PREVENTIVE MEDICINE ASSOCIATES, INC., & another [FN1] *vs.* COMMONWEALTH.

SJC-11252.

Suffolk. March 7, 2013. - July 15, 2013.

Electronic Mail. Privileged Communication. Search and Seizure, Warrant. *Practice, Criminal,* Warrant, Assistance of counsel, Subpoena. *Constitutional Law,* Search and seizure, Assistance of counsel. *Rules of Criminal Procedure.*

CIVIL ACTION commenced in the Supreme Judicial Court for the county of Suffolk on June 13, 2012.

The case was reported by *Spina,* J.

Timothy E. Maguire for the plaintiffs.

Thomas E. Bocian, Assistant Attorney General, for the Commonwealth.

Present: Ireland, C.J., Spina, Cordy, Botsford, Gants, Duffly, & Lenk, JJ.

BOTSFORD, J.

This case concerns the search by the Commonwealth of electronic mail messages (e-mails) of a criminal defendant after he has been indicted. Because the e-mails sought by the Commonwealth are intermingled with many other e-mails that are likely to be protected by the attorney-client privilege, the case concerns more particularly the intersection between search and seizure law and that privilege.

The issue arises in the following context. On behalf of the Commonwealth, the Attorney General sought, and a grand jury returned, indictments charging the defendants, Preventive Medicine Associates, Inc. (PMA), and Punyamurtula Kishore, with Medicaid fraud in violation of G.L. c. 118E, §§ 40 and 41.

[FN2] Thereafter, on two different occasions, the Commonwealth applied for and obtained search warrants to obtain and search designated e-mail accounts of Kishore and of PMA's former billing director, Cheryl Church; both e-mail accounts were with Google, Inc. (Google), which stored the e-mails on its own server. On learning that the Commonwealth had begun reviewing Kishore's e-mails pursuant to the warrants, the defendants moved for a protective order, claiming that the attorney-client privilege protected many of those e-mails.

After several hearings, on June 4, 2012, a judge in the Superior Court (motion judge) entered an amended order permitting the Commonwealth to search the e-mails by using a so-called "taint team" comprised of assistant attorneys general not involved in the investigation or prosecution of the defendants. The defendants filed a petition under G.L. c. 211, § 3, in the county court, seeking relief from the motion judge's order. The single justice stayed the motion judge's order and reserved and reported the following questions to the full court:

"(1) Whether the Commonwealth may, by means of an ex parte search warrant, search the post-indictment emails of a criminal defendant.

"(2) If question (1) is answered in the affirmative, whether the 'taint team' procedure authorized in the Amended Order dated June 4, 2012, is permissible under the Massachusetts Constitution."

With some important limitations, we answer yes to both questions.

Background. The Commonwealth's "statement of the case" [FN3] alleges, in relevant part, that Kishore owned and operated PMA, a network of group medical practices in Massachusetts. The Commonwealth asserts that PMA performed numerous drug tests for patients over a period from July, 2006, to April, 2011, for which PMA was paid approximately $18.9 million from MassHealth, the Massachusetts Medicaid program. PMA obtained some of these payments from MassHealth as a result of an illegal kickback scheme, by which PMA paid certain "sober homes" [FN4] in order to induce the sober homes to refer their residents to PMA for drug testing. A grand jury investigation commenced in 2009, and on September 29, 2011, the grand jury returned indictments charging Kishore and PMA each with eight counts of violating the Medicaid false claims statute (based on the alleged kickback scheme), G.L. c. 118E, § 40; and eight counts of violating the Medicaid antikickback statute, G.L. c. 118E, § 41. [FN5] (See note 2,*supra.*)

In connection with its continuing investigation of the defendants, the Commonwealth sought to search the Google e-mail accounts of Kishore and of Church. Because Google held the e-mails on its own servers, [FN6] on September 7, 2011, the Commonwealth requested in writing that Google preserve Kishore's and Church's e-mail accounts. Thereafter, on December 21, almost three months after the defendants were indicted, the Commonwealth applied to a judge in the Superior Court for a search warrant to search the e-mail accounts of Kishore and Church for documents relating to:

"1. [PMA's] violation of the Medicaid False Claims Act, PMA's billing MassHealth for services that were not medically necessary, and PMA's billing MassHealth for services that were not authorized by a MassHealth provider actively involved in the treatment of the MassHealth member; or

"2. bills submitted to MassHealth by PMA; or

"3. financial arrangements between Dr. Kishore and/or PMA and/or NLA [[FN7]] and/or Massachusetts sober houses that referred residents to PMA for urine drug screen testing."

The affidavit in support of the search warrant application did not mention that a grand jury previously had returned indictments charging the defendants with having operated an illegal kickback scheme with certain sober homes. As conceded by the Commonwealth, the search warrant affidavit also failed to establish probable cause to believe that any of the e-mails would contain evidence of a kickback scheme between the defendants and sober homes, the third category of information for which the Commonwealth sought to search. Rather, the affidavit provided information relating only to allegedly fraudulent billing practices of the defendants--separate crimes that were the subject of an ongoing investigation by the grand jury. Nonetheless, the search warrant as issued permitted the Commonwealth to search for all three categories of information that it had sought in its search warrant affidavit, and the Commonwealth served the warrant on Google. [FN8] In response, Google sent the Commonwealth two digital video discs (DVDs) containing copies of all e-mails dated from March 21, 2008, to December 22, 2011, in Kishore's and Church's e-mail accounts. The

DVDs contained 68,516 e-mails from Kishore's e-mail account and 11,737 e-mails from Church's e-mail account, for a total of 80,253 e-mails.

The deputy chief of investigations for the Attorney General's Medicaid fraud division, who was also a certified forensic computer examiner, began searching the e-mails in Kishore's account in early January, 2012. [FN9] He started by identifying and segregating e-mails potentially covered by the attorney-client privilege. To do so, he used a computer program to search for the names of attorneys and law firms believed by the prosecuting assistant attorneys general to have been associated with the defendants. As a result of those searches, 7,700 e-mails were segregated from the rest, and no one in the Attorney General's office reviewed the contents of those e-mails. Additionally, the deputy chief of investigations used computer programs to identify duplicate e-mails and e-mails generated from commercial Web sites. He removed those e-mails as well, and turned over the remaining 51,309 e-mails to an investigator in the Medicaid fraud division.

That investigator started reviewing those e-mails on January 18, 2012. Sometime between that date and February 28, he discovered that some of the e-mails had been sent or received after September, 2011, when, according to the Commonwealth's information, PMA had ceased its operations. The investigator ceased his review because he was concerned that he could not search e-mails pursuant to the December, 2011, warrant that were sent or received after PMA had ceased its operations. On February 28, 2012, the Commonwealth applied to a Superior Court judge [FN10] for a second search warrant, specifically seeking to search Kishore's and Church's e-mail accounts for e-mails dated from September 29, 2011 (the date of the indictments), to December 22, 2011. The affidavit in support of the second search warrant application incorporated by reference the first search warrant and, in addition, stated in one of its final paragraphs (paragraph forty-two of forty-six) that a grand jury had returned indictments charging the defendants with having operated a kickback scheme with certain sober homes.

On February 29, 2012, as part of pretrial discovery, the Commonwealth provided defense counsel with one of the e-mails it had received from Google pursuant to the first search warrant that related to the alleged kickback scheme. As a result, defense counsel learned for the first time that the Commonwealth had seized and was in the process of searching the e-mails in Kishore's Google e-mail account. Concerned that the seized e-mail account contained communications protected by the attorney-client privilege, counsel filed an emergency motion for a protective order the next day.

The motion judge held a hearing on March 2, 2012, on the emergency motion, at the end of which the motion judge ordered the Commonwealth to cease its review of the e-mails in its possession until further court order and to provide a copy of all those e-mails to the defendants. At a subsequent hearing approximately two weeks later, the motion judge ordered the Commonwealth to produce to the defendants a separate copy of all e-mails that had been segregated as potentially privileged and not reviewed. The defendants compared the group of all e-mails to the group of e-mails identified as potentially privileged, and concluded that the Attorney General's segregation process had failed to identify all privileged e-mails. On April 23, 2012, the defendants filed a motion to dismiss the indictments, alleging violation of the defendants' constitutional right to counsel guaranteed by the Sixth Amendment to the United States Constitution and art. 12 of the Massachusetts Declaration of Rights. That motion remains pending.

Meanwhile, the defendants learned also that the Commonwealth had obtained e-mails from Church's e-mail account, and thereafter filed a second motion for a protective order concerning the Church e-mails; the motion judge ordered the Commonwealth to cease its

review of those e-mails as well.

At another hearing on the same matter held May 9, 2012, the Commonwealth suggested to the motion judge the appointment of a special magistrate to review all e-mails in the Commonwealth's possession and remove those e-mails covered by the attorney-client privilege. In a subsequent filing, however, the Commonwealth informed the judge that it had changed its position, and believed that the appointment of a special magistrate to review the entire set of e- mails would prove too costly. On May 23, the motion judge entered an order requiring a "taint team" to review the Church e-mails. The judge entered an amended order on June 4 (amended order), extending the taint team procedure to review of the Kishore e-mails as well as the Church e-mails. [FN11]

Pursuant to G.L. c. 211, § 3, the defendants sought relief from this order from a single justice in the county court. As indicated, the single justice stayed the amended order and reserved and reported the two questions set forth above.

Discussion. 1. *Postindictment search of a criminal defendant's e-mails by means of an ex parte search warrant.* The first reported question asks whether the Commonwealth may obtain ex parte a search warrant to search a criminal defendant's e-mails after he has been indicted. [FN12] The fundamental problem posed by such a search is the substantial likelihood that privileged attorney-client communications will be present in the e-mail account of a defendant under indictment. We address that problem by answering the reported question in two steps. First, we consider whether the Commonwealth may *seize* e-mails of a defendant under indictment by means of an ex parte search warrant. Second, we examine whether, if the Commonwealth may seize such e-mails, there are special conditions or procedures that the Commonwealth must follow in conducting any search of them. [FN13]

As a preliminary matter, the Commonwealth contends that it obtained both search warrants with the sole purpose of finding evidence of uncharged crimes, not the charged kickback scheme. [FN14] The Commonwealth suggests that this fact should be material to our analysis of the issues before us. We disagree. Whether the Commonwealth searches the e-mail account of an indicted defendant for evidence of an indicted offense, or for evidence of uncharged--and even unrelated--criminal conduct, it runs the risk of encountering the defendant's privileged communications. The following discussion applies to all e-mails the Commonwealth seeks to search in this case, regardless of whether the Commonwealth sought them as part of its investigation of the crimes that are the subject of the pending indictments or different crimes.

a. *Postindictment seizure of e-mails by means of an ex parte search warrant.*

[FN15] Under G.L. c. 276, § 1, a court or judge may issue a search warrant to search for "property"--defined to include, inter alia, "records" that there is probable cause to believe are associated with the commission of a crime. Under G.L. c. 276, § 1B, a court or judge is authorized to issue a warrant to search "records," including the content of a user's electronic communications, such as e-mails, "stored by an electronic communication or remote computing service." [FN16] Section 1B applies in a case such as this one, because

the e-mails at issue were stored by Google, a third-party provider of electronic communication and remote computing services. Neither G.L. c. 276, § 1, nor § 1B, however, contains any language restricting in any way the issuance of a search warrant that seeks to search for records or other property belonging to or associated with a criminal defendant under indictment.

The Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2006 & Supp. IV 2010) (SCA), to which G.L. c. 276, § 1B (*a*), refers (see note 16, *supra*), provides the procedures that a "governmental entity"--defined to mean any department or agency of the United States or any State or political subdivision, see 18 U.S.C. § 2711(4)--must follow in order to obtain a user's e-mails or other electronic communications from third-party providers of electronic communication services and remote computing services. See 18 U.S.C. § 2703. See also *United States v. Weaver,* 636 F.Supp.2d 769, 770 (C.D.Ill.2009). See generally Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L.Rev. 1208 (2004). The SCA authorizes and in some instances requires the governmental entity to obtain a search warrant in order to gain access to e-mails [FN17] but, like G.L. c. 276, §§ 1 and 1B, does not distinguish between the periods before and after the return of an indictment.

Notwithstanding these statutory provisions, the defendants contend that Mass. R.Crim. P. 17, 378 Mass. 885 (1979) (rule 17), precludes the postindictment issuance of a warrant to obtain a defendant's e-mails (and thereby precludes the Commonwealth from obtaining those e-mails for which the SCA requires a warrant). [FN18] Rule 17 governs the issuance of subpoenas [FN19] in criminal cases. Under rule 17(a)(2), a subpoena may issue for a witness to produce "books, papers, documents, or other objects" (collectively, records) at any type of criminal proceeding in which evidence may be adduced, including grand jury proceedings, evidentiary hearings, and trial. See *Commonwealth v. Odgren,* 455 Mass. 171, 180-181 (2009), and sources cited. In addition, rule 17(a)(2) authorizes the court to direct the production of subpoenaed records "within a reasonable time prior to the trial or prior to the time when they are to be offered in evidence." See *id.* at 181. In *Commonwealth v. Odgren, supra* at 186, and *Commonwealth v. Lampron,* 441 Mass. 265, 270 (2004), we concluded that a party to a pending criminal case seeking pretrial production of third-party records under rule 17(a)(2)--whether the party be the Commonwealth or the defendant--must file a motion seeking prior judicial approval.

The defendants read the rule 17(a)(2) procedure of obtaining prior access to subpoenaed records as coming into play only after the return of an indictment, at which point it becomes the exclusive means of seeking third-party records. The defendants are incorrect. Rule 17 may apply even before the return of an indictment; as noted, the rule authorizes the issuance of a subpoena to a third party to produce records before the grand jury. See *Commonwealth v. Odgren,* 455 Mass. at 180-181, and sources cited. See also *United States v. R. Enters., Inc.,* 498 U.S. 292, 299 (1991) ("the focus of our inquiry is the limit imposed on a grand jury by Federal Rule of Criminal Procedure 17[c], which governs the issuance of subpoenas duces tecum in federal criminal proceedings"); 2 C.A. Wright & P.J. Henning, Federal Practice & Procedure § 272, at 242-243 (4th ed.2009). [FN20] It seems clear, and the defendants do not suggest otherwise, that rule 17 does not preclude the use of search warrants while a grand jury investigation is pending. See, e.g., *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162, 1175 (9th Cir.2010) (considering preindictment grand jury investigation by government: "It isn't per se unreasonable to conduct an investigation using both search warrants and subpoenas [issued pursuant to Fed.R.Crim.P. 17]"); 3 W.R. LaFave, J.H. Israel, N.J. King, & O.S. Kerr, Criminal Procedure § 8.8(g) (3d ed. 2007 & Supp.2012-2013) ("prosecutors may appropriately use both search warrants and subpoenas to obtain related material in the same investigation"). Rather, the Commonwealth's ability to secure grand jury subpoenas and its authority to seek and obtain search warrants derive from separate sources of authority,

> [FN21] and nothing in rule 17 suggests that the ground rules change with respect to search warrants once an indictment has issued. [FN22] Decisions by Federal Courts in

cases governed by the Federal Rules of Criminal Procedure, including Fed.R.Crim.P. 17, support this view. See, e.g., *KRL v. Moore,* 384 F.3d 1105, 1112 (9th Cir.2004) (discussing "evidence recovered pursuant to a post-indictment search warrant"); *United States v. Cooney,* 26 Fed.Appx. 513, 524 (6th Cir.), cert. denied, 535 U.S. 1118 (2002) (suggesting that police could have obtained warrant to search home of defendant under indictment).

We thus conclude that the postindictment issuance of an ex parte search warrant to obtain e-mails does not run afoul of rule 17, and that an ex parte search warrant is an acceptable means by which the Commonwealth may seek to seize e-mails of a defendant under indictment. That does not end our discussion, however. As we explain *infra,*judicial supervision is essential where the Commonwealth seeks to search the e-mails of an indicted defendant, because of the risk that privileged attorney-client communications will be included in those e-mails. In order to ensure proper judicial supervision over this process, and as an exercise of our supervisory powers, we shall require in all future cases that only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment. [FN23] In addition, the affidavit submitted in support of the warrant application must inform the judge at the outset that the individual whose e-mails are being sought is presently under indictment, and must explain the nature and scope of the pending indictment (or indictments), as well as the relationship, if any, between the pending indictment and the search warrant being sought. Finally, the affidavit must explain the need for using a search warrant instead of the rule 17(a)(2) procedure to obtain prior access to subpoenaed records (e.g., because the SCA requires a search warrant). The Commonwealth's failure to justify the need for a search warrant rather than a rule 17 subpoena would be an appropriate basis for a judge to deny the Commonwealth's application for a search warrant. See note 22, *supra.*

b. *Search of e-mails seized pursuant to a postindictment search 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. See *United States v. Ramirez,* 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis ... governs the method of execution of the warrant"); *Bellville v. Town of Northboro,* 375 F.3d 25, 32 (1st Cir.2004) ("the Fourth Amendment's prohibition of unreasonable searches and seizures extends not only to the initiation of searches but also to the manner in which searches are conducted"); *Commonwealth v. McDermott,* 448 Mass. 750, 777, cert. denied, 552 U.S. 910 (2007) (*McDermott*) (search of computers and disks storing records "must be reasonable"). When 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, we conclude that a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege. See, e.g., *Klitzman, Klitzman & Gallagher v. Krut,* 744 F.2d 955, 961 (3d Cir.1984) (search of law office unreasonable where investigators "took not one step to minimize the extent of the search or to prevent the invasion of the clients' privacy guaranteed by the attorney-client privilege"). See also McArthur, The Search and Seizure of Privileged Attorney-Client Communications, 72 U. Chi. L.Rev. 729, 730 (2005) (arguing that "the Fourth Amendment is violated whenever law enforcement officials have reason to believe that a search or seizure is likely to expose them to privileged attorney-client communications and fail to take reasonable steps to minimize their exposure").

Given the constitutional command of reasonableness and in light of the risk involved to the integrity of a defendant's attorney-client privilege, we conclude that in the future, when the

Commonwealth seizes pursuant to a search warrant the e-mails of a defendant under indictment, before any search of those e-mails may take place, the Commonwealth must present to a Superior Court judge and obtain the judge's approval of the search protocol to be used and specifically the procedures proposed to protect against searches of privileged communications between the defendant and his attorneys. [FN24] Court supervision is necessary because the harm to the defendant could be irreparable if the Commonwealth viewed privileged materials, even if only by accident.

> [FN25] Further, unless the Commonwealth can demonstrate a compelling contrary reason, the defendant must have an opportunity to be heard before the judge approves a particular search method. [FN26]

2. *Taint team search procedure.* The second question reserved and reported by the single justice asks whether the taint team search procedure set forth in the amended order is a permissible method to conduct such a search under the Massachusetts Constitution.

We begin by summarizing the amended order's provisions that set out the taint team procedures. The amended order requires the Commonwealth to "designate a team of attorneys and/or agents employed by the Office of the Attorney [General] who have not at any time been involved in the investigation(s) and/or prosecution of the defendants ... and who shall not be assigned to any such investigation or prosecution in the future (the TEAM)." After the formation of the taint team, the defendants are to "provide a list of search terms which may facilitate the review of emails to be conducted by the TEAM so designated." Then, over the next twenty days, the taint team is to (1) review all e-mails from the Church and Kishore e-mail accounts that previously have not been designated privileged; and (2) separate into two groups "those emails which the TEAM and/or members thereof deem possibly privileged and those deemed not to be privileged on their face." After the taint team's review, the defendants are to have fourteen days to review all the e-mails that the taint team has reviewed, both "possibly privileged" and not privileged, and to prepare and file written objections to any of the taint team's privilege determinations. If such objections cannot be resolved by agreement, the Superior Court judge is to resolve them on motion of the defendants. The taint team is not to disclose or provide access to any e-mails under review until the defendants have completed their review. At that point, the taint team is to release to the prosecuting attorneys all e-mails that the team has determined to be nonprivileged and as to which the defendants have not filed an objection. The amended order prohibits members of the taint team from disclosing the search terms submitted by the defendants. Finally, all members of the taint team are required to "sign an acknowledgment and agreement to be subject to the terms of [the amended order], particularly with respect to the limitations on disclosure."

The defendants argue that the amended order's taint team procedures violate their constitutional right to counsel. They contend also that the amended order authorizes an unconstitutional general search. We consider these arguments in turn.

a. *The taint team, the attorney-client privilege, and the right to counsel.* "Federal courts have taken a skeptical view of the Government's use of 'taint teams' as an appropriate method for determining whether seized or subpoenaed records are protected by the attorney-client privilege." *United States v. SDI Future Health, Inc.,* 464 F.Supp.2d 1027, 1037 (D.Nev.2006). See *United States v. Taylor,* 764 F.Supp.2d 230, 234 (D.Me.2011) ("there is a healthy skepticism about the reliability of a filter agent or Chinese or ethical wall within a prosecutor's office"); *In re Search Warrant for Law Offices,* 153 F.R.D. 55, 59 (S.D.N.Y.1994) ("reliance on the implementation of a Chinese Wall, especially in the context of a criminal prosecution, is highly questionable, and should be discouraged"). [FN27] But

see *United States v. Triumph Capital Group, Inc.,*211 F.R.D. 31, 43 (D.Conn.2002) ("use of a taint team is a proper, fair and acceptable method of protecting privileged communications").

Despite the generally widespread skepticism about government agents reviewing a defendant's privileged attorney-client communications, Federal court decisions reflect different views on whether to authorize the use of a taint team. Some have rejected its use. See *In re Grand Jury Subpoenas,* 454 F.3d 511, 524 (6th Cir.2006) (trial court must employ special master to review documents for privileged communications); *United States v. Regan,* 281 F.Supp.2d 795, 806 (E.D.Va.2002) (same); *Black v. United States,* 172 F.R.D. 511, 516 (S.D.Fla.1997) (ordering judge or judge's designee to review documents for privileged communications). Others have approved its use. See *United States v. Triumph Capital Group, Inc., supra;* In re Ingram, U.S. Dist. Ct., No. 12-431 (E.D.La. Apr. 12, 2012). And still others have approved the use of a taint team review procedure while expressing a preference for review by an independent special magistrate. See *United States v. Hunter,* 13 F.Supp.2d 574, 583 & n. 2 (D.Vt.1998); *United States v. Skeddle,* 989 F.Supp. 890, 898 n. 6 (N.D.Ohio 1997).

It is possible, as the defendants argue, that government intrusion into the attorney-client privilege may rise to the level of a violation of a defendant's Sixth Amendment rights, for the attorney-client privilege "is key to the constitutional guarantees of the right to effective assistance of counsel and a fair trial." *United States v. Neill,* 952 F.Supp. 834, 839 (D.D.C.1997). See *Commonwealth v. Fontaine,* 402 Mass. 491, 496 (1988) ("monitoring of privileged communications between a defendant and his attorney touches the core of the right to counsel"). Nonetheless, courts generally have held that a violation of the attorney-client privilege implicates the right to counsel "only under certain circumstances--specifically, when the government interferes with the relationship between a criminal defendant and his attorney," and that interference "substantially prejudice[s] the criminal defendant." *Partington v. Gedan,* 961 F.2d 852, 863 (9th Cir.), cert. denied sub nom. *Partington v. Lum,* 506 U.S. 999 (1992). On this basis Federal courts have concluded that the government's use of a taint team does not violate a defendant's Sixth Amendment right to counsel so long as the taint team procedure prevents the disclosure of privileged communications to the prosecution team. See *United States v. Neill, supra* at 840-841, citing *Weatherford v. Bursey,* 429 U.S. 545, 558 (1977). See also *United States v. Dupree,* 781 F.Supp.2d 115, 163 (E.D.N.Y.2011) ("the mere fact that the government obtained privileged information does not mean it violated defendants' [right to counsel]"). The defendants have not cited, and we have not found, any case in which a court has concluded that the use by the prosecution of a taint team to review a criminal defendant's potentially privileged communications in itself violated the defendant's Sixth Amendment right to counsel.

While in some respects this court has interpreted the right to counsel set forth in art. 12 of the Massachusetts Declaration of Rights more generously than the Sixth Amendment, we see no cause to do so in the context presented here. Cf. *Commonwealth v. Murphy,* 448 Mass. 452, 466 (2007), citing *Commonwealth v. Rainwater,* 425 Mass. 540, 553-554 (1997), cert. denied, 522 U.S. 1095 (1998), abrogated on other grounds by *Texas v. Cobb,* 532 U.S. 162 (2001), and cases cited (noting limited "instances where this court has interpreted the art. 12 right to counsel more expansively than the Sixth Amendment"). "In deciding whether art. 12 offers more protection of the right to counsel than the Sixth Amendment, 'our guiding consideration is whether the Federal rule adequately protects the rights of the citizens of Massachusetts.' "*Commonwealth v. Murphy, supra* at 465, quoting *Commonwealth v. Mavredakis,* 430 Mass. 848, 858 (2000). Here, insofar as the Sixth Amendment right to counsel appears to permit the use of a taint team only where the

government can establish that the taint team will prevent the disclosure of privileged information to the prosecution team, see *United States v. Neill,* 952 F.Supp. at 841, we conclude that the Federal rule does offer adequate protection to the Commonwealth's citizens. The defendants advance no justification for a stricter constitutional rule that would prohibit the use of taint teams categorically. Cf. *Commonwealth v. Fontaine,* 402 Mass. at 496-497 (Commonwealth's monitoring of privileged communications between defendant and his attorney warranted dismissal where it resulted in irremediable prejudice to the defense).

With the foregoing principles in mind, we turn to the taint team procedures set out in the amended order. We read the amended order to contain four distinct 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.

We consider each of these four requirements to be an essential component--a sine qua non--of a valid taint team procedure. [FN28] The defendants' involvement in the review procedure in particular is a crucial check against the potential for mistakes or abuse by the taint team. Compare *In re Grand Jury Subpoenas,* 454 F.3d at 523 (where holders of privilege would have had no opportunity to dispute taint team's privilege determination, court "[did] not see any check in the proposed taint team review procedure against the possibility that the government's team might make some false negative conclusions, finding validly privileged documents to be otherwise"). [FN29] Because the amended order includes these requirements, we conclude that it satisfies art. 12--that is, the amended order prescribes a constitutionally permissible method by which to identify privileged materials and exclude them from review by members of the investigation or prosecution team. [FN30]

While we reach this conclusion in the present case, we also share the skepticism of other courts about the use of a taint team drawn from members of the prosecutor's office. See *In re Search Warrant for Law Offices,* 153 F.R.D. at 59 ("The appearance of Justice must be served, as well as the interests of Justice. It is a great leap of faith to expect that members of the general public would believe any such Chinese wall would be impenetrable; this notwithstanding our own trust in the honor of [a prosecutor]"). In future cases, before a judge may authorize the use of a taint team procedure that draws on members of the prosecutor's office to be the taint team members, the Commonwealth must establish the necessity of doing so; 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. In ruling on a prosecution request to employ a taint team procedure, 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. The judge should consider also in each case the Commonwealth's ability to erect an impenetrable wall between members of the taint team and members of the prosecution team. Relevant to this inquiry will be the size of the particular prosecutor's office. For example, we have 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.

b. *General search warrant.* The amended order appears to contemplate that after the taint team completes its work, the Commonwealth will review all the remaining, nonprivileged e-mails in searching for evidence within the scope of the two warrants. The defendants argue that the court should restrict the Commonwealth to use only certain search terms in conducting its search, in order to limit the search to e-mails that are likely, or at least more likely, to fit within the warrants' scope. In response, the Commonwealth presses its ability to conduct a cursory review of every nonprivileged e-mail.

The Fourth Amendment requires that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." Similarly, art. 14 of the Massachusetts Declaration of Rights requires warrants to be "accompanied with a special designation of the persons or objects of search, arrest, or seizure." This particularity requirement "both defines and limits the scope of the search and seizure, thereby protecting individuals from general searches, which was the vice of the pre-Revolution writs of assistance." *Commonwealth v. Balicki,* 436 Mass. 1, 8 (2002), quoting *Commonwealth v. Freiberg,* 405 Mass. 282, 298, cert. denied, 493 U.S. 940 (1989).

In a different context, we have concluded that "a cursory examination of a computer's files" in searching for evidence within the boundaries of a valid warrant is permissible and does not necessarily violate the particularity requirement of the Fourth Amendment or art. 14. See *McDermott,* 448 Mass. at 776. In fact, we explained that "[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary.... Indeed, the judge or officer issuing the search warrant likely does not have the technical expertise to assess the propriety of a particular forensic analysis." *Id.* See generally Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L.Rev. 1241 (2010). But see *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162, 1179 (9th Cir.2010) (Kozinski, C.J., concurring) (where evidence sought is electronically stored, issuing judicial officer should include in warrant "a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown"). [FN31]

The Commonwealth asserts that the *McDermott* case resolves the limited issue before us, i.e., whether the Commonwealth may conduct a cursory review of all the nonprivileged e-mails to find evidence within the scope of the two warrants. It is not so clear that the case does so. *McDermott* concerned a deadly shooting rampage by the defendant, resulting in murder charges against him. *McDermott,* 448 Mass. at 751. During their investigation of the crime, the Commonwealth's investigators had sought and obtained a warrant to search the defendant's computer files for evidence concerning, inter alia, weapons used and the defendant's mental functioning. *Id.* at 773. The search warrant issued and the search was conducted before the defendant was indicted for murder, and the warrant related directly to the investigation of those murders. See *id.* at 773-774. In the present case, we are concerned with postindictment searches of e-mail accounts pursuant to search warrants that purport to relate to an investigation of crimes distinct from those at issue in the pending indictments. Moreover, in the *McDermott* case, the investigators conducted their preliminary review of the defendant's computer files by using a set of preset search terms. See *id.* at 774, 777.

We take 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. [FN32] See *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d at 1176. See also Kerr, Searches and Seizures in a Digital World, 119 Harv. L.Rev. 531, 565 (2005) (Kerr) ("computer technologies may allow warrants that are particular on their face to become general warrants in practice"); Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 Va. L.Rev. In Brief 1, 11 (2011) ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic"); Note, Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search-Protocol Warrant Restrictions, 49 Am.Crim. L.Rev. 301, 303 (2012) ("the plain view doctrine may transform legally authorized limited searches into prohibited general ones").

The Commonwealth has not yet conducted its post-taint-team search of e-mails in this case. Thus, we do not know whether the Commonwealth during its search will locate particular e-mails for which it will seek later to invoke the plain view doctrine as a basis for their introduction into evidence in this case. Accordingly, we leave for another day the question whether use of the plain view doctrine as a justification for admission of evidence should be precluded or at least narrowed in the context of searches for electronic records, as a means to protect the particularity requirement of the Fourth Amendment and art. 14. See Kerr, *supra* at 576 ("the best way to neutralize dragnet searches is to rethink the plain view exception in the context of digital evidence").

Conclusion. For the reasons discussed, we answer both of the reported questions in the affirmative. The matter is remanded to the single justice for further proceedings consistent with this opinion.

So ordered.

FN1. Punyamurtula Kishore.

FN2. General Laws c. 118E, § 40, punishes the making of false statements or representations in connection with a medical services provider's application for or receipt of payments under the Commonwealth's Medicaid program; G.L. c. 118E, § 41, in relevant part, punishes the solicitation as well as the payment of a bribe or any form of remuneration as an inducement to perform a service that may be paid for under the Medicaid program.

FN3. The Commonwealth filed an unsworn "statement of the case" in the underlying criminal cases pending in the Superior Court, in which the Commonwealth noted that the statement was "not a full and complete recitation of the facts that support the indictments ... and [was] not meant to be a Bill of Particulars." We summarize in the text the Commonwealth's allegations set out in its statement of the case, but express no view on the accuracy or validity of any allegation.

FN4. A sober home is a residential property that provides a sober living environment to its residents. Some sober homes use drug testing to monitor their residents' drug use.

FN5. On September 21, 2011, approximately one week before the return of the

indictments, a criminal complaint issued in the District Court charging Kishore with one count of violating the Medicaid antikickback statute, G.L. c. 118E, § 41. The record before us does not indicate the status of that case.

FN6. The electronic mail (e-mail) service of Google, Inc. (Google) "is a 'cloud-based' email program, meaning the data and applications of the user reside on remote computer servers operated by Google." *Electronic Privacy Info. Ctr.* v. *National Sec. Agency,* 678 F.3d 926, 930 n. 1 (D.C.Cir.2012).

FN7. "NLA" refers to the National Library of Addictions, which, the Commonwealth alleges in its statement of the case, was a charitable organization operated by Kishore.

FN8. The Superior Court judge who reviewed the Commonwealth's December, 2011, search warrant application and issued the search warrant was not the same judge who in June, 2012, issued the amended order that we review in this case (motion judge).

FN9. It does not appear that the Commonwealth reviewed any e-mails from the Church account that it had obtained pursuant to the December 21, 2011, warrant.

FN10. The motion judge reviewed the second search warrant application and issued the warrant on February 28, 2012.

FN11. We describe and discuss the amended order's specific provisions concerning the taint team *infra.*

FN12. The reported question specifically asks whether the Commonwealth may "search the post-indictment e-mails of a criminal defendant," but the parties have treated the question as asking whether the Commonwealth may search a criminal defendant's e-mails postindictment. We also consider the issue of postindictment status to apply to the criminal defendant, not his e-mails--that is, the question raised concerns e-mails of a criminal defendant after he has been indicted, regardless of whether the e-mails are dated before or after the indictment. In answering the question before us, we do not mean to suggest that the same or at least similar issues concerning e-mail searches and the attorney-client privilege could not arise before indictment--where, for example, the Commonwealth seeks to search the e-mails of a person it has charged by way of complaint but not yet by indictment, or of an uncharged person who is the target of an ongoing criminal investigation and who is known by the Commonwealth to have retained counsel in connection with that
investigation.

FN13. Where, as here, the search and seizure of electronically stored information is at issue, "the normal sequence of 'search' and then selective 'seizure' is turned on its head"; first the government seizes the property, then it searches it. See *United States*

v. Bowen, 689 F.Supp.2d 675, 682 (S.D.N.Y.2010), aff'd sub nom. *United States v. Ingram,* 490 Fed.Appx. 363 (2d Cir.), cert. denied, 133 S.Ct. 374, and 133 S.Ct. 630 (2012) (citation omitted).

FN14. The Commonwealth does concede that the first search warrant sought, inter alia, "documents relating to ... financial arrangements between Dr. Kishore and/or PMA ... and/or Massachusetts sober houses that referred residents to PMA for urine drug screen testing." As noted, however, the affidavit in support of the application for the first search warrant does not include any facts establishing probable cause to believe that evidence of the indicted kickback scheme would be found in Kishore's and Church's e-mail accounts.

FN15. Following the parties' lead, when we refer to the issuance of a search warrant, we assume the search warrant issues ex parte. See *Commonwealth v. Bond,* 375 Mass. 201, 205 n. 6 (1978) ("A search warrant issues ex parte and results in an immediate intrusion"). Our understanding that the issuance of a search warrant to seize e-mails implies an ex parte proceeding comports with G.L. c. 276, § 1B, and 18 U.S.C. § 2703 (2006 & Supp. IV 2010), the statutes governing the seizure of e-mails from a third party. Under G.L. c. 276, § 1B, and 18 U.S.C. § 2703(b)(1), when the government uses a warrant to seize an individual's e-mails from a third party, the government need not provide prior notice to the individual; by contrast, when the government uses a trial subpoena to seize any of the individual's e-mails for which a warrant is not required, the government must provide prior notice to the individual. As indicated previously, the issuance of a search warrant for e-mails and resulting seizure of the e-mails pursuant to that warrant are distinct from any search of them. We consider in part 1.b, *infra,* the issue whether notice must be provided to the e-mail user before the search of those e-mails takes place.

FN16. General Laws c. 276, § 1B (*a*), defines "[e]lectronic communication services" and "[r]emote computing services" by reference to the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2006 & Supp. IV 2010) (SCA). An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2006). See 18 U.S.C. § 2711(1) (applying definitions set forth in 18 U.S.C. § 2510 to SCA). A "remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

A single provider may perform both electronic communications services and remote computing services. See, e.g., *Crispin v. Christian Audigier, Inc.,* 717 F.Supp.2d 965, 986-987 & n. 42 (C.D.Cal.2010); *United States v. Weaver,* 636 F.Supp.2d 769, 770 (C.D.Ill.2009). See also Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L.Rev. 1208, 1215-1216 (2004).

FN17. For example, under the SCA, a governmental entity must obtain a search warrant to acquire access to certain e-mails that are 180 days old or less by search warrant; a subpoena is not a permissible means. See 18 U.S.C. § 2703(a). See

also *Crispin v. Christian Audigier, Inc.,* 717 F.Supp.2d at 982; *United States v. Weaver,*636 F.Supp.2d at 771.

FN18. The defendants argue that Mass. R.Crim. P. 14, as amended, 444 Mass. 1501 (2005), which defines the discovery process between parties in a criminal case, also may apply to and govern the Commonwealth's efforts to obtain access to the defendants' e-mail accounts with Google. Because Google is not a party to the criminal case but a third-party holder of records, we

disagree that rule 14 has any application here and, therefore, focus our discussion in the text on the application of Mass. R.Crim. P. 17, 378 Mass. 885 (1979) (rule 17).

FN19. Rule 17 uses the term "summons" instead of "subpoena," but the terms are synonymous. See *Commonwealth v. Lampron,* 441 Mass. 265, 269 n. 5 (2004).

FN20. "The 'prototype' for our rule 17 was Fed.R.Crim.P. 17," to which we have looked for interpretive guidance in past decisions. *Commonwealth v. Odgren,* 455 Mass. 171, 180 (2009). See *Commonwealth v. Lampron,* 441 Mass. at 269.

FN21. As noted, G.L. c. 276, §§ 1 and 1B, authorize the issuance of search warrants. Authority for issuing subpoenas in criminal cases is granted by G.L. c. 233, § 1; G.L. c. 277, § 68; and Mass. R.Crim. P. 17. See *Commonwealth v. Odgren,* 455 Mass. at 178.

FN22. While the Massachusetts Rules of Criminal Procedure do not preclude the Commonwealth from seeking ex parte a warrant to conduct a postindictment search of third-party records, we interpret the rule to create in essence a

presumption that after an indictment issues, the Commonwealth will pursue third-party records pursuant to the procedure spelled out in rule 17.

FN23. See *Commonwealth v. O'Brien,* 432 Mass. 578, 584 (2000) ("When exercising our supervisory powers, we are not limited to correcting error, but may be guided by whatever is needed to ensure that cases are tried fairly and expeditiously"); *Commonwealth v. Bastarache,* 382 Mass. 86, 102 (1980) ("In matters concerned with the administration of the courts and the trial of cases, we may impose requirements [by order, rule or opinion] that go beyond constitutional mandates").

FN24. See *United States v. Regan,* 281 F.Supp.2d 795, 806 (E.D.Va.2002) ("The Court is mindful that the Defendant's ... computers may contain attorney-client information and memoranda; therefore the Court will carefully circumscribe the parameters and method of the search"). Cf. *In re Impounded Case (Law Firm),* 840 F.2d 196, 202 (3d Cir.1988) (reversing trial judge's order requiring return of potentially privileged records seized from law firm because "the attorney-client privilege [was] sufficiently protected by the procedure established by the magistrate requiring that the government obtain leave of the court before examining any seized items").

FN25. See *In re Lott,* 424 F.3d 446, 451-452 (6th Cir.2005), cert. denied, 547 U.S. 1092 (2006) ("disclosure is not remedied merely because a disclosed confidence is not used against the holder in a particular case").

FN26. See, e.g., *United States v. Taylor,* 764 F.Supp.2d 230, 235 (D.Me.2011) ("government behaved reasonably" by seeking judicial approval of proposed search method and giving defendant opportunity to be heard "once its agent noticed that e-mail headers reflected communications between lawyer and client").

FN27. As stated by one court:

"[T]aint teams present inevitable, and reasonably foreseeable, risks to privilege, for they have been implicated in the past in leaks of confidential information to prosecutors. That is to say, the government taint team may have an interest in preserving privilege, but it also possesses a conflicting interest in pursuing the investigation, and, human nature being what it is, occasionally some taint-team attorneys will make mistakes or violate their ethical obligations. It is thus logical to suppose that taint teams pose a serious risk to holders of privilege, and this supposition is substantiated by past experience. In *United States v. Noriega,* 764 F.Supp. 1480 (S.D.Fla.1991), for instance, the government's taint team missed a document

obviously protected by attorney-client privilege, by turning over tapes of attorney-client conversations to members of the investigating team. This *Noriega* incident points to an obvious flaw in the taint team procedure: the government's fox is left in charge of the appellants' henhouse, and may err by neglect or malice, as well as by honest differences of opinion."

In re Grand Jury Subpoenas, 454 F.3d 511, 523 (6th Cir.2006).

FN28. Depending on the circumstances, the Commonwealth's failure to comply with the terms of an order establishing a taint team and defining its procedures could result in the dismissal of the indictments. Cf. *United States v. Neill,* 952 F.Supp. 834, 840-841 (D.D.C.1997), citing *Weatherford v. Bursey,* 429 U.S. 545, 558 (1977) (use of taint team does not violate defendant's Sixth Amendment right to counsel so long as taint team procedure prevents disclosure of privileged communications to prosecution team). In addition, a taint team member who commits a breach of the terms of such an order could be subject to individual discipline, including criminal contempt. Cf. *Birchall, petitioner,* 454 Mass. 837, 848 (2009), quoting *Sodones v. Sodones,* 366 Mass. 121, 130 (1974) (criminal contempt imposed "to vindicate the court's authority and to punish the contemnor for doing a forbidden act or for failing to act as ordered").

FN29. In this regard, see United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 111 (3d ed.2009) (recommending that defense counsel have opportunity to review taint team's results before turning over documents to prosecution in order to enhance legitimacy).

FN30. The defendants' motion to dismiss is not before us. Therefore we do not decide whether the Commonwealth's actual search of some of the allegedly privileged e-mails in Kishore's e-mail account, conducted before the amended order establishing the taint team entered, requires the dismissal of the pending indictments because the search violated the defendants' attorney-client privilege. Nor does our decision preclude the defendants from arguing in the future that their constitutional rights were violated if the Commonwealth fails to follow scrupulously the taint team procedure set out in the amended order.

FN31. The present case does not present the separate but related issue concerning a judge's authority to define the scope of a search warrant for electronic evidence by means of search terms rather than a traditional description of the evidence. See *In re Appeal of Application for Search Warrant,* 2012 VT 102, ¶ 25 n. 12 (2012), cert. denied, 133 S.Ct. 2391 (2013) (distinguishing between decisions concerning "whether certain ex ante

parameters are *required* " and decisions concerning "whether such conditions are a *permissible* exercise of authority" [emphases in original]).

FN32. As indicated at the outset, the Commonwealth has conceded that the affidavit in support of the first search warrant did not establish probable cause to believe that the third category of evidence for which the Commonwealth sought to search--namely, evidence of the alleged kickback scheme that is the subject of the pending indictments--would be found in Kishore's and Church's e-mail accounts.

END OF DOCUMENT