer, police installed a GPS tracking device in his car. See id. at 809–10. 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. Police obtained a warrant for the tracker, though there was some question as to whether the warrant had expired. The Supreme Judicial Court took the opportunity to hold 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. See id. Second, the government's use of the vehicle to obtain information was itself an interference with the defendant's interest in it. See 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.").

- Berger v. State of New York, 388 U.S. 41 (1967). The Court held that wiretaps "seize" conversations in violation of the Fourth Amendment. See Berger, 388 U.S. 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 . . . . Berger stands for the proposition that the government may seize intangible items . . . .").

- 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. See id. at 217–18. After he was convicted of destroying records in a federal investigation, the defendant attacked his conviction on constitutional grounds. See id. at 218. 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. See 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, which are contraband. Id.

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)). The case below demonstrates how this analysis works in a digital evidence case.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). The defendant in this case 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. After finding more child pornography at the house, defendant was arrested and charged. 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). The 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 April 30, 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 for him 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). 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.

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 Mass. Gen. Laws ch. 276, §§ 1and 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 fresh information, see United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008), and officers must execute them in a timely fashion, see Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 329–30 (2014). Warrants must be executed in a reasonable manner. Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 821 (2013). Finally, executing officers must have the signed warrant with them when commencing the search. The sections below focus on probable cause, particularity, staleness, 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 (2009) (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) (citations omitted).

Probable cause is typically established by law enforcement submitting 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. The following cases address probable cause and affidavits in the digital evidence context.

- 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 63. Shortly after the arrest, the suspect took a receipt out of his pocket and tore it up. Id. 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 fact and inference to support a nexus between the alleged crime and the locations to be searched. Id. 72–73.

- 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. 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 that affidavit 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 emailed images had actually been accessed. 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 finding that the defendant's computer likely contained child pornography. Id.

- Mem. of Decision and Order on Def.'s Mot. for Franks Hr'g and Mots. to Suppress Evidence and Statements at 12, Commonwealth v. Hall, No. MICR-2012-771 (Mass. Super. Ct. July 26, 2013). When a computer connects to the internet through a residential IP address, there is a reasonable probability that the computer or device in question will be located in that residence. The court found the defendant's argument about the possibility of wireless piracy meritless, stating that it was still reasonable to infer that evidence of the transmission of child pornography would be recovered from inside the defendant's home. Id.

(2) 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. 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. The defendant asserted that this was unlawful because the warrant did not specifically authorize the seizure of these items. The warrant did authorize, however, seizure of several types of documents. Id. The Court held that the seizure of the computers was reasonable because they functioned as "closed containers" storing documents. Id. at 766. [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 received 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. 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 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," so protecting "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 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 court 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.

- *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—employed in a recent D.C. District Court case (since overruled)—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. 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. See id. Courts have recognized the practical necessity of copying hard drives for later examination, so the government has been allowed 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.

(3) 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). The reasoning behind this requirement is that the passage of time "reduc[es] the likelihood that the 'evidence of the offense will be found at the place to be searched.'" Id. (quoting United States v. Woodbury, 511 F.3d 93, 97 (1st Cir. 2007)). 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.

- United States v. Morales-Aldahondo, 524 F.3d 115 (1st Cir. 2008). The defendant was convicted of possessing child pornography as a result of an investigation targeting a child pornography website and its subscribers. Id. at 117. 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 defendant's motion to suppress for staleness. Id. Focusing on the characteristics of child pornography collection, 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. The court also cited other cases in which child pornography had been kept for years. Id. (citing United States v. Irving, 452 F.3d 110 (2d Cir. 2006) (two years); United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) (five years)). 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. 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.

(4) Timely Execution of the Warrant

General Laws c. 276, § 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 . . . ." Id.; 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. Ericson, 85 Mass. App. Ct. 326 (2014). The 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, 333. Relying on the reasoning in Commonwealth v. Kaupp, 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) (citing Commonwealth v. Kaupp, 453 Mass. 102, 115 (2009) (explained 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 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. Though invalidating the warrant on probable cause grounds, the Supreme Judicial Court 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 115. 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. The Court found a written return listing the devices to be examined that was filed within seven days after the search warrant issued satisfied G.L. c. 276, § 3A. Id.

(5) 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, 821 (2013). The cases below deal with this requirement in the digital evidence context.

- 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. As part of that search, they seized computers and disks. Id. 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. The Court stressed the need for conducting reasonable digital searches with

minimal intrusion. 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. This case also contains liberal language suggesting 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.

- Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810 (2013). This case dealt with the search of a defendant's email account after indictment, raising the distinct possibility of intercepting privileged communications. Id. at 822–23. 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. More broadly, 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.

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) (citing Commonwealth v. Forde, 367 Mass. 798, 800 (1975)). "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. (citing Commonwealth v. Phillips, 413 Mass 50, 55 (1992)). 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 G.L. c. 276, § 1, which is generally seen as more restrictive than these constitutional provisions. 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" (such as examining papers) is disallowed, id. (citing Commonwealth v. Vuthy Seng, 436 Mass. 537, 551–552 (2002)). The case below involves 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 cellphone—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 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 2486–88. 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. (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.

(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) (laying out the requirements for plain view) (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 at 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. Ericson, 85 Mass. App. Ct. 326 (2014). The 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, 333. 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 "they 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. (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. His statements of intent to exchange pictures of his nude body with the purported child gave police reasonable ground to believe the pictures were evidence of enticing the child 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). The 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 for that image as well as proof that he had sent the emails. Id. at *2. During their search of all 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, 131 S. Ct. 1849, 1856 (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. 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 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, 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 [their classroom] 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.

3. The Exclusionary Rule

Generally, the exclusionary rule prohibits the introduction of evidence obtained as a result of a violation of a defendant's Fourth Amendment or art. 14 rights. See Commonwealth v. Brown, 456 Mass. 708, 715 (2010).

a) Good Faith / Substantial and Prejudicial

The Supreme Court has limited the application of this judicially crafted remedy in federal cases where officers acted in good faith, but Massachusetts does not recognize the good faith exception for 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, 20 Mass. App. Ct. 691, 697 (2014) (citing Commonwealth v. Wilkerson, 436 Mass. 137, 142 (2002)). Where there has been a constitutional violation, "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, 709–710 (2014) (citations 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. During this search, agents found child pornography, and the defendant moved to suppress the evidence at trial, 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 43. 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. See supra Part 2.b)(2), p. 20.]

B. Cases Relating to Specific Digital Devices

1. Cell Phone Searches

- Riley v. California, 134 S. Ct. 2473 (2014). In two consolidated cases, law enforcement officials inspected the contents of an arrestee's cellphone—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 SITA because the justifications undergirding the exception do not apply to cell phones. Id. at 2484–85. First, the digital contents of a cell phone cannot pose an immediate risk of physical injury to an officer. Id. at 2485–86. The Court does allow for physical inspection of the cell phone to mitigate the risk of a hidden weapon. Id. at 2485. Second, once the phone has been seized by law enforcement (which the Court does allow), the arrestee cannot hide or destroy any evidence thereon. Id. at 2486–88. Confronting the issues of encryption and remote wiping, the Court expressed doubt that those issues are particularly common, drew a distinction between such actions and the arrestee-initiated destruction of evidence in a typical SITA exception case, and noted that police could employ other means of preventing such actions. Id. (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.

2. Cell Site Location Information

- Commonwealth v. Augustine, 467 Mass. 230 (2014). Police investigating a murder obtained the defendant's Cellular Site Location Information (CSLI) from his service provider pursuant to a § 2703(d) order. Id. at 233. 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 that 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, requires a warrant to overcome. Id. at 252–55. Then-Justice Gants, writing in dissent, was careful to distinguish between the call CSLI sought in this case (which is only recorded when a telephone call is placed) and registration CSLI (which records the phone's location every few seconds it is powered on). See id. at 258–59 (Gants, J., dissenting). He argued that such call CSLI, which is essential to completing a call, should be covered by the third-party doctrine while registration CSLI should not. Id. at 872–73.

3. Search of Computer Files

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment for evidence linking him to the shooting pursuant to a warrant. Id. at 764–65. As part of that search, they seized five computers and disks. Id. The defendant asserted that this was unlawful because the warrant did not specifically authorize the seizure of these items. The warrant did authorize, however, seizure of several types of documents. Id. The Court held that the seizure of the computers was reasonable because they functioned as "closed containers" storing documents. Id. at 766.

- 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 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, 56 (2004)). In this case, the court found 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 [their classroom] 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.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). The 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, 333. 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 "they 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. (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. His statements of intent to exchange pictures of his nude body with the purported child gave police reasonable ground to believe the pictures were evidence of enticing the child 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)).

- 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 received 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. 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 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," so protecting "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.

4. Email

- 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 ISP. The defendant challenged such access to his email on Fourth Amendment grounds. 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 this reasonable expectation of privacy, the Sixth Circuit analogized 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 Commonwealth v. Augustine, 467 Mass. 230

(2014)—noted that the ISP in this case was an *intermediary* rather than the intended target of a conversation. Id. at 288. This case ruled the Stored Communication Act to be unconstitutional to the extent it allowed warrantless searches of email. Id. Though binding only in the Sixth Circuit, this case has been widely cited by courts and technology companies in requiring warrants to obtain the contents of email.

C. 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 service[s]" (RCS). Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 375 (2014). ECS providers are email services like Gmail or Yahoo! along with certain aspects of social media like a user's Facebook "wall." 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 11–12 (2013).

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. G.L. c. 276, § 1B; see also 18 U.S.C. § 2703 (outlining process by which state courts exercise jurisdiction over ECS and RCS providers).

D. Encryption and Self Incrimination

1. The Fifth Amendment and the Foregone Conclusion Doctrine

The relevant part of the Fifth Amendment states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . . ." U.S. Const. amend. V. 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. But compelled action that communicates something can also be testimonial in nature. Id. at 520–21.

"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." Id. At 520 (quoting United States v. Hubbell, 530 U.S. 27, 43 (2000)). For example, giving blood and fingerprint samples and 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).

Even in cases where the act of producing of evidence 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). "For the exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence." Id. (citing Fisher, 425 U.S. at 410–13).

2. Massachusetts Declaration of Rights Article Twelve

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, 525–26 (2014) (citations omitted). Massachusetts also recognizes the "foregone conclusion" exception to art. 12. Id. at 526.

3. Encryption

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. Encryption presents a problem for law enforcement because readily available encryption software can be virtually impossible to encrypt. See id. at 516–17. Files thus encrypted can only be viewed if an authorized user enters a password, see id. at 517, something they are unlikely to do voluntarily if those files contain incriminating evidence. But compelling the user to enter or disclose their password presents a possible violation of the Fifth Amendment and art. 12. The case below examines the interplay of these issues in Massachusetts.

- Commonwealth v. Gelfgatt, 468 Mass. 512 (2014). The 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 defendant's computers, and they obtained a search warrant naming them, 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. The SJC reversed and held 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 524. 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. [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 below.]

4. Model Decryption Protocol

In Commonwealth v. Gelfgatt, the Commonwealth employed a specific 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 Computer Forensics Laboratory of Massachusetts Attorney General Martha Coakley 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.
>
> At the hearing on the motion to compel decryption, the Commonwealth stated that it "would be seeking to introduce the fact of encryption in order to suggest consciousness of guilt."

Id. at 517 n.10.

E. Searches Implicating Attorney-Client Privilege

Searches that may intercept privileged communications between a suspect and his lawyer deserve special care. See 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 sections 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 and less than 180 days old. See id. at 819 n.17 (citing 18 U.S.C. § 2703(a) (2012)).

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 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 they can "offer adequate protection to the Commonwealth's citizens," id. at 827. To do so, the SJC has put in place a two-tiered set of requirements surrounding 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 228 (citing 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.

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)).

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 it's 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." Renzi, 452 Mass. at 52 (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)).

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. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011).

2. Photographs and Digital Images, Videos, and CDs

When authenticating a photograph or video in the Courts of the Commonwealth, a witness will authenticate the evidence sufficiently with testimony that it fairly and accurately depicts circumstances personally observed by that witness. Commonwealth. v. Pytou Heang, 458 Mass. 827, 855–56 (2011) (citing Commonwealth v. Figueroa, 56 Mass. App. Ct. 641, 646 (2002)). Testimony by a witness that a video fairly and accurately represents what that witness actually saw will authenticate that video sufficiently. Id. Digital photographs and videos are treated as equivalent to their analog counterparts. See Commonwealth v. Leneski, 66 Mass. App. 291, 294–95 (2006).

Alternatively, a witness may authenticate a digital photograph or video by testimony about the process used to create it. See Mass. G. Evid. § 901(b)(9). For example, a witness sufficiently authenticated a CD containing digital images created by a digital camera system at a convenience store where that witness testified they had "viewed the images on the computer and 'burned' the CD copy; he testified as to the procedure he used in the surveillance process, the copying process, and to the contents of the CD." Leneski, 66 Mass. App. Ct. at 295.

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. Renzi v. Paredes, 452 Mass. 38, 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 (1st Cir. 1999). Objections to evidence on the grounds that it lacks a proper foundation are allowed at the discretion of the judge. Id. at 20–21. In Iacobucci, where the audio portion of a video was auditorily 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.

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.

4. Transcriptsof 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. 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.

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. 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. The defendant answered a call to that number, and emailed photograph depicted the defendant. Id. at 674–675.

Other confirming circumstances include: (1) emails originating from an account that bear the defendant's name and that the defendant admits having used; (2) emails 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." Purdy, 459 Mass 442, 450 (2011) (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)."

Safavian, 435 F. Supp. 2d at 41. The court added that the defendant would be entitled, however, to raise any issue of alteration with the jury. Id.

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. 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 website such as Facebook or MySpace 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. 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." Tienda v. State, 358 S.W.3d 633 (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 web pages belonged to defendant 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).

8. 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. Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326–27 (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. 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.

9. GPS and Probation

Official GPS records should be maintained by the Commonwealth and a copy must be attested to and certified by the officer having legal custody of the record in order to minimize concerns about authenticity. Commonwealth v. Thissell, 457 Mass. 191, 199 (2010).

GPS records are sufficiently reliable to show that the defendant violated conditions of probation. Thissell, 457 Mass. at 198–99 (2010). In Thissell, GPS records were factually detailed and made close in time to the events in question by persons responsible for monitoring and communication with defendant. Id. They were attested to by the Chief Probation Officer who testified about the GPS monitoring system, how it worked, and what happened on the day in question, and the records were contemporaneously corroborated by the defendant himself. Id. at 197–99.

D. 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, 725–726 (1970) (emphasis added). Most photographs and videos depict objects rather than writings. Id. at 725. Consequently, the best evidence rule does not typically apply, *inter alia*, to photographs or videotapes. 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." Id. 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 Lenesky 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 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.

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 emphasizes 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."); Commonwealth v. Greenberg, 339 Mass. 557, 581–82 (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. G. Evid. § 1006.

E. Hearsay

1. Software Programs

When software merely provides information to a witness, the software does not make a "statement," and therefore is not subject to the hearsay rule. Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326–327 (2009) (holding that information provided by measuring software that indicated to the witness the distance between real-world objects were not statements subject to the hearsay rule) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)).

2. Social Networking Sites

An image from a defendant's own webpage is generally falls under the admission of a party opponent hearsay exception. See People v. Beckley, 185 Cal. App. 4th 509, 514–15 (Cal. Ct. App. 2010) (reasoning that while an image from a defendant's own webpage should be an admission of a party opponent, the image wasn't admissible when it was offered in this as impeachment evidence against an alibi witness rather than against the webpage owner).

F. 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. G.L. c. 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, 818–819 (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 Wingate v. Emery Air Freight Corp 385 Mass. 402, 406 (1982)) (internal quotation marks omitted); McLaughlin, 445 Mass. at 818–819 (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 printout 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 818–19 ("The affidavits plainly establish that the records satisfy these foundational requirements.").

G. Confrontation Clause

1. 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. United States v. Soto, 720 F.3d 51, 58–60 (1st Cir. 2013) (citing Melendez–Diaz v. Massachusetts, 557 U.S. 305 (2009)).

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.

However, "the 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.

H. Encryption

See supra Part I.D, p. 26.

III. Crimes

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 [M.G.L. c. 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)).

2. Brief Possession is Sufficient

Brief possession of offending images is sufficient to sustain a violation of M.G.L. c. 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, 458–59 (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.

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 M.G.L. c. 272 § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 330 (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) (citing United States v. Pruitt, 638 F.3d 763, 767 (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.

B. Statutory Terms of M.G.L. c. 272 (Knowing Purchase, Possession, or Dissemination)

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) (citing M.G.L. c. 272, § 31 (2010)).

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.

"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, 323–24 (2011). The 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.

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 M.G.L. c. 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 *2 (Mass. Super. Ct. 2001) (quoting M.G.L. c. 272, § 29C (2010)).

5. "Nudity" under M.G.L. c. 272 §31

The definition of "nudity" under §31 was examined 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. 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. "The defendant claims that his activities do not fall within the ambit of §29(a). He first contends that the photographs do not depict a minor in a state of 'nudity' as: 'uncovered or less than opaquely covered human genital, 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.

6. "Performance" under M.G.L. c. 272 § 29A

A "performance" under M.G.L. c. 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, 539–540 (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.

7. "Knowingly Permit" under M.G.L. c. 272 § 29A

In proving the element that "the victim engaged in a live performance involving sexual conduct" 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." Commonwealth v. Bundy, 465 Mass. 538, 542 (2013). In determining the defendant's specific intent, all facts and circumstances may be considered including the defendant's acts and statements. Id. "The statute also permits the Commonwealth to establish that the defendant knowingly permitted [the victim] to engage in a live performance involving sexual conduct. Id.

What "knowingly permit" means 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. 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.

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. Naked photos in the hands of a pedophile do not transform them into lewd photos. Id. at 44 (citing United States v. Villard, 885 F.2d 117, 125 (3d Cir.1989)).

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. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011) (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)).

V. Table of Authorities

Massachusetts Cases

Almeida-Sanchez v. United States,
413 U.S. 266 (1973) 12

Beal Bank, SSB v. Eurich,
444 Mass. 813 (2005) 39

Berger v. State of New York,
388 U.S. 41 (1967) 10

Cavallaro v. United States,
284 F.3d 236 (1st Cir. 2002) 31

Commonwealth v. Amaral,
78 Mass. App. Ct. 671 (2011) 32, 34, 37, 39, 45

Commonwealth v. Anthony,
451 Mass. 59 (2008) 13, 14

Commonwealth v. Augustine,
467 Mass. 230 (2014) 9, 23, 26

Commonwealth v. Balicki,
436 Mass. 1 (2002) 21, 25

Commonwealth v. Balukonis,
357 Mass. 721 (1970) 36, 37

Commonwealth v. Blevines,
438 Mass. 604 (2003) 19

Commonwealth v. Brandwein,
435 Mass. 623 (2002) 11, 12

Commonwealth v. Brown,

456 Mass. 708 (2010) 22

Commonwealth. v. Bundy,
465 Mass. 538 (2013) 43

Commonwealth v. Catanzaro,
441 Mass. 46 (2004) 22, 24

Commonwealth v. Connolly,
454 Mass. 808 (2009) 6, 10

Commonwealth v. Cormier,
28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011) 11

Commonwealth v. Cote,
407 Mass. 827 (1990) 9

Commonwealth v. Donahue,
430 Mass. 710 (2000) 13

Commonwealth v. Durham,
No. 9610398, 1998 WL 34064623 (Mass. Super. Ct. Oct. 13, 1998) 19

Commonwealth v. Ericson,
85 Mass. App. Ct. 326 (2014) 13, 18, 20, 21, 24

Commonwealth v. Figueroa,
56 Mass. App. Ct. 641 (2002) 33

Commonwealth v. Finglas,
81 Mass. App. Ct. 1102 (2011) 14

Commonwealth v. Fontaine,
84 Mass. App. Ct. 699 (2014) 22

Commonwealth v. Forde,
367 Mass. 798 (1975) 19

Commonwealth v. Gelfgatt,
468 Mass. 512 (2014) 26, 27, 28

Commonwealth v. Gousie,
13 Mass. L. Rptr. 585 (Mass. Super. Ct. 2001) 15, 17, 25, 42, 43

Commonwealth v. Greenberg,
339 Mass. 557 (1959) 38

Commonwealth v. Hall,
80 Mass. App. Ct. 317 (2011) 41, 42

Commonwealth v. Hall,

No. MICR-2012-771 (Mass. Super. Ct. July 26, 2013) 14

Commonwealth v. Harvard,
365 Mass. 452 (1969) 41

Commonwealth v. Harvey,
397 Mass. 351 (1986) 37

Commonwealth v. Hinds,
437 Mass. 54 (2002) 42

Commonwealth v. Kaupp,
453 Mass. 102 (2009) 7, 13, 18, 22, 24

Commonwealth v. Leneski,
66 Mass. App. Ct. 291 (2006) 32, 33, 36, 37

Commonwealth v. Leonard,
428 Mass. 782 (1999) 34

Commonwealth v. Leone,
386 Mass. 329 (1982) 11, 12

Commonwealth v. Magri,
462 Mass. 360 (2012) 6

Commonwealth v. Mahoney,
400 Mass. 524 (1987) 37

Commonwealth v. Maingrette,
20 Mass. App. Ct. 691 (2014) 22

Commonwealth v. McDermott,
448 Mass. 750 (2007) ..... *passim*

Commonwealth v. Mimless,
53 Mass. App. Ct. 534 (2002) 38

Commonwealth v. Nelson,
460 Mass. 564 (2011) 12

Commonwealth v. Noxon,
319 Mass. 495 (1946) 32

Commonwealth v. Ocasio,
434 Mass. 1 (2001) 36, 37

Commonwealth v. Phillips,
413 Mass 50 (1992) 19

Commonwealth v. Porter P.,

456 Mass. 254 (2010) 22

Commonwealth v. Provost,
418 Mass. 416 (1994) 43

Commonwealth v. Purdy,

459 Mass. 442 (2011) 32, 34, 35

Commonwealth. v. Pytou Heang,
458 Mass. 827 (2011) 33

Commonwealth v. Rabb,
431 Mass. 123 (2000) 41

Commonwealth v. Raboin,
24 Mass. L. Rptr. 278 (Mass. Super. Ct. 2008) 11

Commonwealth v. Rex,
469 Mass. 36 (2014) 44

Commonwealth v. Rollins,
470 Mass. 66 (2014) 41

Commonwealth. v. Ruddock,
No. 08–1439, 2009 WL 3400927 (Mass. Super. Ct. Oct. 16, 2009) 32

Commonwealth v. Sands,
424 Mass. 184 (1997) 45

Commonwealth v. Sheldon,
423 Mass. 373 (1996) 36, 38

Commonwealth v. Sliech-Brodeur,
457 Mass. 300 (2010) 20

Commonwealth v. Sullo,
26 Mass. App. Ct. 766 (1989) 20

Commonwealth v. Thissell,
457 Mass. 191 (2010) 36

Commonwealth v. Upton,
394 Mass. 363 (1985) 6

Commonwealth v. Valerio,
449 Mass. 562 (2007) 13, 15

Commonwealth v. Vuthy Seng,
436 Mass. 537 (2002) 20

Commonwealth v. Weichell,
390 Mass. 62 (1983) 36

Commonwealth v. Whitlock,
74 Mass. App. Ct. 320 (2009) 36, 38

Commonwealth v. Wilkerson,
436 Mass. 137 (2002) 22

Commonwealth v. Williams,
456 Mass. 857 (2010) 34, 35

Commonwealth v. Wilson,
389 Mass. 115 (1983) 20

Coolidge v. New Hampshire,
403 U.S. 443
(1971)..... 12

Dahl v. Bain Capital Partners, LLC,
714 F. Supp. 2d 225 (D. Mass. 2010) 31

Fauci v. Mulready,
337 Mass. 532 (1958) 37

Fisher v. United States,
425 U.S. 391 (1976) 26, 27

Griffin v. State,
419 Md. 343 (2011) 34

Horton v. California,
496 U.S. 128 (1990) 20

Iacobucci v. Boulter,
193 F.3d 14 (1st Cir. 1999) 33

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) 16

In re F.P.,
878 A.2d 91 (Pa. Super. Ct. 2005) 35

Katz v. United States,
389 U.S. 347 (1967) 7, 15

Kentucky v. King,
131 S. Ct. 1849 (2011) 21

LeClair v. Hart,
800 F.2d 692 (7th Cir. 1986) 10

Lorraine v. Markel Am. Ins. Co.,
241 F.R.D. 534 (D. Md. 2007) 33, 35

McLaughlin v. CGU Ins. Co.,
445 Mass. 815 (2006) 39

Melendez–Diaz v. Massachusetts,
557 U.S. 305 (2009) 39

Mincey v. Arizona,
437 U.S. 385 (1978) 21

Parker v. State,
85 A.3d 682 (Del. 2014) 35

People v. Beckley,
185 Cal. App. 4th 509 (Cal. Ct. App. 2010) 38

Preventive Medicine Assocs., Inc. v. Commonwealth,
465 Mass. 810 (2013) ..... *passim*

Renzi v. Paredes,
452 Mass. 38 (2008) 32, 33

Riley v. California,
134 S. Ct. 2473 (2014) 6, 20, 23

Simmons v. Commonwealth,
no. 2012–SC–000064–MR, 2013 WL 674721 (Ky. Feb. 21, 2013) 35

Smith v. Maryland,
442 U.S. 735 (1979) 8

Texas v. Brown,
460 U.S. 730 (1983) 10

Tienda v. State,
358 S.W.3d 633 (Tex. Crim. App. 2012) 35

United States v. Ademaj,
170 F.3d 58 (1st Cir. 1999) 33

United States v. Anderson,
452 F.3d 66 (1st Cir. 2006) 33

United States v. Borowy,
595 F.3d 1045 (9th Cir. 2010) 7

United States v. Burdulis,
No. 10–40003–FDS, 2011 WL 1898941 (D. Mass. May 19, 2011) 21

United States v. Crespo-Rios,
645 F.3d 37 (1st Cir. 2011) 23

United States v. Heckencamp,
482 F.3d 1142 (9th Cir. 2007) 7

United States v. Hicks,
438 F. App'x 216 (4th Cir. 2011) 10

United States v. Hubbell,
530 U.S. 27 (2000) 27

United States v. Irving,
452 F.3d 110 (2d Cir. 2006) 17

United States v. Jackson,
208 F.3d 633 (7th Cir. 2000) 35

United States v. Jacobsen,
466 U.S. 109 (1984) 11

United States v. Jones,
132 S. Ct. 945 (2012) 9

United States v. Karo,
468 U.S. 705 (1984) 6

United States v. King,
509 F.3d 1338 (11th Cir. 2007) 7

United States v. Ladeau,
No. 09–40021–FDS, 2010 WL 1427523 (D. Mass. April 7, 2010) 8

United States v. Lichtenberger,
19 F. Supp. 3d 753 (N.D. Ohio 2014) 12

United States v. Miller,
425 U.S. 435 (1976) 8

United States v. Morales-Aldahondo,
524 F.3d 115 (1st Cir. 2008) 13, 16, 17

United States v. Pierre,
484 F.3d 75 (1st Cir. 2007) 17

United States v. Pruitt,
638 F.3d 763 (11th Cir. 2011) 41

United States v. Riccardi,
405 F.3d 852 (10th Cir. 2005) 17

United States v. Rogers,
714 F.3d 82 (1st Cir. 2013) 41

United States v. Safavian,
435 F. Supp. 2d 36 (D.D.C. 2006) 34, 35

United States v. Schesso,
730 F.3d 1040 (9th Cir. 2013) 16

United States v. Soto,
720 F.3d 51 (1st Cir. 2013) 39

United States v. Stevenson,

727 F.3d 826 (8th Cir. 2013) 12

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) 8

United States v. Villard,
885 F.2d 117 (3d Cir.1989) 44

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 9, 25

United States v. Woodbury,
511 F.3d 93 (1st Cir. 2007) 16

Warshak v. United States,
490 F.3d 455 (6th Cir. 2007) 9, 25

Welch v. Keene Corp.,
31 Mass. App. Ct. 157 (1991) 38

Wingate v. Emery Air Freight Corp.,
385 Mass. 402 (1982) 39

Constitutional Provisions

Mass. Declaration of Rights art. 12 ..... 27, 28

Mass. Declaration of Rights art. 14 ..... *passim*

U.S. Const. amend. IV 6, 13

U.S. Const. amend. V 27

Statutes

18 U.S.C. § 2258A 12

18 U.S.C. § 2258B 12

18 U.S.C. § 2703 ..... 9, 23, 26, 30

Mass. G.L. c. 233, § 78 39

Mass. G.L. c. 272, § 29 ..... 41, 42, 43

Mass. G.L. c. 272, § 31 ..... 42, 43

Mass. G.L. c. 276, § 1 ..... 12, 19, 26

Mass. G.L. c. 276, § 2 ..... 12, 15

Mass. G.L. c. 276, § 3 ..... 17, 18

Rules

Fed. R. Crim. P. 41 17

Mass. G. Evid. § 1002 36

Mass. G. Evid. § 1006 38

Mass. G. Evid. § 104 34

Mass. G. Evid. § 901 33

Mass. R. Crim. P. 14 32

Other Authorities

Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373 (2014) 26

Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 8-11 (2013) 26

Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 11-12 (2013) 26

Jeffrey Paul DeSousa, Self-storage Units and Cloud Computing, 102 Geo. L.J. 247 (2013) 26