
David W Degnan
**United States v. O’Keefe:** Do the Federal Rules of Civil Procedure Provide the Proper Framework for Managing “Data Dumping” in a Criminal Case?  
By David W. Degnan∗

**Abstract**

In 2008, two criminal cases addressed large amounts of unintelligible documents being dumped on the unprepared defendant: *United States v. O’Keefe* and *United States v. Graham*. *O’Keefe* teaches that when the Rules of Criminal Procedure are silent in a criminal case, the civil discovery rules provides a thoughtful and well reasoned answer for how to handle the production of large quantities of unintelligible documents stored electronically. *Graham*, on the other hand, did not apply the civil rules to a comparatively similar criminal data dumping case, but that case did re-emphasize the need and the duty to manage electronic discovery before discovery obligations overwhelm the litigants. As a result, these two cases are cries out for change to the criminal rules to account for electronic discovery.

**Introduction**

Scores of cases and articles address “data dumping” in civil cases—where one party purports to comply with disclosure or discovery obligations by making available to an opponent vast amounts of random, unintelligible and/or unindexed computer data.† The standards for producing and discovering electronically stored information in such civil cases have evolved such that they are generally easy to identify, although difficult to apply in practice.‡ What standards, however, apply when the same issue arises in a criminal case?

Suppose, for example, that an individual is facing a felony indictment for alleged financial improprieties. Counsel for the defendant requests, pursuant to Federal Rule of

---

* Third year law student, Oklahoma City University Law School..  
† *GP Industries, LLC v. Bachman*, 2008 WL 1733606 (D. Neb. April 10, 2008) (Plaintiffs unsuccessfully argued that the documents were produced in a “jumbled fashion” because they were kept that way in the ordinary course-of-business); *In re Payment Card Interchange Fee & Merchant Discount Antitrust Litigation*, 2007 U.S. Dist. LEXIS 2650 (E.D.N.Y. Jan. 12, 2007)(not producing the documents in searchable form violates FRCP 34(b); *3M Company v. Kanbar*, 2007 WL 1725448, (N.D. Cal. June 14, 2007)(producing 170 boxes of unorganized data did not meet the requirements imposed by Rule 34(b)).  
‡ *Id.*
Criminal Procedure 16, that the government produce or allow for inspection all “photographs, books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items in the government’s possession, custody, or control [i]f the item is material to preparing the defense; [i]f the government intends to use the item in its case-in-chief at trial; or [i]f the items obtained from or belongs to the defendant.” After accepting the government’s production of thousands of pages of paper documents and large quantities of electronic evidence, including back up tapes, the defendant makes a good faith effort to examine and cull relevant information from the electronic data, without much success. From the defendant’s perspective, the cost to do further analysis would be substantial, with the restoration of back up tapes alone perhaps costing upwards of $6,000 dollars to attain the reviewable information, and the cost of conducting a review of the millions of relevant documents is equally prohibitive. From the government’s perspective, however, it has complied with the defendant’s request and produced all relevant evidence. And, as a general rule, each party is responsible for the cost of its own review of information produced and disclosed. Substantively, however, with such a vast quantity of data produced, any attempt at review by the defendant is futile.

This criminal hypothetical is a classic illustration of “data dumping.” Although data dumping is litigated far more frequently in civil cases, two significant criminal cases decided in 2008 squarely address the production of large amounts of electronic evidence

---

4 See Degnan, David W., Seven Questions (and Some Answers) on Electronic Discovery, Pretrial Practice and Discovery Newsletter (Spring 2008).
5 The Sedona Principles, Principle 13 (2d ed. 2007)(annotated version) (“Absent a specific objection, party agreement, or court order, the reasonable costs of retrieving and reviewing electronically stored information should be borne by the responding party.”).
in a criminal case: *United States v. O'Keefe*\(^6\) and *United States v. Graham*.\(^7\) With the vast majority of information now being transmitted electronically,\(^8\) computer forensics and related production problems are sure to be confronted more and more frequently in criminal cases, meaning the issue is of vital—and emerging—importance.

This article specifically addresses the issue of how data dumping should be addressed in criminal cases under Federal Rule of Criminal Procedure 15, 16, 17, and 26.\(^9\) The article first compares the rules of discovery and disclosure in civil and criminal cases pending in federal court with electronic discovery and disclosure in mind. The article next explores *O'Keefe*, which promises to be a seminal case addressing electronic data in criminal cases. The article follows with a comparison of *O'Keefe* to existing case law where the Federal Rules of Civil Procedure have been used—either directly or by analogy—in criminal cases. This discussion includes an examination of *United States v. Graham*, an electronic data case decided just months after *O'Keefe*, while using a very different analysis. The article then explores the strategic impact of using the Federal Rules of Civil Procedure as persuasive authority in criminal cases involving electronic discovery.

In the end, the court’s reference in the *O'Keefe* case to the civil rules when the criminal rules were silent was not only smart, but it helped produce a thoughtful and well reasoned result for all the parties. Moreover, the court in *Graham*, while not specifically

---

\(^6\) 537 F. Supp. 2d 14 (D.D.C. 2008) (this case may be distinguishable from Graham because it addresses large amounts of data in the custody of a non-party).

\(^7\) 2008 WL 2098044 (S.D. Ohio May 16, 2008) (This is a classic example of a data dumping in a criminal case).


\(^9\) Rule 41 & 42, which deal with the acquisition of data by the government prior to indictment under the search warrant procedure, is not addressed in this Comment. For a discussion of this, see Regensburger, *Bytes, BALCO, and Barry Bonds*, 97 Journal of Criminal Law and Criminology 1151 (2007).
citing to the civil rules, noted that parties and the court should actively manage electronic discovery cases or risk the dismissal of its case. When electronically stored information is involved, the civil rules incorporate practices that have developed through years of experience by which diligent judges and thoughtful counsel may work together to achieve a just and fair result. For now, these practices can be efficiently utilized where the criminal rules are silent. In the future, the *Graham* case serves as a wake up call for criminal rule-makers: with 93% of data now being transferred electronically, it is time to prepare the criminal rules for a new era in litigation – the era of electronic discovery.


While liberal discovery is a hallmark of the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure provide a far more restricted scope for discovery and fewer avenues by which to pursue it. Moreover, criminal courts do not have the discretion to use the civil rules in criminal cases when those rules conflict with an existing criminal rule, but in a limited number of cases, courts have looked to Federal Rules of Civil Procedure as persuasive authority to achieve a fair result when the criminal rules are silent. And to understand why judges would do this, this section will look at some of the key differences between the criminal rules and civil rules.

Under U.S. civil jurisprudence, the duty to produce discoverable information is well defined under the Federal Rules of Civil Procedure 16, 26, 30, 34, 37, and 45 and clarified by their subsequent comments, including the recent 2006 amendments, which

---

11 With very few exceptions.
added provision for electronically stored information. In addition, as a general rule under the common law, litigants have a duty to preserve reasonably accessible information – electronic or otherwise – that is relevant and in their possession, custody or control when litigation is started or can be reasonably anticipated. Upon request for the production of documents, Federal Rule of Civil Procedure 34(b) requires that the documents be reasonably usable. Common law has further defined that to mean that electronically stored information should be organized, indexed and identifiable such that the documents can be read or used by the other party. And before one document is exchanged, parties are required to “meet and confer” during the 26(f) conference before meeting with the judge at the 16(b) conference to limit scope of discovery and discuss the form(s) of production, among other things, before judicial involvement becomes necessary. Failure to work through the above steps in good faith may result in sanctions under Rule 37(e).

Under the Federal Rules of Criminal Procedure, Rule 16 covers discovery of documents. Assuming the trial judge allows for discovery, the pertinent part of this rule provides:

\[\text{See \textit{Fed. R. Civ. P. 26, 34, 37} and accompanying advisory committee’s notes.}\]

\[\text{\textit{Zubulake v. UBS Warburg}, 220 F.R.D. 212, 217 (S.D.N.Y 2003) ("Zubulake IV") ("While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is subject of a pending discovery request.") (quoting \textit{Turner v. Hudson Transit Lines}, 142 F.R.D. 68, 72 (S.D.N.Y. 1991).}\]

\[\text{\textit{Fed. R. Civ. P. 34}.}\]

\[\text{\textit{Fed. R. Civ. P. 16 and 26(f)}; \textit{MANUEL FOR COMPLEX LITIGATION} (Fourth) §§ 11.445 to 11.447.}\]

\[\text{\textit{Fed. R. Civ. P. 37 and advisory committee’s note.}}\]

\[\text{\textit{Weatherford v. Bursey}, 429 U.S. 545 (1977) (discovery is not a constitutional right in criminal cases); however, the dichotomy between \textit{Bursey}, noting that discovery is not a constructional right in criminal cases and \textit{Brady} and the Federal Rules of Criminal Procedure, noting that the defendant shall be allowed to discover certain data that is material to the preparation of its case, is interesting and worth serious consideration, especially when the government decides it wants to seize an organization’s computers.}\]
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.19

Considering this request could come after the government seizes an individual’s or a company’s computers,20 there could be several virtual truckloads of electronic evidence, all of which may be relevant and material. And there is no provision in the criminal rules allowing for presenting documents in an organized fashion – or for that matter, against dumping those documents on an ill-equipped litigant. Under the criminal rules, a party’s failure to provide discovery may result in an order to comply or any other order the court deems necessary.21 And, if there is any dispute between the parties over what is material or relevant, the parties may hold a pretrial conference “to promote a fair and expeditious trial.”22

There are also due process considerations in criminal cases that are less pressing in civil cases. In overturning a first degree murder charge, Brady v. Maryland,23 the court held that “the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.”24 But Brady is

19 Fed. R. Crim. P. 16(a)(1)(E) (this obligation being mutual under Fed. R. Crim. P. 16(b)(1)(A); “If a defendant requests disclosure under Fed. R. Crim. P. 16(a)(1)(E) and the government complies, then the defendant must permit the government, upon request [to attain reciprocal discovery]).
21 Fed. R. Crim. P. 16(d)(2)
pressed to its limits when potential exculpatory evidence that could prove that the defendant did not commit the alleged crime is buried deep in the hard drive, requiring access to an organization’s seized computers or bit stream images to perform forensic analysis.\textsuperscript{25}

The criminal and civil rules are inconsistent at best. Not only do they establish different precedents, but they also allow for different remedies: civil jurisprudence provides specific remedies and precedent for cost shifting, sampling, and spoliation remedies, while criminal jurisprudence leaves the remedies to the discretion of the trial court; civil procedure requires the parties to meet and confer before speaking the judge at the 16(b) conference, while criminal procedure rule 17.1 notes that pretrial conferences may be useful; and the civil rules provide that the documents must be organized and presented in a usable manner, while the criminal rules are silent on the subject.

Given the last update to the Federal Rules of Criminal Procedure was in 2002,\textsuperscript{26} when electronic discovery was still in its embryonic stage, it is time to start advocating for a change in the rules to account for electronically stored information. And without such change, the criminal defendant and his or her counsel – more often than not appointed by the court – will be left at the mercy of the prosecutor and the diligence of the trial judge, as the rules make no provision for electronic discovery or electronically stored information.

\section*{II. United States v. O’Keefe.\textsuperscript{27}}

\textsuperscript{25}See, e.g., United States v. Competitive Drug Testing, Inc., 513 F.3d 1085 (9th Cir 2008).
\textsuperscript{26}FED. R. CRIM. P. 16 advisory committee’s note.
*O’Keefe* involved allegations that defendant Sunil Agrawal bribed co-defendant Michael O’Keefe, Sr.—an employee of the United States Department of State at the United States Consulate in Toronto, Ontario, Canada—and, in exchange, Mr. O’Keefe expedited the issuance of visas into the United States “contrary to policy and established procedures.” 28 Defendants were charged with conspiracy to commit bribery and the giving and receiving (respectively) of bribes. 29 A key issue was whether the alleged payments were made “corruptly” and with the “intent . . . to influence” an “official act.” 30

Defendants contended that “there was no criminal act . . . as a matter of fact” because expediting visas was a common practice, that the State Department’s procedures and practices were not to the contrary, and that the payments were gifts were based on a friendship, rather than a *quid pro quo* bribe. 31 Defendants then sought discovery from the government regarding (a) visa requests involving defendant Agrawal and his company; (b) rules, policies, procedures and guidelines regarding expediting visa applications and approvals at United States Consulates in North America; (c) names of individuals and entities who were granted expedited visas; and (d) other information. 32 Defendants argued that the responsive information sought—both paper documents and electronic data—would show that there were no formal policies in place, thereby negating any possible criminal intent, as a matter of law. 33

---

29 *Id.*
30 *Id.*
31 *Id.*
32 *Id.* at *3-4.*
33 *Id.* at *1.*
The government objected to these requests on a variety of grounds, including that the material sought did not meet the materiality standard, the requests were overbroad, that identifying and producing responsive documents and data would be “time-consuming, burdensome and logistically difficult.”


In addressing defendants’ motion to compel discovery, O’Keefe I noted that “‘the government cannot take a narrow reading of the term ‘material’ in making its decisions on what to disclose’” under Federal Rule of Criminal Procedure 16. While Rule 16 states discovery must be material, the court noted that considerations based on logistical difficulty or burden may be persuasive in weighing whether to permit discovery, but those considerations are not determinative of the question of whether the discovery sought is material “to the preparation of the case.”

Because the information requested met the materiality test, O’Keefe I ordered the government to produce expedited visa applications and decisions made in other consulates relating to expediting visa applications. The court also ordered the government to produce applicable policies or procedures for requests to expedite visa applications, and if there were none, electronic mail, facsimiles and other records that would evidence policies of the State Department. The government was expected to conduct “thorough and complete searches of both hard copy files and electronic files, in a

---

34 Id. at *1.
35 Id. at *1. Technically, defendant Agrawal filed a motion to compel in which defendant O’Keefe joined. Id. at *1.
29 Id.
37 Id. at *3.
38 Id. at *3. In doing so, the court set forth detailed protocols about how information was to be sought from the consulates and how the parties were to proceed going forward. Id. at *4.
good faith effort to uncover all responsive information in its ‘possession, custody or control.’”


When the government provided materials responsive to the order in O’Keefe I, defendants were not satisfied and, accordingly, filed another motion to compel “protesting that the government has not fulfilled the responsibilities” imposed by O’Keefe I. According to defendants, the information provided about the government’s search efforts posed substantial concerns.

The government provided an affidavit describing what a six-member team did in an effort to comply with the O’Keefe I order. That affidavit described what paper documents the government had searched as well as electronic data searches. Electronic data searches used keyword searches and included searches of active servers and backup tapes (“retained for two weeks”), with the data then reviewed for responsiveness. Any deleted email or backup tapes stored before the search was no longer recoverable. In the second motion to compel, the defendants challenged the government’s production of paper documents as well as the government’s electronic production. The O’Keefe II court analyzed those two challenges separately.


39 Id. at *3 n.2.  
41 Id. at 16.  
42 537 F. Supp. 2d at 16-18 (quoting declaration of Peggy L. Petrovich, Visa Unit Chief, United States Consulate General, Toronto, Ontario Canada).  
43 Id. at 17-18.  
44 Id. at 17-18.  
45 Id. at 18.  
46 Id.
In filing their second motion to compel in *O’Keefe II*, defendants demanded that the government produce an index for the document production showing, “for each document, the custodian of the documents, his or her title, the source of the document, whether it is a paper document or electronically stored information and the Bates number of the document.” The defendants also demanded that electronic documents be produced in an organized and readable manner because without such organization, the defendant could not conduct any kind of meaningful review of the produced documents.

In ruling on this aspect of defendants’ motion to compel, *O’Keefe II* looked to the Federal Rules of Civil Procedure for the applicable analysis:

In criminal cases, there is unfortunately no rule to which the courts can look for guidance in determining whether the production of documents by the government has been in a form or format that is appropriate. This may be because the “big paper” case is the exception rather than the rule in criminal cases. Be that as it may, Rule 34 of the Federal Rules of Civil Procedure speaks specifically to the form of production. The Federal Rules of Civil Procedure in their present form are the product of nearly 70 years of use and have been consistently amended by advisory committees consisting of judges, practitioners, and distinguished academics to meet perceived deficiencies. It is foolish to disregard them merely because this is a criminal case, particularly where, as is the case here, it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problems.

The *O’Keefe II* court then looked to Federal Rule of Civil Procedure 34 to fashion an order under Federal Rule of Criminal Procedure 16 for the production of paper documents and Electronically Stored Information.

---

47 *Id.*
48 *Id.* at 18-19
49 *Id.* at 19.
50 *Id.* at 19.
Federal Rule of Civil Procedure 34 states, in relevant part, that:

A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request; if a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and a party need not produce the same electronically stored information in more than one form.\(^{51}\)

As noted in *O'Keefe II*, Federal Rule of Civil Procedure 34 was amended in 1980 “to prevent the juvenile practice whereby the producing party purposely rearranged the documents prior to production in order to prevent the requesting party’s efficient use of them.”\(^{52}\) Indeed, *O'Keefe II* cited several cases for the proposition that the reviewed documents must be either produced in the ordinary course of business, or they must be indexed, tabbed and otherwise produced in a manner that “render[s] them usable by the requesting party.”\(^{53}\)

Applying this standard, and without having reviewed the documents, the court found that the government’s production fell well short of the mark:

I have not seen the documents at issue in this case, but I can say that, if all of the documents have been produced in an undifferentiated mass in a large box without file folders or labels, then these documents have not been produced in the manner in which they were ordinarily maintained as Rule 34(b)(2)(E)(i) requires. To be useful at the consulate, in their original state, they must have been placed in labeled file folders in the file cabinets described by [the government’s affidavit]. Without such file folders and

\(^{51}\) **Fed. R. Civ. P. 34(b)(2)(E).**

\(^{52}\) *O'Keefe II*, 537 F. Supp. 2d at 19; *see also* Fed. R. Civ. P 34 advisory committee’s notes.

labels, it is impossible to understand how anyone who
needed to find these documents could have done so.\textsuperscript{54}

Moreover, the document stamps did not specify what Consulate the information was coming from.\textsuperscript{55} This, in turn, would leave the defendants guess to “about the evidentiary value of the documents” as well as the author(s) for purposes of authenticity.\textsuperscript{56} Indeed, given the nature of the production, the court recommended that all documents produced by the government be deemed authentic.\textsuperscript{57}

Another problem was determining what documents were relevant.\textsuperscript{58} Because many of the documents did not have identifiable provenance, the court ordered parties to meet in good faith to attempt to stipulate who is the “author, recipient (if any), date of each document, and where the document was found.”\textsuperscript{59} After the parties confer, any document still in dispute would be addressed by the court at a later date.\textsuperscript{60}

\textbf{2. Analysis of Electronic Data Production.}

In addressing the government’s production of electronic data, the court looked to the Federal Rules of Civil Procedure to address issues of preservation of electronic documents, metadata, alleged search term inadequacies and other deficiencies alleged by defendants.\textsuperscript{61}

\textsuperscript{54} Id.
\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
\textsuperscript{59} Id. at 21.
\textsuperscript{60} Id.
\textsuperscript{61} Id. at 22-24.
Starting with purported destruction of electronic data, the court observed that destruction “of evidence pursuant to a neutral policy and without any evidence of bad faith does not violate the due process clause if the evidence was destroyed before the defendants raised the possibility that it was exculpatory and the government had no objective reason to believe that it was exculpatory.”\footnote{Id. at 22 (citing \textit{Arizona v. Youngblood}, 488 U.S. 51, 57, 109 S.Ct. 333, 102 L.Ed.2d 281 (1988); \textit{In re: Sealed Case}, 99 F.3d 1175, 1178 (D.C.Cir.1996). Accord \textit{United States v. Beckstead}, 500 F.3d 1154, 1158-62 (10th Cir.2007); \textit{Bower v. Quarterman}, 497 F.3d 459, 476-77 (5th Cir.2007)).} This concept “finds its analogue” in Federal Rule of Civil Procedure 37(e), which states that “absent exceptional circumstances, sanctions will not be awarded for a party’s failure ‘to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.’”\footnote{\textit{O’Keefe II}, 537 F. Supp. 2d at 22 (quoting \textit{Fed. R. Civ. P. 37(e)}).} But describing the defendants’ complaint as “vague notions that there should have been more than what was produced,”\footnote{Id. at 22.} the court directed defendants to make specific, factually-supported assertions that the government failed to produce evidence in bad faith within 21 days, or that claim would be waived.\footnote{Id. at 23.}

The court next addressed defendants’ complaint that electronic data was produced as PDF or TIFF files, rather than in the files native format with accompanying metadata.\footnote{Id.} Acknowledging that \textit{O’Keefe I} did not direct the format of the government’s production of electronic data, the court again looked to the Federal Rules of Civil Procedure for the answer.\footnote{Id.} More specifically, “if, as occurred here, electronically stored information is demanded but the request does not specify a form of production, responding party must produce the electronically stored information in the form which it
is ordinarily maintained or in a reasonably usable form or forms;” “a party ‘need not produce the same electronically stored information in more than one form.’” 68 Given that defendants failed to specify the format in which the government should produce electronic data, the court refused to issue orders regarding the form of production. 69

The final issue related to the use of search terms by the government, which defendants claimed were deficient. 70 Citing authority discussing the use of search terms in the civil context, the court observed that whether keywords are appropriate “is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics.” 71 Given this complexity, “for lawyers and judges to dare opine that a certain search term would be more likely to produce information than the terms that are used is truly to go where angels fear to tread.” 72 As a result, the court denied the defendants’ motion with regard to keywords without prejudice, adding that “if defendants are going to contend that the search terms used by the government were insufficient, they will have to specifically so contend in a motion to compel and their contention must be based on evidence that meets” the expert witness requirements of Federal Rule of Evidence 702. 73

III. Analysis and Implications.

68 Id. (quoting FED. R. CIV. P. 34(b)(2)(E)(ii) and (iii)).
69 Id. In doing so, the court noted “that the government seems ready and willing to produce the documents in native format.” Id.
70 Id. at 24.
72 O’Keefe II at 24.
73 Id.
What, then, is the impact of O'Keefe? Viewed narrowly, the O'Keefe decisions simply granted in part and denied in part motions to compel discovery in a comparatively unique criminal case. Indeed, to date, O'Keefe has not been followed by any court to show that the Federal Rules of Civil Procedure should have any applicability to discovery in criminal cases. 74

Viewed more broadly, however, O'Keefe stands for the proposition that the Federal Rules of Civil Procedure may have application to criminal cases when the criminal rules are silent. This is particularly true where time worn issues in civil cases—such as voluminous document production and the production of electronic data—are at issue in a criminal case. Indeed, O'Keefe has already been identified by thoughtful observers in the area in which the best practices for representing clients in civil cases are carrying over into the criminal context. 75 Several other commentators appear to read O'Keefe as providing, in the right case, a roadmap to use the Federal Rules of Civil Procedure as a guide for production of electronic discovery in criminal cases where doing so promotes the general principles applicable in criminal cases. 76 The reasons to do so are

74 However, O'Keefe has been cited in one case for its applicability to the Federal Rule of Evidence 702; See Equity Analytics v. Lundin, 248 F.R.D. 331 (D.D.C. 2008).
75 See, e.g., Cecil A. Lynn, You've Been Served: Corporate response to Grand Jury Subpoenas and Search Warrants for ESI, 9 Sedona Conf. L. J. --, at *7 (2008). (Forthcoming); Daniel K. Gelb, Litigating Criminal Issues when ‘ESI’ is the Subject of ‘CSI’, Digital Discovery and E-Evidence, Vol. 8, No. 4, 84-87 (4/1/08) (“The proliferation of telecommunications, e-mail, the Internet, electronic faxing, and digital voicemail has refined both the meaning of “relevant evidence” and how much evidence should be obtained, preserved, and produced. All of the aforementioned mediums of communication contain ESI which could significantly impact the outcome of your client’s case, regardless of whether the litigation context is civil or criminal [citing O'Keefe].”)
many, including that there have been more than 70 years of experience in applying the Federal Rules of Civil Procedure in ‘the big paper case.’”

Before O’Keefe, courts in criminal law cases have analogously drawn upon the Federal Rules of Civil Procedure from time to time. For example, in United States v. Morrison, a case involving the sale of contraband cigarettes to Native Americans in violation of Contraband Cigarettes Trafficking Act (CCTA), the court held that when the Federal Criminal Rules of Procedure are silent, a court may draw upon the analogous Federal Rules of Civil Procedure as instructive, because “courts in this district have resolved such motions according to the same principles that apply in the civil context.”

Similarly, United States v. Balistrieri, in a coram nobis claim—a comparatively unique case involving the reconsideration of a closed criminal case for alleged procedural irregularities, which is a historically civil remedy—the court relied on the Federal Rules of Civil Procedure in the interest of a speedy trial or efficiency, as failing to do so (and relying solely on the Federal Rules of Criminal Procedure) would provide an unjust result. And in In re Grant Jury Subpoena Dated October 22, 2001, citing civil rule

---

78 521 F.Supp. 2d 246 (E.D.N.Y. 2007)
79 Id. at 252 (specifically, Federal Rule of Civil Procedure 54(b) and relevant civil case law); see also U.S. v. Gigante, 971 F.Supp. 755 (E.D.N.Y. 1997).
81 Id. at 221 (A coram nobis motion is “a remedy available in a criminal case to correct fundamental errors that render that proceeding irregular and its judgment invalid. Nevertheless, because it is a postjudgment attack upon a conviction by a defendant no longer in any form of custody, and insofar as it is still governed by civil rules, forms and pleadings, its character reflects the vestiges of its civil origins: the intrinsic all-writs jurisdiction of the Court.”).
82 United States v. Balistrieri, 606 F.2d 216, 221 (The court explains that “Rule 16, F.R.Cr.P., is an unsatisfactory vehicle for discovery requests in proceedings on a coram nobis motion. Facts which affect the validity of the conviction or sentence are unlikely to be found solely within the narrow scope of discovery allowed by Rule 16. On a coram nobis motion, statements made by government witnesses or prospective witnesses, expressly protected from discovery by Rule 16(a)(2), may be highly relevant to the applicant’s ability to prove his allegations. For reasons of policy, as well as the consistency of legal
26(b)(3), the court applied the civil work-product rule to a criminal case without explanation.\textsuperscript{84}

But just because the Federal Rules of Civil Procedure can be used by analogy does not mean they should be applied in criminal cases, as several courts have found. In *Application of Eisenberg*,\textsuperscript{85} the court forbade a civil discovery request since such a request “was a disguised attempt at criminal discovery.” Similarly, in *U.S. v. Stewart*,\textsuperscript{86} a criminal case in which the defendant argued that the emails counsel forwarded to a family member during the course of the trial should be protected from disclosure under the work-product doctrine,\textsuperscript{87} the court opined that while the document would probably be protected under the Federal Rules of Civil Procedure, those rules do not apply in a criminal case.\textsuperscript{88} The court went to great detail to weigh the protections offered for work-product under the criminal and civil rules but ultimately found that this criminal case “was not governed by the civil rules.”\textsuperscript{89}

Courts have been wary of applying civil procedure rules in another procedural context: arbitration. In *Mississippi Power v. Peabody Coal*,\textsuperscript{90} the first district court judge

\textsuperscript{83} 282 F.3d 156, 161 (2nd Cir. 2002).
\textsuperscript{84} While courts have occasionally used the Federal Rules of Civil Procedure as persuasive authority in criminal cases, civil procedure rules can only be directly applied in criminal cases when expressly authorized by law or statute, e.g. Rule 12 of 18 USC. § 2255 governing proceedings to review sentencing. See, e.g., *Stead v. United States*, 67 F. Supp. 2d 1064, 1073 (D.S.D 1999).
\textsuperscript{85} 654 F.2d 1107, 1107 & 1112 (5th Cir. 1981).
\textsuperscript{86} 287 F. Supp. 2d 461 (S.D.N.Y. 2003).
\textsuperscript{87} *Id.* at 464-465.
\textsuperscript{88} *Id.* at 470.
\textsuperscript{89} *Id.* at 466-67.
\textsuperscript{90} 69 F.R.D. 558, 560 (S.D. Miss. 1976).
allowed discovery using the Federal Rules of Civil Procedure. However, upon review, the second District Judge did not allow discovery under the Federal Rules of Civil Procedure because the end result would be contrary to the nature of arbitration, which usually has little or no discovery. Applied to the criminal cases, if the court allows the civil rules to be used, it would go beyond the established scope of criminal discovery.

Cases questioning the applicability of the civil discovery rules to the criminal context were not considered by the court in O’Keefe; however, given the complexity of some issues presented in that case, the result was strikingly fair. In O’Keefe, the government was not providing the defendant with a realistic opportunity to search or use the data. Since the judge is invested with discretion under Federal Rule of Criminal Procedure 16(d) to allow discovery and set reasonable conditions, the court might have ruled that the government’s failure to produce the requested documents or conduct the requested searches amounted to inadequate discovery without reference to the Federal Rules of Civil Procedure. But by incorporating reference to the civil procedure rules, the judge was able to provide a thoughtful and well reasoned opinion by which the litigants could follow and know what steps are necessary to meet the judge’s expectations in future e-discovery disputes.

But for those not as “plugged-in” to the recent updates in the Federal Rules of Civil Procedure and their application to Federal Rules of Criminal Procedure, another federal court has confronted a similar data dumping criminal case without using the civil rules. In this tax case in which the court decided a motion to dismiss brought by the

---

92 Id. at 566 (“We feel appellee makes no satisfactory answer to appellant’s contention that a court order of discovery would be affirmatively inimical to appellee’s obligation to arbitrate.”).
defendant under the Speedy Trial Act, *United States v. Graham*, the court held that there is a continuing need to manage electronic discovery, even in complex criminal cases.

In *Graham*, the defendants were indicted with several criminal tax offenses, including setting up “abusive tax shelters” and “conspiracy to defraud” the federal government. But before reaching the merits of the case, the court spent two years on pretrial issues. Indeed, the government had produced an “unprecedented volume of discovery, including . . . approximately 1.5 million documents, 300 videotapes, 500 recorded conversations, 90 hard drives of computers, and 3,000 diskettes.” But that production had its share of problems, as 1) the large quantity of documents produced was not organized, 2) “like a restless volcano, the government periodically spews forth new discovery,” and 3) the government’s “discovery itself has often been tainted or incomplete,” resulting in the electronic production of documents being riddled with viruses.

As a result of the unprecedented amount of discovery and the subsequent production shortfalls in this criminal case, the defendant sought to have the case dismissed under the Speedy Trial Act. The court agreed. In determining whether the dismissal mandated by the Speedy trial Act would be with or without prejudice, the court

---

94 Id. at *7 (“Consequently should this case be re-indicted, the Court will be more acutely aware of the potential pitfalls to be avoided.”).
96 Id. at *5.
considered three factors: 1) the seriousness of the offense 2) the government’s neglect and 3) prejudice in determining whether to dismiss this case as this is a felony charge.\footnote{Id. at *6.}

First, the court considers the felonies of which the defendants were accused very seriously.\footnote{Id. at *6.} The court also found that there was no bad faith on the part of the government in failing to complete discovery in a timely manner.\footnote{Id. at *6.} Blame, the court noted, should be shouldered by each of the parties.\footnote{Id. at 6.} First, the government must share its share of the blame because “in a matter of this complexity and magnitude, the government cannot be permitted to remain inert in the face of large volumes of unsorted discovery material. Nor can the government be permitted to refuse to share databases and search engines with defense counsel. . . . Electronic discovery must be provided in virus-free, non-corrupt form.”\footnote{Id. at *6.} Similarly, the defendants are to blame for not bringing the issues faced in discovery, such as the corrupt electronic files, to the court’s attention sooner.\footnote{Id. at 6.} And, the court must also shoulder its share of blame for failing to set forth reasonable deadlines for a trial.\footnote{Id. at *6.} For those reasons, the court indicated that the defendants did suffer prejudice from the delay because, as the \textit{Barker} Court explains, “inordinate delay between public charge and trial, wholly aside from possible prejudice to a defense on the merits, may seriously interfere with the defendant’s liberty.”\footnote{Id. at *7.} Since

\begin{footnotes}
\footnotetext{97} Id. at *6.
\footnotetext{98} Id. at *6.
\footnotetext{99} Id. at *6.
\footnotetext{100} Id. at *6.
\footnotetext{101} Id. at 6.
\footnotetext{102} Id. at *6.
\footnotetext{103} Id. at *6 -7.
\footnotetext{104} Id. at 7 (quoting \textit{Barker v. Wingo}, 407 U.S. 514, 537 (1972).)
\footnotetext{105} Id. at *7.}
\end{footnotes}
blame could be equally shared, among other things, *Graham* then held that the case should be dismissed without prejudice.\textsuperscript{106}

In many ways, the *Graham* case is the opposite of *O’Keefe*. In *O’Keefe*, the government did not produce data or allow the data sources to be searched. In *Graham*, the government produced literally everything and buried the defendant. Moreover, *O’Keefe* was decided with explicit reference to the civil rules, whereas the court in *Graham* never mentioned them.

But the *O’Keefe* and *Graham* decisions, while based on very different facts and procedural postures, can be reconciled. The court in *O’Keefe* suggests that counsel in the criminal justice system may not be as prepared as their counterparts in the civil justice system for modern litigation, and the rules of criminal procedure offer little help, necessitating resort to the recently updated Federal Rules of Civil Procedure. The court in *Graham*, on the other hand, was able to reach a similar result without having to rely on civil rules, but still noted the need to define and manage electronic discovery issues in this criminal case. Therefore, the results of similar cases in the future – and there will be many – may depend on how comfortable counsel and the judge are with civil practice. Those who are more familiar with the civil rules will be more willing to adopt the dicta of *O’Keefe* because the Federal Rules of Civil Procedure offer much more guidance for effectively managing electronic discovery. However, the *Graham* decision strongly suggests that judges have considerable discretion, if not clear guidance, under the existing rules of criminal procedure to manage electronic discovery. Simply put, *O’Keefe* encouraged the litigants to benefit from the tested methods and experience of the civil

\textsuperscript{106} *Id.* at *1.
rules, while *Graham* teaches that criminal courts need to be aware of and account for electronic discovery.

**Part IV: Strategic Implications**

Electronic discovery issues are certain to present major pretrial management challenges for criminal litigants and courts in future cases, and the need to avoid “data dumping” is a classic challenge in both criminal and civil litigation. Since the 2006 amendments to the Federal Rules of Civil Procedure, there have been several civil cases that specifically address the production of vast quantities of information in an unusable form.\(^\text{107}\) Litigants are required to discuss the form of production before the opening of formal discovery.\(^\text{108}\) Courts and litigants often cite to Rule 34(b) if they believe that production is inadequate.\(^\text{109}\) But there are no equivalent rules on the criminal side, making it difficult to determine how courts have or will handle this issue in the future.\(^\text{110}\) To prevent the occurrence of the unknown, counsel should consider how to apply the three central strategic implications of *O’Keefe* and *Graham*.

A. The Civil Rules May Be Applied Where the Criminal Rules are Silent.\(^\text{111}\)

In a criminal case, as a general rule and barring exceptional circumstances, a court will only apply the civil discovery rules when the established rules of criminal procedure

---

\(^{107}\) See, *supra*, fn. 1.

\(^{108}\) See Fed. R. Civ. P. 26(f)(3) (“A discovery plan must state the parties' views and proposals on . . . any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.”).

\(^{109}\) *Id.*


\(^{111}\) See, *supra*, n. 84.
are silent.\textsuperscript{112} Electronic discovery is one the cutting edge fields of the legal profession, and its practice has experienced tremendous development in civil litigation over the last five years. So in areas such as document organization, discovery plans, and sanctions, it would not be entirely out of reach for a criminal court to cite to the Federal Rules of Civil Procedure as instructive.\textsuperscript{113} As in \textit{O'Keefe} and \textit{Graham}, future courts must find well reasoned and thoughtful ways to understand and manage pressing issues of electronic discovery, especially given the rising cost expected in future criminal cases, as more discovery is produced in electronic form.

B. Counsel Should Consider who is Paying

Approximately 80\% of defendants in the criminal justice system are represented by a government-appointed lawyer.\textsuperscript{114} This means that the government (a.k.a. the taxpayer) is required to pay for both the prosecution and defense. As electronic discovery becomes more common, cooperation – or the lack thereof – may have tremendous ramifications for the criminal justice system. As a result, the Attorney General and the Director of the Administrative Office of the United States Courts instructed the Department of Justice and the Administrative Office of the United States Courts (which runs the Federal Defender and Civil Justice Act programs) to look for ways to cooperate to reduce the anticipated cost of future criminal litigation.\textsuperscript{115} This mandate resulted in the formation of the Administrative Office/Department of Justice


\textsuperscript{113} See \textit{Fed. R. Civ. P} 26, 34, 37 & accompanying 2006 advisory committee’s notes (setting specific requirements for electronic discovery).

\textsuperscript{114} See Kurt Schauppner, Public \textit{Defense Face Heavy Load}, Hi-Desert Star (July 9, 2008), http://www.hidesertstar.com/articles/2008/07/10/news/news2.txt

\textsuperscript{115} See, \textit{infra}, n 116.
Joint Working Group on Electronic Technology in the Criminal Justice System (JET-WG).

In the JET-WG 2003 Draft Report and Recommendations, the working group predicted that electronic discovery will become one of the most pervasive issues in criminal law. Indeed, the report noted that “the ability of all participants in the criminal justice system to address the issues presented by these new technologies will greatly impact that system’s fairness and efficiency.” Therefore, the report recommended that counsel must “meet and confer” to discuss and define e-discovery issues, and develop procedures to account for and reduce the cost of electronically stored information in criminal cases.

The JET-WG recommendations have not been met with universal acceptance. Only a handful of district courts have established local Working Groups or adopted e-discovery protocols for criminal cases. In the civil context, The Sedona Conference®, a legal think tank located in Phoenix, Arizona is leading the charge for cooperation in discovery, with significantly more success. In several of its publications, that

---


118 Id. at 4.

119 Id. at 5 – 7.


123 See, e.g., In re Seroquel Prods. Liab. Litig. 244 F.R.D. 650, 656 (M.D. Fla. 2007) (citing to the Sedona Principles as a leading resource for electronic discovery issues).
organization notes that without cooperation among counsel and the court in electronic discovery matters, litigation will become entirely too costly or even prohibitive, leading to a breakdown of the civil justice system.\textsuperscript{124} The Sedona Conference is in the process of creating a series of “toolkits,” collections of practice resources, to assist civil plaintiffs, defendants, courts, and mediators to better manage e-discovery cases, to avoid or resolve e-discovery conflicts, and to reduce litigation costs for all parties.\textsuperscript{125} As The Sedona Conference “Cooperation Proclamation” and accompanying practice resources gain more acceptance in civil litigation, they will likely be adapted for use in the criminal justice context.\textsuperscript{126}

C. The Criminal Rules Need to Be Changed

Electronic discovery can be incredibly costly. Few commentators have opined about exactly how much it costs,\textsuperscript{127} but several courts have noted that they are not insensitive to the cost of litigation, particularly to the cost involved with electronic discovery. And, as a result, the Federal Rules of Civil Procedure have specific provisions to avoid undue burdens in the production of electronically stored information, the production of data from sources that are not reasonably accessible, and the production of data that are not reasonably useable. The Criminal Rules make no such provisions.

\textsuperscript{124} See, e.g., The Sedona Conference®, \textit{The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production}, Principle 3, 21(2d ed. 2007) (“Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party’s rights and responsibilities”), available at http://thesedonaconference.com/dltForm?id=TSC_PRINCP_2nd_ed_607.pdf

\textsuperscript{125} Id.

\textsuperscript{126} Interview with Ken Withers, Director of Judicial Education and Content at The Sedona Conference®, in Phoenix, Arizona. (July 31, 2008).

\textsuperscript{127} See, e.g., David W. Degnan, \textit{Seven Questions (and Some Answers) on Electronic Discovery}, Pretrial Practice and Discovery Newsletter (Spring 2008).
It is time for change. The criminal rules must be updated to account for electronic discovery – while taking into account due process considerations – otherwise the costs will spiral out of control before the judge realizes what happened. Indeed, in the *Graham* case, it took two years before the court realized the number of discovery abuses.

**Conclusion**

Where the Rules of Criminal Procedure are silent on data dumping, *O’Keefe* provides a thoughtful answer by reference to the Federal Rules of Civil Procedure. And while *Graham* did not apply the civil rules to a criminal case, it re-emphasized that there is a duty to manage and cooperate in electronic discovery. But even more importantly, these two cases are cries out for a change to the criminal rules to account for electronic discovery.