E-Discovery in Criminal Cases: A Need for Specific Rules

Daniel B. Garrie, Esq.[1] & Daniel K. Gelb, Esq.[2]

This article explores how issues concerning electronic evidence and discovery (e-discovery) and its associated electronically stored information (ESI) are not relegated to civil litigation, and that the subject matter has an equal impact on criminal litigation. The folloewing suggests a rapidly growing need for courts to uniformly recognize the increasing necessity for an accused to access ESI in order to effectively build a defense in modern-day criminal prosecutions where the *context* in which the ESI was forensically ascertained may be as important to a defendant as the *content* of the information recovered.

Section I introduces the subject matter of e-discovery and ESI. Section II addresses the manner in which civil litigation pioneered a judicial focus on codifying specific rules of civil procedure governing the pretrial exchange of e-discovery. Section III delves into the manner in which the criminal justice system appears to be handling e-discovery in criminal matters. It further discusses an arguable disconnect between traditional rules of criminal procedure addressing pretrial discovery and the growing need for modernization of the rules in criminal proceedings to *specifically* direct parties

---

1. Daniel Garrie, Esq. holds a BA and MA in Computer Science. He serves as a neutral and mediator for resolving e-discovery and technology advising on many cases and over 40 e-discovery cases last year. He also serves by court appointment as Special Master focusing on e-discovery disputes in state and federal courts with Alternative Resolution Centers (www.arc4adr.com) all over the country. He is also a Managing Director at FSRDG LLC (www.fsrdg.com), a world-class boutique legal strategy consulting firm. He was previously a principal and Director of E-Discovery at the leading global consulting firm of Charles Rivers Associates International (CRA). Prior to joining CRA, Mr. Garrie was a Vice President of LegalTech Group, where he founded and built a boutique legal strategy consulting firm that focused on providing e-discovery, litigation readiness, digital privacy, and digital information risk management. Mr. Garrie has published more than fifty articles and books on various electronic discovery issues and has spoken to judges, attorneys and technologists on electronic discovery and information risk management. He is actively involved with the Sedona Conference WG1. He can be reached at dgarrie@fsrdg.com.

2. Daniel K. Gelb, Esq.is a partner at Gelb & Gelb LLP in Boston, Massachusetts (www.gelbgelb.com), and would like to thank his father, Richard Gelb, Esq., with whom he practices for his insight and contribution to this article. Daniel Gelb represents clients at both the state and federal levels in white collar and general criminal defense matters, complex civil litigation concentrating in business and securities, arbitration and regulatory proceedings. Prior to joining Gelb & Gelb LLP, Mr. Gelb was an Assistant District Attorney with the Norfolk County District Attorney's Office in Massachusetts. He is a member of the National Association of Criminal Defense Lawyers' E-Discovery Task Force, an Advisory Board Member of BNA, Inc.'s *White Collar Crime Report*, chairs the Massachusetts Bar Association's Implementation of Technology Taskforce, and is a member of The Sedona Conference's Working Group on Electronic Document Retention & Production. The opinions and analyses contained herein are that of the authors only and should not be interpreted as legal advice.

on how to uniformly interact concerning ESI where such directions exist in civil litigation matters.[3] Moreover, Section IV addresses the concern that the status quo of e-discovery in criminal matters places parties that lack financial resources at a substantial disadvantage, as opposed to those who are able to retain legal counsel to navigate e-discovery issues. Section V discusses the constitutional implications surrounding e-discovery in criminal matters. Sections VI and VII discuss a proposal for a "balancing test" and possible pretrial discovery tools for the exchange of ESI beyond that which is contemplated in more traditional rules of criminal procedure currently followed by the courts.

I. INTRODUCTION

Criminal defense lawyers are as obligated as their civil law brethren to be conversant with electronic discovery and its various attendant forms of electronically stored information in order to effectively represent their clients. Modern day communications, through email, the Internet, instant messaging, electronic faxing, and digital voicemail, expand the nature and location of "relevant evidence" as well as the obligations to obtain, preserve, produce and manage this evidence.

ESI evidence when handled properly, or if mishandled, can significantly impact the outcome of a client's civil or criminal case. Importantly, e-discovery assumes a critical role unique to criminal proceedings. Unlike hard copy documents and tangible evidence (e.g., gun, picture, clothing, etc.), ESI may contain exculpatory evidence that may not be readily apparent to the prosecution, who maintains custody and control over the ESI. Additionally, the prosecution may improperly possess ESI that should be the subject of a motion to suppress. Finally, the dynamic nature of ESI has the potential to develop into *Brady*[4] material. The government's obligations under *Brady* are not rooted in any particular constitutional right to discovery, but rather in the due process protections defendants are afforded in criminal proceedings.[5]

A. How to Obtain Electronic Evidence

A significant issue many criminal defendants may encounter is ascertaining and obtaining electronic evidence in the possession of the prosecution. The greatest challenge may well lie in successfully convincing the court that the prosecution's approach to the pre-trial exchange of ESI will adversely impact the defendant's constitutional and procedural rights in building a full and fair

3. *See* FED. R. CIV. P. 26; FED. R. CIV. P. 34.

4. Brady v. Maryland, 373 U.S. 83 (1963) (addressing evidence in custody of prosecution that would exculpate accused or mitigate guilt).

5. *See* 2 CHARLES ALAN WRIGHT ET AL., FED. PRAC. & PROC. § 254.2 (quoting U.S. v. Bagley, 473 U.S. 667, 675 (1985)).

defense to the government's charges. The expense and burden of e-discovery must be balanced against the potential of a criminal defendant losing one's liberty.

B. What the Constitution Says About Electronic Discovery

The United States Supreme Court primarily has grounded a defendant's rights to fairness in the criminal process on the defendant's right to invoke the protection of the Fifth Amendment.[6] Moreover, the Due Process Clause applies to each state via the Fourteenth Amendment of the Constitution, which "in effect affirms the right to trial according to the process and proceedings of the common law."[7]

Due process, as a general proposition, adapts to *facts* as they are presented in specific circumstances, and is a progressive principle that has been applied to mediums containing ESI, such as search warrants of computers and testimonial evidence on audio tape.[8] Even though today's technological mediums did not exist when the Due Process Clause was codified, the judicial system has recognized that a defendant's rights must be expanded to accommodate contemporary applications.[9] Evidentiary forms like ESI should be governed by the same Due Process analysis courts have recognized in the past when considering new forms of evidence. The just obligation to make relevant evidence available to the accused or suppress its use when improperly obtained resides with the judicial system as the ultimate protector of a defendant's constitutional rights.

C. The State of Criminal Electronic Discovery Today

Unfortunately, the criminal justice system as of yet has not expanded the Federal Rules of Criminal Procedure in a manner which would ensure that

---

6. See U.S. v. Stein, 435 F. Supp. 2d 330, 357 (S.D.N.Y. 2006).

7. *See* 1 WAYNE R. LAFAVE, CRIM. PROC. § 2.4(b) (3d ed.) (citing 3 J. STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1783 (1833)) ("The original meaning of due process"); *see also* 3 J. STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1783 (1833) (referencing Daniel Webster's argument in the *Dartmouth College* case). Webster similarly stated that "by the law of the land is most clearly intended the general law: a law, which hears before it condemns; which proceeds upon inquiry, and renders judgment only after trial." Dartmouth College v. Woodward, 17 U.S. (4 Wheat.) 518 (1819).

8. *See* U.S. v. Laine, 270, F.3d 71, 76 (1st Cir. 2001).

9. As Justice Brandeis stated in his dissenting opinion in *Olmstead*:

> We have . . . held that general limitations on the powers of government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the states from meeting modern conditions by regulations which a century ago, or even half a century ago, probably would have been rejected as arbitrary and oppressive. Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.

Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

criminal defendants receive reasonable access to ESI evidence sufficient for their counsel to advocate capably for the protection of their Fourth,[10] Fifth[11] and Sixth[12] Amendment rights. Further driving the need for the right electronic discovery rule framework is that, without a rule, the judicial systems risks collapse soon. Because the vast majority of criminal defendants are indigent, and thus, without funds to pay for costly electronic discovery, they could potentially bankrupt the judicial system.[13]

II. CIVIL LITIGATION PIONEERS OF "ELECTRONIC DISCOVERY"

The concept of "electronic" evidence is now commonplace in civil litigation. In fact, in 1970, the Federal Rules of Civil Procedure were amended to incorporate "data compilations" as discoverable items.[14] The Advisory Committee Notes for the 1970 amendments acknowledge that the intent of the revision was to bring the discovery process into accord with changing technology.[15] Over the past decade, there have been further attempts to keep e-discovery on pace with technological advances, as reflected in such cases as *McPeek v. Ashcroft*,[16] *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*[17] and *Zubulake v. UBS Warburg, LLC*.[18] These cases have led to

10. U.S. CONST. amend. VI; *see also* FED. R. CRIM. P. 41(c)(1) (requiring magistrate issue warrant identifying property for seizure and person or place to be searched).

11. U.S. CONST. amend. V.

12. U.S. CONST. amend. VI.

13. *See* CAROLINE WOLF HARLOW, U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS SPECIAL REPORT: DEFENSE COUNSEL IN CRIMINAL CASES 1 (2000); STEVEN K. SMITH AND CAROL J. DEFRANCES, U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS SELECTED FINDINGS: INDIGENT DEFENSE 1, 4 (1996).

14. FED. R. CIV. P. 26; *see also* Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94CIV2120 (LMM) (AJP), 1995 WL 649934, at *1 (S.D.N.Y. Nov. 3, 1995) (acknowledging computerized data compilations can be discoverable).

15. *See* Proposed Amendments to the Federal Rules of Civil Procedure Relating to Discovery, 48 F.R.D. 487, 527 (1970).

16. 202 F.R.D. 31 (D.D.C. 2001). The *McPeek* court used a marginal utility approach to order the producing party to restore a limited number of backup tapes containing emails that may have been pertinent to the case. *Id.* at 34. The court held that there was enough likelihood of finding responsive emails in backup tapes created between July 1, 1998 and July 1, 1999 to justify imposing the costs of the search on the producing party. *Id.* The court further ordered the producing party to keep a record of its costs so the parties could argue whether the search results would justify further backup tape restoration. *Id.* at 35.

17. 205 F.R.D. 421 (S.D.N.Y. 2002). In *Rowe*, a producing party moved for a blanket protective order precluding discovery of email stored on backup disks. *Id.* at 423-24. The court held that, while there was no justification for a blanket protective order, the costs associated with restoring and producing the emails should be shifted to the requesting party. *Id.* at 428, 433. In doing so, the court created and applied an eight-factor cost-shifting test. *Id.* at 429.

18. 217 F.R.D. 309 (S.D.N.Y. 2003). In a gender discrimination suit against her former employer, the plaintiff requested that the defendant produce "all documents concerning any communication by or between UBS employees concerning plaintiff". *Id.* at 312. The defendant produced 350 pages of documents, including approximately 100 pages of email. *Id.* at 312-13. The plaintiff knew that additional responsive emails existed because she, in fact, had produced approximately 450 pages of email from her own correspondence. *Id.* at 313. The plaintiff then requested that the defendants produce the additional email from archival media. *Id.* at 313. Claiming undue burden and expense, the defendant urged the court to shift the cost of production to the plaintiff, citing the *Rowe* decision. *Id.* at 317. The court noted that the application of *Rowe*'s eight-factor, cost-

corporations being ordered to preserve and "produce, sometimes at considerable expense, computerized information, including email messages, support systems, software, voicemail systems, computer storage media and backup tapes and telephone records."[19] On December 1, 2006, the federal courts responded to the growing demands and complexities of e-discovery by amending the Federal Rules of Civil Procedure to address discovery and ESI issues.[20]

A. The Definition of Electronic Stored Information under the Civil Rules

The amended Federal Rules of Civil Procedure defined ESI and set out a series of requirements for parties to identify ESI at the start of litigation. Specifically, amended Rule 34(a) defines ESI as "other data or data compilations . . . stored in any medium from which information can be obtained directly or, if necessary, after translation by the responding party into a reasonably usable form."[21] Courts have applied the amended rules by requiring both corporate and individual parties to preserve,[22] identify,[23] disclose,[24] and produce,[25] on pain of monetary and other sanctions, relevant information on any electronic device.

B. Doctrine of Safe Harbor and Spoliation

The amended Federal Rules of Civil Procedure also recognized a limited safe harbor from sanctions arising from the loss of electronically stored information as a result of the "routine, good faith operation of an electronic

---

shifting test may result in disproportionate cost-shifting away from large defendants. *Id.* at 320. It then modified the test to include only seven factors. *Id.* at 322. Applying the modified test, the court ordered the defendant to produce, at its own expense, all responsive email existing on its optical disks, active servers, and five backup tapes selected by the plaintiff. *Id.* at 324. Discovery of emails stored on the additional eighty-nine backup tapes remained contingent upon a successful initial search of the first five tapes. *Id.*

19. Peter Brown, *Developing Corporate Internet, Intranet, and E-mail Policies*, 520 PLI/PAT 347, 364 (1998) (citing *In re* Brand Name Prescription Drugs Antitrust Litigation, No. 94C897, 1995 WL 360526 (N.D. Ill. June 15, 1995)); *see also* FED. R. CIV. P. 34.

20. *See* FED. R. CIV. P. 16, 26, 33, 34, 37, and 45.

21. FED. R. CIV. P. 34.

22. *See, e.g.*, Arista Records LLC v. Usenet.com, Inc., 60 F. Supp. 409, 442-44 (S.D.N.Y. 2009) (imposing attorneys' fees, costs, and adverse inference sanction for defendant's failure to preserve data); Fox v. Riverdeep, Inc., No. 07 Civ. 13622, 2008 U.S. Dist. LEXIS 101633, at *18-20 (E.D. Mich. Dec. 16, 2008) (sanctioning defendant for failure to preserve evidence, including emails, upon receiving cease-and-desist letter).

23. *See* Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 644 (D. Colo. 2007) (imposing monetary sanctions and awarding costs where defendant failed to identify and preserve relevant ESI).

24. *See* Amersham Biosciences Corp. v. PerkinElmer, Inc., 2007 WL 329290 (D.N.J. 2007) (unpublished letter decision).

25. *See* Gordon Partners v. Blumenthal, 244 F.R.D. 179 (S.D.N.Y. 2007) (imposing adverse inference spoliation sanction in securities fraud action because defendant corporation had the practical ability to obtain documents it needed from a non-party corporation and defendant corporation's failure to preserve relevant email was grossly negligent).

information system."[26] However, the application of this rule requires that the producing litigant demonstrate[27] that it tried to preserve in good faith evidence it knew or should have known to be relevant to reasonably anticipated or commenced litigation.[28] In addition, the amended rules address digital spoliation[29] by recognizing that it can occur in various ways and result in varying penalties depending upon the facts and legal context in which the claim arises.[30]

C. Shifting Costly Electronic Discovery in Civil Litigation

While cost has always been a discovery concern, the advent of "e-discovery" has raised such concerns to a high level, especially when ESI impacts the manner in which a case may proceed.[31] Since 1970, courts have struggled to integrate the highly variable cost structure associated with producing ESI into the Federal Rules of Civil Procedure's[32] traditional discovery principles.[33] Electronic discovery consultant fees can typically start at $275 per hour and costs of collecting, reviewing and producing a single email can be between $2.70 and $4 per document.[34] Experts in this market estimated that in 2007, litigants would spend more than $2.4 billion on electronic discovery services

26. *See* FED. R. CIV. P. 37(e). Note that the good faith requirement of Rule 37(e) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. Nonetheless, this requirement is not explicit.

27. *See* Doe v. Norwalk Community College, 2007 WL 2066497 (D. Conn. July 16, 2007) (finding defendant's failure to suspend document destruction after notice of litigation not good under Rule 37(f)).

28. *See* Columbia Pictures Industries v. Bunnell, 2007 WL 2080419, at *14 (C.D. Cal. May 29, 2007); Hynix Semiconductor v. Rambus, Inc., 591 F. Supp. 2d 1038, 1060 (N.D. Cal. 2006); W.T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984).

29. *See Spoliation—Definition from the Merriam-Webster Online Dictionary*, http://www.merriam-webster.com/dictionary/spoliation ("The act of injuring, especially beyond reclaim.").

30. *See* Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071, at *7 (Fla. Cir. Ct. Mar. 1, 2005) *rev'd on other grounds sub nom* Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc., 955 So. 2d 1124, 1128 (Fla. Dist. Ct. App. 2007).

31. For example if the collection, review and production of ESI is cost prohibitive to asserting or defending a claim, civil litigants are forced to settle because no formal cost structure was codified into the new Federal Rules of Civil Procedure.

32. *See* Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978) (holding under Federal Rules, respondent must bear expenses of discovery). The presumption is that the responding party must bear the expense of complying with discovery requests, but he may invoke the district court's discretion under Rule 26(c) to grant orders protecting him from 'undue burden or expense,' thereby precluding discovery or conditioning discovery on the requesting party's payment of discovery costs. *Id.*

33. *See* Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 421 (S.D.N.Y. 2002) (adopting multiple factor test to allocate the costs of electronic discovery burden); *In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, at *2 (N.D. Ill. 1995) (unpublished memorandum opinion) (holding producing party bears costs because the party chose electronic storage). *Compare* McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) (restoring all backup tapes not necessary in every case), *with* Linnen v. A.H. Robins Co., 199 WL 462015, at *9-10 (Mass. Super. Ct. 1999) (imposing obligation to cease recycling backup tapes).

34. See Anne G. Fort, *Rising Costs of E-Discovery Requirements Impacting Litigants*, National Law Journal, March 20, 2007, *available at* http://www.law.com/jsp/article.jsp?id=1174307784199.

and there is no end in sight to this growth. Only two years later, this expense had increased.[35]

The construct of proportionality respective to discovery requests is gaining traction with the courts. Judges and lawyers alike realize that discovery costs[36] can be determinative of a litigant's decision to litigate or settle a case.[37]

III. BASIC CRIMINAL ELECTRONIC DISCOVERY

In the federal criminal justice system, there is no landmark case or rule which operates as a counterpart to the Federal Rules of Civil Procedure on e-discovery.[38] There are examples, such as *United States v. O'Keefe*,[39] where the federal judiciary addressed the developing influence the Federal Rules of Civil Procedure's e-discovery standards have had on criminal litigation.[40] Despite these examples, the Federal Rules of Criminal Procedure do not afford criminal defendants an established right to access ESI beyond the scope of Rule 16 (for evidence in the custody of the government) or Rule 17 (for evidence in the possession of third parties). Although the accused may argue that the spirit of the Federal Rules of Criminal Procedure provides criminal defendants with a constitutional right to access ESI in the possession, custody, and control of the prosecution (e.g., *Brady*), in practice, the criminal justice system is devoid of procedural tools that provide criminal defendants with *automatic* access to ESI in the same fashion civil litigants enjoy pursuant to Rule 26 of the Federal Rules of Civil Procedure. Certain cases are emerging, however, that clearly evidence the need for specific rules of criminal procedure relating to ESI.[41]

At the federal level, a criminal defendant is "entitled to rather limited discovery, with no general right to obtain the statements of the [g]overnment's witnesses before they have testified."[42] Therefore, it is not unreasonable to assume this principle would apply to items such as email, text messages and

35. *Id.*

36. *See* FINAL REPORT ON THE JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND THE INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM (2009), *available at* http://www.actl.com/AM/Template.cfm?Section=Home&template=/CM/ContentDisplay.cfm&ContentID=4030 (last visited, Sept. 17, 2009). The American College of Trial Lawyers Task Force on Discovery recently issued their final report based on their survey of the Fellows of the American College of Trial Lawyers.

37. *See* Cason-Merenda v. Detroit Med. Ctr., 2008 WL 2714239 (E.D. Mich. July 7, 2008) (denying defendant's cost-shifting motion made after the costs had been incurred); Petcou v. C.H. Robinson Worldwide, Inc., 2008 WL 542684 (N.D. Ga. Feb. 25, 2008) (denying plaintiff's motion to compel discovery of eight years of emails).

38. *See* Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978) (holding under the Federal Rules, presumption is responding party bears expense of compliance).

39. 537 F. Supp. 2d 14 (D.D.C. 2008).

40. *Id.* (addressing the impact of the evolution of e-discovery in civil litigation on criminal litigation matters).

41. *See, e.g.*, Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (addressing appropriate metrics in analyzing application for search warrants seeking ESI).

42. Degan v. United States, 517 U.S. 820, 825 (1996).

other forms of ESI. In a civil case, by contrast, a party is entitled as a general matter to discovery of any information sought if it is relevant and "reasonably calculated to lead to the discovery of admissible evidence."[43] This imbalance places criminal defendants potentially at risk of being denied access to what may be legitimate "*Brady* material."[44] Without a uniform procedural rule in criminal proceedings, defendants place themselves in forums where a party's ability to access ESI varies from court to court.[45] The lack of a codified procedure in the Federal Rules of Criminal Procedure for gaining access to ESI, similar to what the Federal Rules of Civil Procedure provides, potentially places criminal defendants at a substantial disadvantage when gathering evidence.[46]

Unlike in civil litigation matters, where a litigant's right to access ESI from an opposing party is codified, in criminal litigation, pre-trial exchange of ESI is not incorporated into the rules of criminal procedure. Moreover, a criminal defendant is typically at the mercy of the prosecution's own policies as to whether to produce certain ESI evidence, as well as the manner and form of production.[47] The discrepancy in how ESI is exchanged between parties to civil versus criminal proceedings may be attributable, among other reasons, to the fact that the concept of proportionality is a far more prominent consideration in civil cases than in criminal matters. Arguably, the government is not as concerned with how the cost of pursuing ESI compares with the value of the evidence likely to be derived from it. This issue is often encountered in the context of grand jury subpoenas where a target may be inclined to challenge the scope of a subpoena seeking burdensome volumes of ESI. The government may then be concerned that an over-reaching subpoena will threaten the overall viability of the government's case; however, it is more likely than not that the subpoena will be pursued by the prosecutor until a motion to quash or amend

43. *See id.* For the purposes of this article, *Degan* is cited for comparing Rules 16(a)(2) and 26.2 of the Federal Rules of Criminal Procedure with Rule 26(b)(1) of the Federal Rules of Civil Procedure. For exceptions regarding witness statements not subject to disclosure under Rule 16(a)(2) of the Federal Rules of Criminal Procedure, see 18 U.S.C. § 3500; *see also* FED R. CRIM. P. 16 (regarding witness statements made when an organizational defendant is involved).

44. *See* Brady v. Maryland, 373 U.S. 83 (1963) (defining *Brady* material). *Brady* covers exculpatory evidence either absolving or mitigating a defendant's criminal liability, or, in the alternative, evidence that tends to undercut the government's case (e.g., impeachment evidence).

45. An example of where an approach to ESI evidence is likely to vary is in the context of evidence maintained by the government when investigating and prosecuting offenses derived from the Adam Walsh Child Protection and Safety Act of 2006. The Walsh Act established, among other things, a national database incorporating the use of DNA evidence collection in addition to a DNA registry that tracks convicted sex offenders with Global Positioning System technology. As particularly important laws of this nature are, it is presented here as an example of a context where a defendant's access to the government's electronic database could be outcome determinative for the defendant.

46. E-discovery has become more prevalent in the current-day criminal justice system. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 574–76 (D.N.J. 2001).

47. FED. R. CIV. P. 26(f)(3) (codifying discovery of ESI).

the subpoena is adjudicated.[48] Therefore, challenging a subpoena *duces tecum*, for example, is a much more daunting task for a criminal defendant than is a civil litigant's challenge to a request for production of documents by way of a protective order.[49]

Moreover, challenging the government's approach to e-discovery could be a perilous endeavor for a defendant who is attempting to resolve a prosecution in order to eliminate or reduce exposure to potential penalties.[50] For example, defendants may have to decide whether to challenge a grand jury subpoena or a search warrant, knowing that doing so may present the appearance of non-cooperation, which could adversely affect the opportunity to enter into a satisfactory plea or deferred prosecution agreement.

Likewise, many cases pursued by prosecutors are investigated in tandem (within the parameters of the laws governing parallel proceedings) with other governmental agencies that may be investigating potential civil and/or regulatory violations of federal laws (e.g., securities law, health care regulations, intellectual property guidelines, etc.).[51] Therefore, the lack of common procedures among forums for the handling of ESI may adversely affect individuals who produce ESI to the government in non-criminal proceedings without knowing whether they are targets or witnesses in criminal actions. [52] As annoying as such assertions of obstacles to ESI production on behalf of the defendant may be to the prosecution, well-settled Sixth Amendment[53] precedent mandates that defendants have a constitutional right to know exactly the nature and cause of the government's case. This precept, when applied to twenty-first century practice, should involve the production (or at the very least the inspection) of ESI. [54] Defendants who do not diligently

48. FED. R. CRIM. P. 6 (setting forth grand jury procedure).

49. FED. R. CIV. P. 34 (providing rules for producing documents); FED. R. CIV. P. 26 (governing protective orders).

50. Earl J. Silbert & Demme Doufekias Joannou, *Under Pressure to Catch the Crooks: The Impact of Corporate Privilege Waivers on the Adversarial System*, 43 AM. CRIM. L. REV. 1225, 1230 (2006).

51. 1 JOEL ANDROPHY, WHITE COLLAR CRIME § 4:5 (2d ed. 2009) (mitigating criminal exposure in Bankruptcy Court).

52. *Id.* at § 7:16. Androphy wrote:

> [A] defendant pled guilty to a drug charge. The defendant signed a plea agreement agreeing to forfeiture of the $3,000 on his person at the time of his arrest and making no mention of the possibility of any further forfeiture. The AUSA had previously told defendant that the United States Attorney's office had no interest in seizing defendant's farm but that she could not speak for the IRS. After conviction, the IRS sought to forfeit defendant's farm. The court found that, without an express warning by the United States to the defendant to the contrary, it was reasonable for defendant to rely on the original oral understanding he had with the AUSA that his farm would not be seized.

Id.

53. U.S. CONST. amend. VI.

54. Nevertheless, a defendant has the general right to file an omnibus discovery motion seeking discovery corroborating the government's case. *Rosen v. United States*, 161 U.S. 29 (1896) (holding defendant

pursue ESI are at risk, especially when the indictment is facially unclear about the nature of the conduct being prosecuted, as well as and the location and nature of electronic evidence that may be central to the charge.[55]

Notably, if the manner in which ESI is to be exchanged between the prosecution and defense were to become more established and streamlined, evidentiary disputes in criminal investigations and prosecutions would likely be eliminated or at least minimized, and the approaches of the judicial system would be more predictable and consistent. In other words, a more effective approach to ESI in criminal matters would likely lead to parties resolving criminal matters at earlier stages in the proceedings by narrowing evidentiary issues.[56]

IV. CRIMINAL ELECTRONIC DISCOVERY TACTICS FOR THOSE WHO ARE POOR BUT NOT POOR ENOUGH

Not all defendants have access to, let alone the financial resources to engage, e-discovery vendors in order to "cooperate" with the government and avoid indictment.[57] Yet, all defendants should be entitled to build a defense and advocate for the most favorable outcome.

As technology becomes ever more inextricably tied to the way people communicate[58] and the way evidence develops, criminal defendants will likely seek discovery of ESI from third parties as well as the government.[59] Addressing ESI is a tactical decision defendants must make when conferring with criminal defense counsel because the approach may impact the course of the case, as well as the government's perception of whether a target is cooperating. Counsel who does not press the government effectively to produce ESI may deprive the client of an adequate defense.[60] Counsel should

---

entitled "to be informed of . . . nature and cause of . . . accusation against him").

55. *See* Mosteller, Robert P., *Exculpatory Evidence, Ethics, and the Road to the Disbarment of Mike Nifong: The Critical Importance of Full Open-File Discovery*, 15 GEO. MASON L. REV. 257 (2008).

56. For example, the manner of resolving discovery disputes through Rule 26(f) of the Federal Rules of Civil Procedure, which concerns conferencing civil proceedings, could provide guidance in criminal proceedings.

57. *See* Robert M. Barker, Andrew T. Cobb, and Julia Karcher, 52-2 BUSINESS HORIZONS (2009).

58. *See, e.g.*, Jean-Luc Chatelain and Daniel B. Garrie, *The Good, the Bad and the Ugly of Electronic Archiving*, 2 J. OF LEGAL TECH. RISK MANAGEMENT 96, 97 (2007).

59. *See* FED. R. CRIM. P. 17(c)(1). The rule states:

> [a] subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

Id. See generally OFFICE OF LEGAL EDUCATION OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

60. Criminal defendants should acknowledge that although "cooperation" with the government's

also investigate all sources that may be available to clients for underwriting the expense of e-discovery such as directors and officers insurance.[61]

Criminal defendants who lack substantial financial resources necessary to retain counsel[62] to explore pre-indictment relief tools[63] may be financially eligible for appointment of a public defender. In other words, they must meet certain criteria under the Criminal Justice Act (CJA), which also applies to appointment of CJA "panel counsel."[64] Those criminal defendants that are unable to afford counsel prior to indictment are at a substantial disadvantage,[65] particularly where a governmental investigation focuses on the seizure of ESI.[66] Those defendants who are unable to retain legal counsel pre-indictment may be unable to demonstrate to the prosecution the existence of ESI that might have deterred the government from pursuing the charges prior to indictment of the matter.[67]

Another problem that plagues all defendants other than the super wealthy is that they generally are not able to retain legal representation pre-indictment, and thus forego the chance of potentially being able to alter their "status" with the government. For example, there are times when individuals will be first considered "witnesses" and then turn into "targets" of the prosecution as an investigation progresses. There are times when "targets" are able to cooperate with the prosecution and may be able to avoid an indictment or obtain a more favorable result as to criminal liability than if the target had not effectively communicated with the prosecution. Unfortunately, this witness-versus-target dynamic is not accessible to all. Instead, it is typically accessible to wealthier

---

investigation will typically assist the defendant's potential of ingratiating oneself with the prosecution, in any given matter, this is never a guarantee, which is why such strategic decisions must be fully vetted when seeking discovery such as ESI and other forms of what may arguably be considered unconventional discovery where the context of the information is equally if not more important to the defendant than merely the contents of a communication (e.g., email versus the meta data associated with the authored communication). *See generally* UNITED STATES ATTORNEYS MANUAL, Title 9 (Criminal Division), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/title9.htm (recommending how federal prosecutors handle discovery in the course of building a criminal case).

61. *See* Press Release, U.S. Dep't of Justice, Fiat Agrees to $7 Million Fine in Connection with Payment of $4.4 Million in Kickbacks by Three Subsidiaries under the U.N. Oil for Food Program (Dec. 22, 2008) (on file with author).

62. *See* Caroline Wolf Harlow, Ph.D., *Defense Counsel In Criminal Cases* (Bureau of Justice Statistics) (Nov. 2000), *available at* http://www.ojp.gov/bjs/pub/pdf/dccc.pdf (noting "[i]ndigent defense involves use of publicly financed counsel; defendants unable to afford private counsel"). The report states that "[a]t the end of their case approximately 66% of felony Federal defendants and 82% of felony defendants in large State courts were represented by public defenders or assigned counsel." *Id.*

63. JOEL ANDROPHY, 1 WHITE COLLAR CRIME § 2:3 (2d ed.) (explaining how federal courts regulate the manner in which grand jury investigations are conducted).

64. See 18 U.S.C. 3006A(a)(1) (ensuring adequate representation of federal criminal defendants).

65. For a detailed explanation of the importance of the criminal prosecutorial process and an accompanying flowchart, *see* The Justice System: What is the Sequence of Events in the Criminal Justice System, http://www.ojp.usdoj.gov/bjs/justsys.htm#entry (explaining criminal procedure subsequent to arrest).

66. *Id.*

67. *Id.*

litigants because CJA counsel is appointed by courts post-indictment, and litigants lacking financial resources are unlikely to afford the substantial cost of pre-indictment legal representation. If evidentiary issues surrounding ESI are at the heart of a criminal investigation, the subject or witness of such an investigation can substantially benefit from the representation of legal counsel in the "pre-indictment" stages. The reality is that a substantial number of defendants cannot afford legal counsel, and as technology becomes more involved in legal matters, those who wish to cooperate with the government in areas such as e-discovery may not know how to do so effectively due to a lack of financial and technological resources.[68]

V. CONSTITUTIONAL IMPLICATIONS OF THE E-DISCOVERY STATUS QUO

Historically, criminal defendants have been concerned with issues pertaining to Fourth Amendment protections of their persons,[69] Fifth Amendment protections of statements they made to the government,[70] and Sixth Amendment protections to their right to challenge third-party statements made to the government.[71] The following are some examples of constitutional issues counsel should consider where ESI may be central to the procedural aspects of a defense.

A. Fourth Amendment & Electronic Discovery

The Fourth Amendment protects individuals from unreasonable governmental searches and seizures of their property. Like any other business entity, electronic communications are used by modern day law enforcement. A major tenet of due process is that all individuals prosecuted in the United States enjoy a reasonable expectation of privacy surrounding their person and personal effects. The due process principle is triggered whenever the government oversteps its bounds and improperly seizes evidence. E-discovery is especially fertile ground for motions to suppress because ESI is dynamic and can be fragile, so its mishandling may unlawfully interfere with a defense.

A Fourth Amendment challenge is triggered when: (1) the challenged

68. The fact that the average defendant may not have the resources to retain an attorney pre-indictment where e-discovery is central to the government's case-in-chief raises critical questions as to the constitutionality of such procedural disadvantages faced by the criminal defendant with limited financial resources for building a defense in such cases, particularly where traditional challenges to the presentment of evidence to the grand jury could be raised with the court had the defendant been represented by counsel during the investigation phase of a matter. *See In re* Grand Jury Investigation of Hugle, 754 F.2d 863, 864 (9th Cir. 1985); *In re* Grand Jury Investigation of Lance, 610 F.2d 202 (5th Cir. 1980); In the Matter of the Special April 1977 Grand Jury, 587 F.2d 889, 891-92 (7th Cir. 1978); Westin v. McDaniel, 760 F. Supp. 1563 (M.D. Ga. 1991), *aff'd*, 949 F.2d 1163 (11th Cir. 1991).

69. *See* Smith v. Maryland, 442 U.S. 735 (1979).

70. *See* Miranda v. Arizona, 384 U.S. 436 (1966).

71. *See* Crawford v. Washington, 541 U.S. 36 (2004).

intrusion is the product of governmental action;[72] (2) the intrusion breaches society's objectively reasonable expectation of privacy;[73] and (3) the intrusion breaches the legitimate expectations of privacy of the individual in question.[74] The Supreme Court has affirmed that defendants do not maintain a reasonable expectation of privacy in information voluntarily revealed to third parties.[75]

A warrant is required before every search or seizure, "subject only to a few specifically established and well-delineated exceptions."[76] Most targets of a criminal investigation are not privy to information from inter-governmental agency efforts, such as the government's motive in issuing administrative subpoenas that may be related to a parallel proceeding, the existence of which the target is not yet aware. [77] Defendants must be cognizant of why an agency is seeking certain ESI through discovery tools available to it in a civil litigation or regulatory proceeding, and whether such forums have been pursued as a pretext for building a criminal prosecution.[78]

1. Valid Evidence for Search Warrant

Targets of criminal prosecutions should ascertain whether the government obtained evidence pursuant to a valid search warrant, especially when the government seizes ESI based on an affidavit that did not appropriately (or even worse, truthfully) describe the places to be searched and items to be seized from an information system.[79] This challenge, known as a *Franks* Hearing, is advanced by defendants attacking the truthfulness of the facts contained in an officer's statements made to obtain a search warrant.[80] In order to be entitled to a *Franks* hearing, a defendant must make a substantial preliminary showing that the affidavit contains a false statement made by the affiant law

72. *See* Bd. of Educ. v. Earls, 536 U.S. 822 (2002) (recognizing public school teachers are government actors).

73. U.S. CONST. amend. IV. 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.

Id.

74. ANDREA K. GEORGE, SEARCHES, SEIZURES AND STATEMENTS: THE BUSY LAWYER'S HANDBOOK ON THE 4TH, 5TH & 6TH AMENDMENTS (Federal Defender's Office, District of Minnesota) (Updated October 25, 2007).

75. Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

76. Katz v. United States, 389 U.S. 347, 357 (1967).

77. *See* United States v. Stringer, 408 F. Supp. 2d 1083, 1089-90 (D. Or. 2006) (dismissing indictments due to DOJ's pretextual use of SEC civil investigation to develop case).

78. *Id.*

79. Franks v. Delaware, 438 U.S. 154 (1978).

80. The *Franks* test not only applies to cases where false information is included in an affidavit, but also when affiants omit material facts "with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading." United States v. Reivich, 793 F.2d 957, 961 (8th Cir. 1986).

enforcement agent, who either knowingly and intentionally made the false statement, or did so with reckless disregard for the truth.[81] In addition, for a defendant to prevail in a *Franks* hearing, the false statement must be shown to have been necessary for the court to find probable cause to issue the warrant.[82]

2. FOURTH AMENDMENT AND IMPEACHMENT EVIDENCE

ESI is not only an area of discovery that is likely to be implicated in the *Franks* hearing context. Issues relating to ESI also come into play when a defendant is forced to challenge whether the prosecution, regardless of good or bad faith, failed to produce impeachment evidence of its witnesses pursuant to *Giglio v. U.S.*[83] *Giglio* held that "[w]hen reliability of a given witness may well be determinative of guilt or innocence, nondisclosure of evidence affecting credibility falls within [the] general rule" that "suppression of material evidence justifies a new trial irrespective of good faith or bad faith of the prosecution."[84]

The Supreme Court reversed Giglio's conviction because the prosecution did not disclose that it had granted immunity to a witness upon whose testimony the prosecution was heavily dependent to corroborate its case. With the increasing use of email, digital media, and other forms of technology, scenarios where criminal defendants could determine the impeachment utility of electronic evidence in the custody of the government but are unable to make an offer of proof to the court without an opportunity to first review the ESI are likely to arise more frequently. For example, prior iterations of the same data (e.g., meta data) may carry testimonial evidence subject to impeachment at trial, which arguably may provide standing for a *Giglio* challenge. Currently, criminal procedure does not provide a codified rule addressing an issue of this nature. Instead, federal courts are guided by Rule 16 of the Federal Rules of Criminal Procedure, which does not provide a defendant an automatic right to

81. To obtain a "*Franks* hearing," the defendant must make a "substantial preliminary showing" that a particular portion of the warrant affidavit is false. See *Franks v. Delaware*, 438 U.S. 154, 171 (1978). This is usually accomplished by an "offer of proof" through affidavits or otherwise. *Id.* When the defendant is unable to produce such evidence, he or she should explain the absence of such evidence to the satisfaction of the court. *Id.*

82. *Id.* In some cases involving ESI, defendants are typically limited to accessing e-discovery that the prosecution intends to use in its case-in-chief. FED. R. CRIM. P. 16. The protections provided by traditional omnibus pretrial discovery motions in the criminal justice system do not protect modern-day defendants, as the context surrounding particular forms of ESI have become much more prevalent in building one's defense. The *Franks* hearing protection against a violation of the Warrant Clause is a good example of a law enforcement official applying for a search warrant and neglecting to properly discharge his duty of including all known facts in the affidavit in support of the warrant sought. *See* United States v. Leon, 468 U.S. 897 (1984). As law enforcement communicate among themselves more regularly through electronic mediums such as email, law enforcement officials will likely rely on representations made in such mediums when applying for search warrants, and defendants should be able to obtain those internal communications. This should include identifiable characteristics associated with them (e.g., meta data) that may affect the veracity of a search warrant affidavit, which supports a defendant's ability to secure a *Franks* hearing.

83. Giglio v. United States, 405 U.S. 150 (1972).

84. *Id.* at 154.

ESI. As a result, defendants may find themselves in an uphill battle in order to convince courts that prosecutors do not adequately meet their *Brady* obligation by producing only a mirrored or hard copy version of ESI during discovery rather than files in native format.[85]

B. E-Discovery and the Fifth Amendment

An individual's right against self-incrimination under the Fifth Amendment is well established. The constitutional concerns regarding protection of ESI under the Fifth Amendment are the same as those applicable when a defendant is the subject of a criminal investigation and there is a question as to whether the subject should voluntarily speak to law enforcement officials, knowing that such statements may be used against the individual.[86]

When analyzing the reasoning invoked by the Supreme Court in the cases discussed below, it is conceivable to imagine a scenario where a defendant may not have an act-of-production privilege with respect to a hard copy document, but still may be able to assert the privilege with respect to the work product contained therein (i.e., meta data). This consideration is particularly applicable when it appears evident that the data sought is likely to be used by the government at trial as an adopted admission by the defendant that is testimonial in nature.

The Supreme Court has addressed whether the compelled production of records pursuant to a subpoena *duces tecum* violates the Fifth Amendment privilege against self-incrimination.[87] The legal precedents discussed below may be applied to the ESI sought by the prosecution in criminal proceedings. Therefore, counsel must exercise extreme care on a case-by-case basis, as a client's admissions may be embedded in ESI, and therefore not readily apparent.[88]

Starting as far back as 1886, the Supreme Court held in *Boyd v. U.S.* that the compelled production of invoices violated the Fourth Amendment right against unreasonable searches and seizures, and the Fifth Amendment privilege against compelled self-incrimination.[89] Almost a century later, the Supreme Court decided *Couch v. United States* in the context of the Internal Revenue Service

85. Various governmental agencies are beginning to develop their own internal protocol with respect to the exchange of e-discovery between parties. *See* UNITED STATES SECURITIES AND EXCHANGE COMMISSION, ENFORCEMENT MANUAL § 3.2.6.4.1.2 (discussing guidance and suggestions on how the SEC should maintain files and records produced in electronic formats in investigations). The Enforcement Manual generally discusses how the SEC is approaching the pursuit and exchange of e-discovery.

86. Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (holding voluntariness determined under totality of circumstances test).

87. *See* Fisher v. United States, 425 U.S. 391 (1976)

88. *See* United States v. Nicholas, 594 F. Supp. 2d 1116 (C.D. Cal. 2008) (denying defendant's motion to suppress privileged email and granting government's application to disclose privileged email).

89. Boyd v. United States, 116 U.S. 616 (1886).

summoning a taxpayer's records from her accountant.[90] The defendant taxpayer intervened in a summons enforcement proceeding and claimed a Fifth Amendment privilege.[91] The Court held no Fifth Amendment privilege existed for documentation in the custody of the taxpayer's accountant because the factor of personal compulsion against the accused was lacking; it was the accountant, not the defendant who was ordered to produce the documents to the government. [92]

The Supreme Court faced the identical issue raised in *Couch* in *Fisher v. United States*, except here the third party record holder was the taxpayer's attorney as opposed to the taxpayer's accountant. [93] The Court held that as far as the element of "personal compulsion" was concerned, the attorney in *Fisher* was in the same posture as the accountant in *Couch*.[94] However, the Court held that the attorney-client privilege may still protect records in the hands of the attorney.[95] It is in *Fisher* that the Supreme Court incorporated the "act of production" doctrine into Fifth Amendment constitutional jurisprudence. The Court held that the physical production of the documents alone may contain an element of "compulsion" and may be "incriminating" irrespective of the content of the documents. In *Fisher*, the Court concluded that the production of documents would not be incriminating because the authentication of the documents was a "foregone conclusion."[96]

In *United States v. Doe*,[97] the grand jury conducted "an investigation of corruption in the awarding of county and municipal contracts."[98] The government served a subpoena on the target, the owner of several sole proprietorships, seeking virtually all of his business records. The Supreme Court first observed that it reserved the issue in *Fisher* of whether the tax records would have been protected in the taxpayer's hands, as the Fifth Amendment only protects "the person asserting the privilege from compelled self-incrimination."[99] The Court reasoned that, "where the preparation of business records is voluntary, no compulsion is present."[100] The Supreme Court further held that, "[a]lthough the contents of a document may not be privileged, the act of producing the document may be."[101] As the Supreme Court stated in *Fisher*: "Compliance with the subpoena tactically concedes the existence of the papers demanded and their possession or control by the

90. Couch v. United States, 409 U.S. 322 (1973).
91. *Id.*
92. *Id.* at 328-29.
93. Fisher v. United States, 425 U.S. 391, 393 (1976).
94. *Id.* at 398.
95. *Id.* at 404-05.
96. *Id.* at 412-13.
97. 465 U.S. 605 (1984).
98. *Id.* at 606.
99. *Id.* at 610.
100. *Id.*
101. United States v. Doe, 465 U.S. 605, 612 (1984).

taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena."[102] Additionally, the Court considered how the act of production would affect the taxpayer, and concluded that the act of production would have limited testimonial value and would not operate to incriminate the taxpayer.[103]

Unlike *Fisher*, the *Doe* Court explicitly found that the act of producing the documents would result in testimonial self-incrimination.[104] The "act of production" doctrine, first addressed in *Fisher* and expanded upon in *Doe*, calls into question the remaining viability of the holding in *Bellis v. United States*[105] (i.e., that a representative of a corporation has no Fifth Amendment privilege against providing corporate documents).[106]

The Second, Third, Fourth and D.C. Circuits have held that the "act of production" doctrine applies to corporate representatives.[107] The First, Fifth, Sixth, Eighth, Ninth and Tenth Circuits have rejected the application of the act of production doctrine as to corporate representatives.[108] Notably, the Eleventh Circuit has ruled both ways regarding whether the production of documents can be considered compelled self-incriminating testimony.[109]

A further dilemma ESI has created for defendants seeking Fifth Amendment protection is presented in the context of cooperating with the prosecution during an investigation (e.g., grand jury subpoena, regulatory proceeding, etc.) by forensically reviewing one's computer hardware. In many instances, the government will be reluctant to stipulate on "search terms" for ESI responsive to their requests, which places the subject of the investigation in a Catch-22 between appearing adversarial and suffering the consequences, or reaping the potential benefits of cooperation and fearing non-production of ESI that was not done with the intent to obstruct an investigation. In other words, some

102. Fisher v. United States, 425 U.S. 391, 410 (1976).

103. *Id.* at 410-11.

104. United States v. Doe, 465 U.S. 605, 613 (1984).

105. 417 U.S. 85 (1974).

106. *See id.* (holding representative of partnership has no Fifth Amendment privilege against providing partnership documents).

107. *See In re* Sealed Case, 832 F.2d 1260, 1279 (D.C. Cir. 1987); United States v. Lang, 792 F.2d 1235, 1240-41 (4th Cir. 1986); United States v. Sancetta, 788 F.2d 67, 74 (2d Cir. 1986); *In re* Two Grand Jury Subpoenae Duces Tecum, 769 F.2d 52, 57-59 (2d Cir. 1985); *In re* Grand Jury Matter, 768 F.2d 525, 529 (3d Cir. 1985) (en banc).

108. *See In re* Grand Jury Proceedings, 814 F.2d 190 (5th Cir. 1987), *judgment aff'd*, 487 U.S. 99, 108; *In re* Grand Jury Subpoena, 784 F.2d 857, 861 (8th Cir. 1986), *cert. granted*, 479 U.S. 811, *cert. dismissed*, 479 U.S. 1048; *In re* Grand Jury Proceedings, 771 F.2d 143, 148 (6th Cir. 1985); *In re* Grand Jury Subpoena, 767 F.2d 1130, 1131 (5th Cir. 1985); *In re* Grand Jury Proceedings United States, 626 F.2d 1051, 1053 (1st Cir. 1980); *see also* United States v. Malis, 737 F.2d 1511, 1512 (9th Cir. 1984); *In re* Grand Jury Proceedings, 727 F.2d 941, 945 (10th Cir. 1984).

109. *Compare In re* Grand Jury Subpoena Duces Tecum (Ackerman), 795 F.2d 904 (11th Cir. 1986) (a corporate representative has no act of production privilege), *with In re* Grand Jury No. 86-3 (Will Roberts Corp.), 816 F.2d 569 (11th Cir. 1987) (sole shareholder corporate representative may have an act of production privilege).

defendants fear *entrapment* and are suspicious of the government's intention in not reciprocally collaborating on search terminology—particularly in prosecutions involving high volumes of data.[110] Twenty-first century criminal targets, particularly businesses or individuals operating among many other parties that routinely communicate by electronic means, are likely seeking a sense of assurance that being a target of an investigation does not preclude one from being able to meet the government's expectation of cooperation when it comes to seeking responsive ESI in good faith.

As discussed above, the federal courts are split as to whether individuals should be compelled to produce documentation they have created for personal use. The greatest challenge for defendants is that the Supreme Court has found that custodians of business records do not have standing to assert the Fifth Amendment privilege.[111] This is pertinent to the production of ESI when the defendant personally created information that resides within the custody of a third party (e.g., internet service provider or web client email services, etc.).

C. Criminal E-discovery Impacts the Sixth Amendment Right to Counsel

As eloquently stated in the opinion of *United States v. Stein*,[112] "the Sixth Amendment right to counsel typically attaches at the initiation of adversarial proceedings—at an arraignment, indictment, preliminary hearing, and so on . . . [b]ut the analysis can not end there."[113] Once the Sixth Amendment right to counsel attaches, the government may not deliberately elicit an incriminating response from a defendant in a conspicuous fashion by uniformed police officers or by surreptitiously using informants or undercover law enforcement personnel.[114] This legal principle, referred to as the *Messiah* doctrine, applies irrespective of whether the target of a criminal investigation is in custody or being subjected to interrogation.[115] It is important to note that no overriding influences, either implied or otherwise inferred by the circumstances, have to

---

110. FED. R. CRIM. P. 12.3(a); *see* United States v. Giffen, 473 F.3d 30, 41 (2d Cir.2006). In *Giffen*, the court stated:

> The defense of entrapment by estoppel can be established without the defendant having received actual authorization. It depends on the proposition that the government is barred from prosecuting a person for his criminal conduct when the government, by its own actions, induced him to do those acts and led him to rely reasonably on his belief that his actions would be lawful by reason of the government's seeming authorization.

473 F.3d at 41.

111. Braswell v. United States, 487 U.S. 99 (1988).

112. 435 F. Supp. 2d 330 (2006).

113. *Id.*

114. Messiah v. United States, 377 U.S. 201 (1964).

115. *Id.* Defendants can raise *Messiah* issues in the context of governmental investigations surrounding the analysis of ESI, especially where the government is seeking to investigate a target on matters that may be collateral to the present case but inextricably tied to it by ESI (e.g., email communications). *See id.*

be present for the *Messiah* doctrine to be triggered.[116]

Criminal defendants and their counsel should recognize that the Sixth Amendment applies to specific offenses, which permits the government to seek discovery of ESI in one matter and then use that information to interrogate the defendant on another matter.[117] The issue of criminal investigators repeatedly visiting the same "forensic well" to acquire information that may be otherwise protected pursuant to *Messiah* should be addressed by criminal defendants and their counsel when determining whether to challenge compound forensic efforts by governmental agencies.

1. Procedural Implications the Current State of E-Discovery Has On Sixth Amendment Protection

The reality is that electronic evidence is no longer simply "evidence that is electronic" regardless whether the legal matter is civil or criminal.[118] ESI is an independent category of evidence, requiring special procedures for handling what the traditional rules of criminal procedure do not properly address.[119] Rule 16(a)(1)(E), the current pre-trial discovery rule in federal criminal proceedings, states as follows:

> (E) *Documents and Objects.* Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:
>
> (I) the item is material to preparing the defense;
>
> (ii) the government intends to use the item in its case-in-chief at trial; or
>
> (iii) the item was obtained from or belongs to the defendant.[120]

The rule identifies the term "data,"[121] but it falls short in defining electronic discovery with any further clarity. For instance, the language of Rule 16 does not explain the manner or mechanisms through which ESI is to be exchanged between the prosecution and defense, and the rule is devoid of direction on how

116. *See* Welsh S. White, *Police Trickery in Inducing Confessions*, 127 U. PA. L. REV. 581, 602-04 (1979) (discussing scope of *Messiah* decision).

117. *See* United States v. Stierhoff, 2007 WL 763984 (D.R.I. Mar. 13, 2007) (holding government exceeded scope of consent searching defendant's computer). In *Stierhoff*, the arrest was for stalking and the information encountered was evidence of an "offshore" file opened by investigator without warrant. *Id.*

118. *See* 8A WRIGHT & MILLER, FED. PRAC. & PROC. CIV.2D § 2218.

119. See BARBARA J. ROTHSTEIN, RONALD J. HEDGES, & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES (2007), *available at* http://www.fjc.gov/public /pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

120. FED. R. CRIM. P. 16(a)(1)(E).

121. FED. R. CRIM. P. 16.

ESI is to be made accessible for review and analysis for the criminal defendant.[122]

Further complicating the matter is that the government is entitled to build its case and develop work product, as it is the party burdened with proving its case beyond a reasonable doubt,[123] which in the digital age inevitably encompasses ESI assuming a testimonial function (e.g., meta data contained in business records). While the prosecution should not be subjected to unnecessary and "vexatious fishing expeditions" by defendants, and should be required to produce *Brady* material and discovery under the Jencks Act[124] and other safeguards, defendants have the Sixth Amendment right to confront witnesses against them by timely moving the court to compel the government to produce statements that may be useful for impeachment of the prosecution's witnesses.[125] For instance, if the government neglected to produce pertinent ESI that contained testimonial evidence (e.g., email, voicemail, SMS text messages, internet postings, etc.), which the prosecution intended to use against the defendant at trial, it would be reasonable for a defendant to assert that such electronic evidence may be testimonial in nature, thereby impacting the defendant's confrontational rights and ability to assert a viable Jenks Act violation.

Rule 16 confines e-discovery to what the court itself believes is "material" to the defense in reliance upon the prosecution's representations of what it intends to use in its case-in-chief.[126] Some information subject to production under the Jencks Act may also be subject to disclosure as *Brady* material, thus requiring production of ESI prior to the framework set forth by the Jencks Act.

Irrespective of particular acts, a defendant's ability to access ESI in criminal prosecutions today is an unmitigated mess. The construct of proportionality to determine cost shifting and reasonableness, upon which a great deal of civil litigation rests, falls short because of various criminal acts and the Fourth,[127] Fifth[128] and Sixth[129] Amendments. At a minimum, the Federal Rules of Criminal Procedure must be amended to provide a procedural mechanism that reconciles what the court believes is "material" to a defense in terms of access to ESI with what is ultimately required by the previously mentioned acts, or others, and the Fourth,[130] Fifth[131] and Sixth[132] Amendments.

---

122. *Id.*

123. *See, e.g.*, Taylor v. Kentucky, 436 U.S. 478 (1978); *In re* Winship, 397 U.S. 358 (1970); People v. Antommarchi, 80 N.Y.2d 247, 252-253 (1992).

124. 18 U.S.C. § 3500 (2006).

125. United States v. Carter, 613 F.2d 256 (10th Cir. 1980).

126. FED. R. CRIM. P. 16 (a)(1)(E)(1).

127. U.S. CONST. amend. IV.

128. U.S. CONST. amend. V.

129. U.S. CONST. amend. VI.

130. U.S. CONST. amend. IV.

131. U.S. CONST. amend. V.

132. U.S. CONST. amend. VI.

VI. THE NECESSITY FOR A "BALANCING TEST" TO GOVERN E-DISCOVERY IN CRIMINAL PROCEEDINGS

Prosecutorial discretion requires the government to produce only what it believes is central to its case-in-chief, or what is set out in the *Brady* material.[133] In the digital arena, this grants the prosecutor a substantial advantage over defendants because the current rules permit the government the latitude to produce emails out of context.[134] For example, in a criminal trial the prosecution may seize and forensically search and discover an email string and produce only the incriminating email from the email thread. In essence, the defendants who lack the necessary fiscal resources have no ability to perform the forensic analysis necessary to find the string and present the context of the email communication. Of course, improper handling of ESI by the prosecutor could adversely affect the defendant, and foster a loss of trust by the public in the office of the prosecutor.

Currently, an indigent defendant may not be in a position to successfully move the court for funds necessary for electronic discovery. One may argue this is because a court will grant such a motion under existing jurisprudence only if a defendant can demonstrate the need for the court's intervention in order to force the government to produce ESI, which may be similar to the analysis applied to an order for a bill of particulars.[135] Today, a defendant has little ability to meet this burden in the electronic space because of the monetary requirement to discover such evidence to produce to a court.[136] Consequently, state and federal courts should, where appropriate, modify the current requirements a defendant must meet when electronic information is pivotal to the prosecution's case.

A. Reasonable Indicia of Review to Determine Cost Shifting for Discovery

One possible modification to the rule would have the court apply a reasonable indicia requirement to be shown by a criminal defendant in order to trigger the state's obligation to cover the defendant's cost (using a national pricing matrix to calculate cost). The matrix would incorporate a "government" rate and a "private" rate to which the government commits when it requests a grand jury target or defendant to retain a service that the government benefits from during an investigation of a case. Moreover, if a defendant is convicted, the prosecution may make a motion to the court seeking restitution from the defendant for the fees incurred with respect to the digital

133. *See* Brady v. Maryland, 373 U.S. 83 (1963) (holding suppressing evidence favorable to accused violates due process where material to guilt or punishment).

134. *See supra* Section IV (describing criminal electronic discovery tactics).

135. FED. R. CRIM. P. 7(f).

136. *See* John Bace, *Cost of E-Discovery Threatens to Skew Justice System*, GARTNER RAS CORE RESEARCH NOTE G00148170 (April 2007).

evidence. Here, a defendant can assert an affirmative defense to the court, that the evidence was critical to the defense.

B. Streamline Exchange of ESI in Criminal Proceedings

Inasmuch as ESI (e.g., cell phone evidence, wiretaps, cybercrime, etc.) is now central to many criminal proceedings, there must be a mechanism in place whereby the exchange of such information is streamlined to the fullest extent possible. One solution may be for the courts to promulgate a legal interpretation of Rule 16 that is instructive for the parties to future cases, in much the same manner in which *Zubulake*[137] influenced cost-shifting protocol for civil litigants. Importantly, current defendants are in dire need of pre-trial discovery tools that incorporate a "reasonableness" standard into complex criminal discovery matters,[138] as opposed to the traditional rules that make novel discovery arguments (such as the production of ESI and the costs associated) difficult for defendants to advance. Moreover, the government should not have carte blanche when it comes to driving up e-discovery costs during its initial investigation of a matter as leverage for compelling cooperation.

Therefore, similar to the spirit of a *Franks* hearing, a solution may be for the court to conduct, upon motion of a defendant, a hearing to determine whether the prosecution's request for ESI is reasonable, the ESI is unavailable from alternative less restrictive means, the request is made in good-faith, and the request is constitutional. In these situations, the court should use the government rate from the aforementioned rate matrix and apply the other rate accordingly.

VII. PROTECTING AND ACCESSING ESI IS MORE CHALLENGING THAN IT SHOULD BE FOR 21ST CENTURY CRIMINAL DEFENDANTS

The rapidly growing role of ESI in criminal prosecutions requires that counsel be conversant with this type of evidence in criminal proceedings. Otherwise, a criminal defendant may be deprived of access to effective assistance of counsel. In civil proceedings, ESI is a cost issue. In criminal proceedings, failure to obtain ESI may result in the client's loss of liberty. Despite the burden and costs of electronic discovery, the courts and parties cannot escape the fact that technology governs the way members of society communicate. The criminal justice system must acclimate itself to the realities of the role of ESI in proceedings in order to ensure that trials are fully and fairly presented in accordance with all protections afforded to defendants under the law.

---

137. *See* Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

138. *See, e.g.*, Hon. Maureen Duffy-Lewis and Daniel B. Garrie, *Dancing in the Rain: Who Is Your Partner in the Corporate Boardroom?*, 25 J. MARSHALL J. COMPUTER & INFO. L. 267, 271 (2008).

The government can essentially issue grand jury or administrative subpoenas for ESI in addition to other statutory mechanisms (e.g., ECPA), while a criminal defendant must seek the court's endorsement for pretrial third-party discovery.[139] The Supreme Court has stated that the government should be permitted to fetter out information in order to protect the people, and unless a valid legal privilege is found, "[n]o pledge of privacy nor oath of secrecy can avail against demand for the truth in a court of justice."[140] The reality faced by the legal system in general is that technology is playing a much greater role in the interpretation, use, and admissibility of evidence—in particular, electronic evidence—in nearly all complex criminal cases. Although it is the prosecution's burden to prove its case, the defendant should not be forced to comply with historical Rule 16 precedent, rendered when access to ESI was not central to the defense, while at the same time subjected to the modernization of prosecution.

It is noteworthy that in civil cases either party can issue Rule 45 subpoenas pursuant to the Federal Rules of Civil Procedure, which may only be challenged by the recipient. Alternatively, in criminal proceedings, a defendant must pursue non-party discovery via Rule 17 of the Federal Rules of Criminal Procedure, which states, in part, the following:

> (c) Producing Documents and Objects.
>
> *(1) In General*. A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.[141]

A defendant's ability to access ESI in the custody and control of a third-party witness may likely be essential to establish certain defenses; however, in order to enjoy the authority of Rule 17, a target will likely have to be subjected to an ongoing prosecution. In contrast, Rule 45 of the Federal Rules of Civil Procedure is a fact-collecting pretrial discovery tool that can be utilized upon the filing of a complaint and typically does not require judicial endorsement. This is a useful tool in the modern world of electronic communications and data storage, which is why Rule 45 has been amended over time to provide a party reasonable access to ESI that supports a claim or defense and is not unduly burdensome on the producing non-party.[142]

---

139. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

140. Branzburg v. Hayes, 408 U.S. 665 (1972) (quoting 8 J. WIGMORE, EVIDENCE § 2286, at 528 (McNaughton rev. 1961)).

141. FED. R. CRIM. P. 17.

142. *See generally* FED. R. CIV. P. 45 advisory committee note.

Contrary to civil litigants, criminal defendants are more substantially confined with respect to third-party discovery, and are at the mercy of judicial discretion concerning discovery from the government as provided by Rule 16 as well as discovery from third parties as provided by Rule 17. Courts must begin to more uniformly recognize the role ESI assumes in particular criminal matters and a defendant's ability to gain access to it from non-parties, in addition to the prosecution. This would ensure that defendants can fully build all constitutional and non-constitutional legal defenses, as well as a basis to assert procedural mechanisms, such as a motion to suppress.[143]

VIII. CONCLUSION

The criminal justice system needs a means to balance a defendant's right to build a defense involving ESI with the government's resources for marshalling ESI in support of its case-in-chief. An argument can be made that this can be accomplished through the adoption of a rule that provides the defense with an opportunity to move the court to hear criminal discovery matters surrounding ESI. The judicial system must give special consideration to the production of ESI sought from and by a defendant, beyond the consideration given to requests for production of non-ESI, in order to ensure that constitutional rights are not compromised during e-discovery.

143. *See* FED. R. CRIM. P. 12, 41.