San Diego Law Review

Volume 47 | Issue 2 Article 7

5-1-2010

"Criminal Cases Gone Paperless": Hanging With the Wrong Crowd

Daniel B. Garrie

Maureen Duffy-Lewis

Daniel K. Gelb

"Criminal Cases Gone Paperless": Hanging with the Wrong Crowd

DANIEL B. GARRIE, ESQ.,*
THE HONORABLE MAUREEN DUFFY-LEWIS,**
DANIEL K. GELB, ESQ.***

---

* Daniel Garrie is a neutral for resolving electronic discovery and related electronic matters faced by warring companies and governmental entities for Alternative Resolution Centers. Mr. Garrie serves by court appointment as Special Master. He is also a managing partner at EMI Capital LLC, a world-class Venture Development Services Company. He was previously a principal and director of electronic discovery at the leading global consulting firm, CRA International, where he specialized in the synchronization of policies with information technologies and related best practices to ensure legal compliance for enterprises worldwide. Prior to joining CRA, Mr. Garrie was a vice president of LegalTech Group, where he provided subject matter expertise and project management in engagements pertaining to electronic discovery, vendor selection, litigation readiness, digital privacy, and digital information risk management. Mr. Garrie has published more than forty articles and books on electronic discovery, software, intellectual property, compliance, technology, legal, telecommunications, United States and European Union privacy policies, and a range of other electronic law issues.

** The Honorable Maureen Duffy-Lewis, a Fulbright Scholar, is a judge for the Superior Court in Los Angeles, California, where she has handled both serious criminal and complex litigation. She has served on many court committees, including the Executive and Alternate Dispute Resolution Committees of the Los Angeles County Superior Court. Additionally, she was in private practice, emphasizing criminal and civil litigation, and has served as a Los Angeles County Deputy District Attorney handling major crimes. Judge Duffy-Lewis has coauthored many legal articles and serves on the Board of Advisors for Pepperdine University in Malibu, California, and on the Board of Trustees of Western University of Health Sciences in Pomona, California. She currently presides in Department 38 at the Stanley Mosk Civil Courthouse in Los Angeles, California.

*** Daniel K. Gelb, Esquire is a partner at Gelb & Gelb LLP in Boston, Massachusetts, where he handles white collar and general criminal defense matters in state and federal court, complex civil litigation, and arbitration and regulatory proceedings. Prior to joining Gelb & Gelb LLP, Mr. Gelb was an Assistant District Attorney in Massachusetts. Mr. Gelb is a member of the Sedona Conference® Working Group on

Long gone or fading fast are the days when only bookmakers, ponzi schemers, predatory mortgage brokers, and insider traders, just to name a few, relied on paperwork to carry on their daily business. The paperless world has come full circle. Not even "respectable" lawbreakers can get along without some electronic communication device or computer.

Much to the chagrin of criminal lawyers who often lamented their clients opening their big mouths to the cops, the criminal case has gone paperless. Criminal lawyers now will be heard advising their clients not to put anything in e-mail or on the Internet unless they want the cops to read it.

Additionally, the landscape of criminal defendants is changing rapidly. The CEOs of the large mortgage companies or financial firms do not see themselves hanging with common criminals; they make their deals at the club or on the golf course. The problem is that the business following such meetings is memorialized by electronic communication, and unknown to them, these business practices have caught the attention of the government. Welcome to twenty-first century communications.

Modern-day communications, through e-mail, the web, instant messaging, electronic faxing, and digital voice mail, expand the nature and location of "relevant evidence" as well as the obligations to obtain, preserve, produce, and manage this evidence.[1] There exists a rapidly emerging need for courts to uniformly recognize the increasing necessity for an accused to access electronically stored information (ESI) in order to effectively build a defense in modern-day criminal prosecutions. Furthermore, the context in which ESI was forensically ascertained may be as important to a defendant as the substantive information recovered.

Electronic Document Retention and Production, and an Advisory Board Member for the Bureau of National Affairs, Inc.'s *White Collar Crime Report*. He is also a member of the National Association of Criminal Defense Lawyers' (NACDL) White Collar Crime Committee, on which he is the Massachusetts District Chair for the NACDL's Electronic Discovery Task Force, and is the Massachusetts State Chair for NACDL's Membership Committee. Mr. Gelb is a member of the Massachusetts Bar Association's Implementation of Technology Task Force, the Massachusetts Academy of Trial Attorneys, the Massachusetts Association of Criminal Defense Lawyers, and the Criminal Law Section of the Boston Bar Association. Mr. Gelb is a Louis D. Brandeis Fellow of the Massachusetts Bar Foundation and has been named a Rising Star in the 2009 edition of *New England Super Lawyers.* Mr. Gelb is a frequent author and lecturer on electronic evidence and discovery, and civil and criminal trial practice and procedure, and is a coauthor of the book *Massachusetts E-Discovery and Evidence: Preservation Through Trial* published by Massachusetts Continuing Legal Education, Inc. The opinions and analyses contained herein are that of the author's only and should not be interpreted as legal advice. In addition, the authors would like to thank Richard L. Gillespie for his ongoing assistance in the production of this Article.

1. *See* FED. R. CIV. P. 34(a); *see also infra* notes 28–32 and accompanying text.

This Article explores issues concerning electronic discovery (e-discovery), its association with ESI, and how it impacts criminal litigation.

Free e-mail accounts, such as Yahoo!, Gmail, and Hotmail and a competitive mobile communications market offering an affordable unification of services, such as e-mail, voice plans, and data on a single handheld device, expand the universe of evidence at issue—irrespective of whether the crime being prosecuted is "corporate" or "street" in nature.[2] The landscape of criminal defendants is also changing rapidly.

ESI evidence can significantly impact the outcome of a client's civil or criminal case. However, e-discovery assumes a unique, critical role in criminal proceedings. Unlike hard copy documents and tangible evidence—guns, pictures, clothing, et cetera—ESI may contain exculpatory evidence that may not be readily apparent to the prosecution who maintains custody and control over the evidence. Additionally, the prosecution may be improperly in possession of ESI that should be the subject of a motion to suppress, but the evidence may exculpate a defendant or affect the strength of the prosecution's case.[3] Due to its dynamic nature, ESI has the potential to develop into *Brady* material.[4] Because the government's obligations under *Brady* are not rooted in any particular constitutional right to discovery but rather in the due process protections that defendants are afforded in criminal proceedings, criminal lawyers must be on alert.[5]

The greatest challenge may be ascertaining and obtaining electronic evidence in the possession of the prosecution. The defense must successfully convince the court that without "full and appropriate" pretrial disclosure and exchange of ESI, the defendant lacks the ability to mount a full and fair defense.[6] Due process, as a general proposition, adapts to facts as they are presented in specific circumstances, and it is a

2. The term *corporate* is historically used in reference to white collar crimes. The term *street* is often used in reference to blue collar crimes.

3. *See infra* note 40 and accompanying text.

4. *Brady* material includes evidence in the custody and control of the prosecution that would either exculpate the accused or undermine the strength of the prosecution's case. Brady v. Maryland, 373 U.S. 83, 87–88 (1963) (holding that suppression by the prosecution of evidence requested by the defendant that exculpates a defendant is a violation of due process).

5. *See id.* at 90–91; *see also* 2 CHARLES ALAN WRIGHT & PETER J. HENNING, FEDERAL PRACTICE AND PROCEDURE § 256, at 157–58 (2009) (citing United States v. Higgs, 713 F.2d 39, 42 (3d Cir. 1983)).

6. *See* 2 WRIGHT & HENNING, *supra* note 5, § 256, at 155–58.

progressive principle that has been applied to mediums containing ESI, such as search warrants of computers and testimonial evidence residing on audiotapes.[7] A defendant's rights must be expanded to accommodate contemporary applications.[8] Criminal ESI discoverability should be governed by the same due process analysis that courts have recognized for other areas of discovery.[9] The obligation to make relevant evidence available to the accused or to suppress its use when improperly obtained should be aggressively protected. Criminal defendants require reasonable access to ESI evidence so that their counsel may capably advocate for the protection of their Fourth,[10] Fifth,[11] and Sixth Amendment rights.[12]

ESI evidence gives rise to financial concerns: the vast majority of criminal defendants are indigent[13] and thus without funds to pay for costly e-discovery. The counsel for such defendants could look to the state and judicial systems for required funding, but the expense and burdensomeness of e-discovery should be balanced against the government's needs and the defendant's rights.[14] Lawyers should be prepared to explain and judges should be aware of the problems and expenses potentially associated with ESI, so they do not "accidentally"

---

7. *See, e.g.*, United States v. Laine, 270 F.3d 71, 76 (1st Cir. 2001) (holding that a defendant's consent to forensically search a computer suspected of containing child pornography did not violate the Fourth Amendment's protection against unreasonable searches and seizures).

8. *See* Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J. dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967). In his dissenting opinion in *Olmstead*, Justice Brandeis observed:

> 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.

Id. (citations omitted).

9. *See Higgs*, 713 F.2d at 42.

10. U.S. CONST. amend. IV; *see also* FED. R. CRIM. P. 41(e) (stating that a magistrate shall issue a warrant identifying the property to be seized and naming or describing the person or place to be searched).

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

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

13. *See* CAROLINE WOLF HARLOW, BUREAU OF JUSTICE STATISTICS, DEFENSE COUNSEL IN CRIMINAL CASES 1 (2000); STEVEN K. SMITH & CAROL J. DEFRANCES, BUREAU OF JUSTICE STATISTICS, INDIGENT DEFENSE 4 (1996).

14. *See* HARLOW, *supra* note 13.

issue a general discovery order that could be overly broad, making discovery burdensome and costly.[15]

Over the past decade, courts have attempted to keep e-discovery in pace with technological advances. In *McPeek v. Ashcroft*, the court used a "marginal utility" approach to craft an order for discovery of e-mails that might have contained relevant information and required the producing party to pay the costs but also to keep an accounting.[16] The parties and the court could then determine if the information gathered in light of the costs justified further discovery.[17]

In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, the party charged with production of e-mail stored on backup disks requested that the court to issue a protective order precluding such discovery due to costs.[18] The court found no justification for a protective order but did create and apply a protocol for cost shifting.[19]

Rowe was further addressed in *Zubulake v. UBS Warburg LLC* when the plaintiff requested e-mails from defendant's archival media, and the defendant, citing *Rowe*, claimed undue burden and expense and urged the court to shift the cost of production to the plaintiff.[20] The court refrained from applying *Rowe* in a strict manner and noted that *Rowe* might result in a disproportionate shifting of costs away from large defendants.[21] The court ultimately issued a modified approach by ordering a partial discovery of the e-mails—the plaintiff selected the e-

15. *See* Daniel B. Garrie & Maureen Duffy-Lewis, *E-Discovery: Federal Rules Versus California Rules—The Devil Is in the Details*, 63 CONSUMER FIN. L.Q. REP. 218 (2009).

16. McPeek v. Ashcroft, 202 F.R.D. 31, 32–35 (D.D.C. 2001).

17. *Id.* at 34–35.

18. Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 423 (S.D.N.Y. 2002).

19. *Id.* at 433.

20. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 317 (S.D.N.Y. 2003).

21. *Id.* at 317. In addition, the court stated the test to be used:

> [I]n conducting the cost-shifting analysis, the following factors should be considered, weighted more-or-less in the following order: (1) [t]he extent to which the request is specifically tailored to discover relevant information; (2) [t]he availability of such information from other sources; (3) [t]he total cost of production, compared to the amount in controversy; (4) [t]he total cost of production, compared to the resources available to each party; (5) [t]he relative ability of each party to control costs and its incentive to do so; (6) [t]he importance of the issues at stake in the litigation; and (7) [t]he relative benefits to the parties of obtaining the information.

Id. at 324.

mails and the partial discovery was at the defendant's expense.[22] Then the parties were instructed to evaluate the search results to determine if further searching and expense was warranted.[23]

Coordinating policies and procedures with technology is important today, not only for prosecutorial agencies but also for corporate America. In the recent past, corporations have been ordered to preserve and produce, sometimes at considerable expense, computerized information, including e-mail messages, support systems, software, voice mail systems, computer storage media, backup tapes, and telephone records.[24] On December 1, 2006, the federal courts responded to the growing demands and complexities of e-discovery by amending Federal Rules of Civil Procedure (FRCP) 16, 26, 33, 34, 37, and 45 to address such discovery.[25] Many states, including California, have begun to do the same, but as expected, the lack of resources still leaves criminal defendants and corporate businesses in a difficult predicament.[26]

The amended FRCP Rule 34(a) defines ESI as "other data or data compilations . . . stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[27] Courts have applied the amended rules by requiring parties to a case, whether corporate or individual, to preserve,[28] identify,[29] disclose,[30] and produce,[31] on pain of

---

22. *Id.*

23. *Id.*

24. *See* FED. R. CIV. P. 34; Peter Brown, *Developing Corporate Internet, Intranet and E-Mail Policies*, *in* SECOND ANNUAL INTERNET LAW INSTITUTE 1998, at 364 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 520, 1998), WL 520 PLI/Pat 347 (citing *In re* Brand Name Prescription Drugs Antitrust Litig., Nos. 94 C 897, MDL 997, 1995 WL 360526 (N.D. Ill. June 15, 1995)).

25. FED. R. CIV. P. 16, 26, 33, 34, 37, 45; *see* Garrie & Duffy-Lewis, *supra* note 15.

26. *See* Posting by G. Krabacher to eDiscoTECH Blog, http://www.bricker.com/legal services/practice/litigation/ediscotech/eblog/details.aspx?id=217#page=1 (July 20, 2009).

27. FED. R. CIV. P. 34(a).

28. *See, e.g.*, Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 140–42 (S.D.N.Y. 2009) (imposing attorneys' fees, costs, and adverse inference sanctions for defendants' failure to preserve usage data and digital music files from its servers); Fox v. Riverdeep, Inc., No. 07-13622, 2008 WL 5244297, at *7 (E.D. Mich. Dec. 16, 2008) (noting that if defendants failed to preserve evidence, including e-mails, once they received cease and desist letter, an instruction to the jury that it could presume missing documents were unfavorable to defendants was appropriate).

29. *See, e.g.*, Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 637 (D. Colo. 2007) (imposing monetary sanctions and requiring defendants to bear the cost of a second review of its computer files and website for relevant ESI).

30. *See, e.g.*, Amersham Biosciences Corp. v. PerkinElmer, Inc., No. 03-4901, 2007 WL 329290, at *7 (D.N.J. Jan. 31, 2007).

31. *See, e.g.*, *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 183–202 (S.D.N.Y. 2007) (imposing adverse inference spoliation sanction in securities fraud action because

monetary and other sanctions, relevant information residing in any electronic device.[32] What happens when relevant evidence suffers digital spoliation?

FRCP Rule 37(e) provides a limited safe harbor from sanctions when the loss of ESI occurs as a result of the "routine, good-faith operation of an electronic information system."[33] Litigants must demonstrate that they took reasonable steps to preserve in "good faith" evidence they knew or should have known to be relevant to reasonably anticipated or commenced litigation.[34] Therefore, a party cannot evade the safe harbor provision by setting ESI to self-destruct.[35] The amended FRCP addresses digital spoliation by recognizing that it can occur in various ways and will result in varying penalties depending on the facts and legal context in which the claim arises.[36] What recourse is available to a defendant whose rights are violated by the prosecution's conduct contravening the safe harbor rules? A criminal defendant's liberty is at stake; spoliation of evidence could result in a dismissal of the criminal case.[37]

Criminal lawyers beware: the Federal Rules of Criminal Procedure do not afford criminal defendants an established right to access ESI beyond the scope of rules 16[38] or 17.[39] The accused should 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, or control of the prosecution as third parties.[40]

---

defendant corporation had the practical ability to obtain documents it needed from a nonparty corporation and defendant corporation's failure to preserve e-mails relevant to plaintiffs' claims was grossly negligent).

32. *See id.* at 201.

33. FED. R. CIV. P. 37(e).

34. *Id.*

35. *See id.*

36. *See* Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., No. 502003 CA005045XXOCAI, 2005 WL 679071, at *6 (Fla. Cir. Ct. Mar. 1, 2005), *rev'd on other grounds*, 955 So. 2d 1124 (Fla. Dist. Ct. App. 2007). A general definition of spoliation is "the act of injuring esp[ecially] beyond reclaim." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1206 (11th ed. 2003).

37. *See, e.g.*, State v. Ferguson, 2 S.W.3d 912, 917 (Tenn. 1999) (noting in dicta that a trial court could dismiss a case if the missing evidence would result in a fundamentally unfair trial).

38. FED. R. CRIM. P. 16 is applicable for evidence in the custody of the government.

39. FED. R. CRIM. P. 17 is applicable for evidence in the possession of third parties.

40. *See* Brady v. Maryland, 373 U.S. 83, 87–88 (1963) (holding that suppression by the prosecution of evidence requested by the defendant that exculpates a defendant is a violation of due process).

Generally, a criminal defendant is entitled to a rather limited discovery, with no general right to obtain the statements of the government's witnesses before they have testified.[41] Additionally, it is not unreasonable to assume this principle would apply to items such as e-mail, text messages, and other forms of ESI. This does not seem just when in civil litigation, 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."[42]

A critical concern is the imbalance of discovery rights between civil and criminal law. Criminal defendants are potentially at risk of being denied access to exculpatory, mitigating, or impeachment evidence that may be legitimate *Brady* material.[43] The often overwhelming and daunting task of mounting a full and complete defense to a prosecutor's charges can result in a defendant pleading to criminal charges before e-discovery is completed. Moreover, criminal defendants' access to ESI varies from court to court on both the state and federal levels because of the lack of uniform rules governing e-discovery.[44]

Many cases pursued by prosecutors are investigated in tandem with other governmental agencies—within the parameters of laws governing parallel proceedings—including Congress, which may be investigating potential civil or regulatory violations of federal laws.[45] Absent common procedures among forums for the handling of ESI, defendants face a risk when they produce ESI to the government in noncriminal

41. *See* Degen v. United States, 517 U.S. 820, 825 (1996), *superseded by statute*, Civil Asset Forfeiture Reform Act of 2000, 28 U.S.C. 2466(a) (2006).

42. *See, e.g.*, *id.* at 825–26 (comparing FED. R. CRIM. P. 16(a)(2) and 26.2 with FED. R. CIV. P. 26(b)(1)). For exceptions regarding witness statements not subject to disclosure under FED. R. CRIM. P. 16(a)(2), see 18 U.S.C. § 3500 (2006). *See generally* FED. R. CRIM. P. 16 (regarding witness statements made when an organizational defendant is involved).

43. *See generally Brady*, 373 U.S. at 87–88 (categorizing *Brady* material as exculpatory evidence either absolving—or at the very least mitigating—a defendant's criminal liability or in the alternative, as evidence that tends to undercut the government's case, such as impeachment evidence).

44. For example, access to ESI evidence is likely to vary 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, 42 U.S.C. § 16901. 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 (GPS) technology. *Id.* §§ 16914(b), 16919(a), 16981(a). Because laws of this nature are particularly important, the Adam Walsh Act is provided as an example of a context in which a defendant's access to the government's electronic database could be outcome determinative for the defendant.

45. Examples of such parallel investigations include, but are not limited to, actions based on securities law, healthcare regulations, and intellectual property guidelines.

proceedings. Such a risk exists when people produce ESI without knowing whether they are targets or witnesses in criminal actions. Defendants have a constitutional right to know *exactly* the nature and cause of the government's case,[46] and when applied to the twenty-first century, that right should include the production—or at the very least the inspection—of ESI. Therefore, defense counsel must be familiar with ESI that is not apparent on the face of a document in electronic form, such as "metadata," which is data about data.

Most targets of a criminal investigation are not privy to information from intergovernmental agency efforts, such as the government's motive in issuing administrative subpoenas when a target is unaware of a parallel proceeding. In *United States v. Kordel*, the United States Supreme Court made it clear that parallel investigations conducted by civil and criminal enforcement agencies must meet the requirements of the Fifth Amendment's Due Process Clause.[47] *Kordel* involved a corporate vice president who answered the government's interrogatories during a civil proceeding reproving allegedly misbranded products.[48] Had the defendant been more informed, he could have invoked his privilege against compulsory self-incrimination.[49] Failing to do so, he was not able to assert that he was compelled to give testimony against himself as ground for overturning a conviction for introducing misbranded drugs into interstate commerce, even if the information supplied in answers provided evidence or leads useful to the government in the criminal prosecution.[50] The Court did find that "[i]t would stultify enforcement of federal law" to limit the government's discretion to conduct dual investigations strategically; the Court suggested that a defendant may be entitled to a remedy when "the [g]overnment has brought a civil action solely to obtain evidence for its criminal prosecution."[51]

Corporate entities are creatures of the state and do not enjoy a Fifth Amendment privilege; however, their employees as individuals do, and counsel must be on alert as to whether a defendant has an "act of

46. U.S. CONST. amend. VI; *see, e.g.*, Sheppard v. Rees, 909 F.2d 1234, 1236 (9th Cir. 1990).
47. United States v. Kordel, 397 U.S. 1, 11–13 (1970).
48. *Id.* at 2, 5, 6.
49. *Id.* at 7–8.
50. *Id.* at 7–10.
51. *Id.* at 11–12.

production" privilege.[52] *Kordel* and *Doe* remain good benchmarks for present-day defendants confronting governmental agencies seeking e-discovery. Defendants should inquire, with the advice of their counsel, whether the forum the government or regulator is utilizing to obtain e-discovery is appropriate and whether the parties have a common understanding as to the implication of production. Defendants must be wary as to whether the e-discovery sought in one forum, such as a regulatory or administrative forum, is a pretext for building a criminal prosecution that compromises a defendant's constitutional rights.[53] Moreover, the protocol for handling ESI and the manner in which it is actually handled should be memorialized in the event that contested issues arise.

Because technology has become inextricably tied to the way people communicate and therefore constitutes important evidence, criminal defendants will likely seek discovery of ESI, such as Facebook, YouTube, Twitter, and any other soon-to-be social networks, from third parties as well as the government. Counsel who does not press the government effectively to produce ESI may deprive the client of an adequate defense. Counsel should also investigate all sources that may be available to clients for underwriting the expense of e-discovery, such as the advancement provisions of the directors' and officers' insurance policies.

As the role of ESI becomes ever more central during pre- and post-indictment proceedings, criminal defendants may need to rely on the resources of friends and relatives in order to retain computer forensic experts in addition to counsel. As for indigent clients, defense attorneys may have to petition for court-ordered funds. ESI may contain golden nuggets of information, and therefore, defendants who do not diligently pursue ESI on a level playing field with the prosecution may place their defense at risk.

E-discovery is fertile ground for motions to suppress, but its dynamics can be fragile, so be aware that its mishandling may unlawfully interfere with a defense. Targets of criminal prosecutions should ascertain whether the government obtained evidence pursuant to a valid search warrant,[54] especially when the government seizes ESI based on an

52. *See* United States v. Doe, 465 U.S. 605, 617 (1984) (holding that contents of business records were not privileged, but the "act of producing" records was testimonial in nature and therefore privileged and could not be compelled by the government without a statutory grant of use immunity pursuant to 18 U.S.C. §§ 6002–6003).

53. *See, e.g.*, *Kordel*, 397 U.S. at 11–12.

54. U.S. CONST. amend. IV states:

affidavit that did not appropriately—or truthfully—describe the places to be searched and items to be seized from an information system.[55]

Fourth Amendment questions that have been plaguing American courts for decades have resurfaced with the development of technology and the emergence of e-discovery. Specifically, arguments have been made to claim that the Fourth Amendment should not apply because electronically shared or stored information does not possess a "reasonable expectation of privacy."[56] Another Fourth Amendment concern that has lost some clarity with e-discovery and has garnered recent criticism in the Ninth Circuit's ruling in *United States v. Comprehensive Drug Testing, Inc.*[57] is the prohibition against general warrants and the need for particularity of description for the issuance of all warrants.[58] E-discovery allows for the search of a suspect's computers and other electronic devices that could hold incriminating information, including hard drives, systems, databases, and e-mails. Additionally, an officer's

> 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.

55. *See* Franks v. Delaware, 438 U.S. 154, 156 (1978) (noting that "the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit").

56. *See* Katz v. United States, 389 U.S. 347, 351–52 (1967) (noting when there is no reasonable expectation of privacy, the protections of the Fourth Amendment do not apply); *see also* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (establishing precedent that there is no reasonable expectation of privacy in e-mails through a company server or on a company computer—including laptops—if a workplace manual gives such warning, even if the defendant does not know of the warning); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding that employees do not have a reasonable expectation of privacy for electronic communications at work).

57. 473 F.3d 915 (9th Cir. 2006), *withdrawn and superseded by* 513 F.3d 1085 (9th Cir. 2008), *aff'd en banc*, 579 F.3d 989 (9th Cir. 2009). This case has garnered national attention because of its connection with professional baseball. *See id.* However, it has attracted scrutiny because of its argument for the expansion of the government's authority to access private individual's digital information without a warrant. *Id.* at 939–40; *see* Aaron Seiji Lowenstein, Search and Seizure on Steroids: *United States v. Comprehensive Drug Testing* and Its Consequences for Private Information Stored on Commercial Electronic Databases (May 2007) (unpublished article, on file with author), *available at* http://works.bepress.com/aaron_lowenstein/1/.

58. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (stating that warrants must "particularly [describe] the place to be searched and the persons or things to be seized").

searches are not limited by the size of evidence[59] or "curtilage" when dealing with e-discovery, as they would be in traditional searches.[60] These types of unencumbered searches seem to further weaken the notion of people being "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[61] which the Fourth Amendment requires.[62]

The rapidly growing role of ESI in criminal prosecutions of all types, including the prosecution of the mortgage broker and lowly bookmaker, is obvious. It requires that counsel be conversant with this type of evidence and understand how it could affect criminal proceedings. Otherwise, a criminal defendant may be deprived of effective assistance of counsel,[63] and who wants to be that lawyer? In civil proceedings, ESI is a cost issue, but in criminal proceedings, failure to obtain ESI may result in the client's loss of liberty. Technology governs the way members of society communicate, and the criminal justice system must adjust itself to the realities of twenty-first century discovery and ESI's role in order to ensure everyone gets a fair shake at trial.

---

59. *See, e.g.*, United States v. Rettig, 589 F.2d 418, 423 (9th Cir. 1978) (citing Gurleski v. United States, 405 F.2d 253, 258 (5th Cir. 1968) (noting "[t]he search must be one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the crime charged had been committed").

60. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 301 (1987) (defining curtilage as the enclosed area of land around a dwelling that can be protected against unreasonable searches by the Fourth Amendment).

61. U.S. CONST. amend. IV.

62. *Id.*

63. U.S. CONST. amend. VI states:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to *have the Assistance of Counsel for his defence*.

Id. (emphasis added).