

THE DECISION TO COMPEL UNRESTRICTED FORENSIC IMAGING: A NOTE DISCUSSING *JOHN B. v. GOETZ*

*Christen M. Steimle**

I. INTRODUCTION

Evidence gathered during discovery can determine the outcome of litigation. The amended Federal Rules of Civil Procedure now recognize electronic discovery as integral to the discovery process. The computer has been compared to a filing cabinet.¹ However, through forensic imaging, parties can obtain direct access to computers, which rarely occurred when information was physically stored in filing cabinets. A mirror image (i.e. forensic imaging) is defined as “an exact duplicate of the entire hard drive, and includes all the scattered clusters of the active and deleted files and the slack and free space.”² Since the implementation of the amended rules, courts have continued to define the boundaries of the rules, and one example of this is the Sixth Circuit’s decision in *John B. v. Goetz*.³ Here, the court set aside the district court’s orders compelling unrestricted forensic imaging of the defendants’ computers, and therefore limited the breadth of discovery.⁴

This Note argues that the *John B. v. Goetz* case was correctly decided because unrestricted forensic imaging should rarely be compelled. In *Goetz* the underlying concerns of privacy and confidentiality outweighed the purported need for unrestricted imaging. Section II provides an overview of the previous and amended Federal Rules of Civil Procedure. Section III outlines the facts of the *John B. v. Goetz* case. Section IV analyzes the Sixth Circuit’s reasoning and discusses important factors other courts have considered when determining whether to compel forensic imaging. Section IV also provides practical tips for effectively utilizing forensic imaging while still protecting important concerns, including privacy, confidentiality, and privilege. Finally, Section V concludes this Note.

II. BACKGROUND LAW

The Federal Rules of Civil Procedure were amended in December of 2006, primarily to address the issue of electronic discovery (hereinafter the “Amended

* Christen M. Steimle is a J.D. candidate for 2010 at the Salmon P. Chase College of Law, Northern Kentucky University. She earned a B.S. in International Business from Wright State University in 2004.

1. *See* Menke v. Broward County Sch. Bd., 916 So.2d 8, 10 (Fla. Dist. Ct. App. 2005).

2. *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 48 (D. Conn. 2002).

3. *John B. v. Goetz*, 531 F.3d 448 (6th Cir. 2008).

4. *Id.* at 461.

Rules”).⁵ Prior to these amendments, it was unclear as to what extent the rules applied to discovery for electronically stored information (hereinafter “ESI”), primarily because of the word “document.”⁶ As the use of computers and electronic data storage became more widespread, electronic discovery became a significant issue and the need for revision became clear.⁷ Specifically, the primary issue was whether all electronically stored information, including computer generated documents and system information were included within the scope of discovery.⁸ The uncertainty surrounding the rules and their application to electronic discovery made it difficult for attorneys and businesses alike to know what information was discoverable, how to efficiently retain data, and how to effectively prepare for litigation.⁹

Generally, the 2006 amendments encourage both the courts and the parties to begin actively discussing the discovery process earlier in litigation.¹⁰ Amended Rule 16(b) states that scheduling orders can now include provisions relating to disclosure and discovery of electronic information, and also recognizes that any agreements made between parties regarding assertion of privilege after production of documents will be respected.¹¹ Amended Rule 26 discusses what electronic information needs to be automatically disclosed, as well as addresses the cost of electronic discovery, allowing for the possibility of cost shifting depending on the breadth of the request and the difficulty of producing the information.¹² The amendment to Rule 34(a) is most significant because it demonstrates that discovery includes all ESI, either manually created or computer generated.¹³ Additionally, the Amended Rules permit parties to copy data.¹⁴ Rule 34 allows a party to copy or photograph sections of ESI, e.g., forensic imaging.¹⁵ Since the Amended Rules became effective, courts have continued to define the boundaries of electronic discovery through cases such as *John B. v. Goetz*.¹⁶

5. THE SEDONA PRINCIPLES, SECOND EDITION: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 11 (2d ed. 2007).

6. *Id.*

7. *Id.*

8. *Id.*

9. *See Analog Devices, Inc. v. Michalski*, No. 01 CVS 10614, 2006 WL 3287382, at *5-6 (N.C. Super. Nov. 1, 2006).

10. *See RONALD J. HEDGES, DISCOVERY OF ELECTRONICALLY STORED INFORMATION: SURVEYING THE LEGAL LANDSCAPE* 37 (BNA Books 2007).

11. *Id.* at 24.

12. *Id.* at 34-41.

13. THE SEDONA PRINCIPLES, *supra* note 5, at 11.

14. HEDGES, *supra* note 10, at 46.

15. *Orrell v. Motorcarparts of Am., Inc.*, Civil No. 3:06DV418-R, 2007 WL 4287750, at *7 (W.D.N.C. Dec. 5, 2007).

16. *John B. v. Goetz*, 531 F.3d 448, 448 (6th Cir. 2008).

III. FACTS

John B. v. Goetz is a class action lawsuit between 500,000 children, who were enrolled in the TennCare program, and the state officials responsible for the creation and administration of the TennCare program.¹⁷ TennCare was a “managed care system” which replaced the state’s Medicaid program.¹⁸ Essentially, the plaintiffs alleged that the state’s TennCare program failed to meet certain requirements of the Social Security Act, including providing services such as “medical screenings, vision, hearing, and dental.”¹⁹ The Social Security Act requires state programs that accept federal funding, such as TennCare, to provide these services, called Early and Periodic Screening, Diagnosis, and Treatment (EPSDT) services, to individuals under the age of twenty-one who are eligible to receive Medicaid.²⁰ In response to the lawsuit and demand for compliance, the parties worked to reach a mutually agreeable plan to correct TennCare’s deficiencies, and the court issued an order for the implementation of the plan in 2000.²¹

In late 2001, the plaintiffs moved to hold the defendants in contempt for failing to implement the agreed upon plan.²² The court noted that although the defendants were working to implement the plan and were well-intentioned, the fundamental inefficiencies of the TennCare program itself slowed the progress.²³ The court delayed ruling on whether the defendants were in contempt and appointed a special master to facilitate the execution of the plan.²⁴

From the time the court appointed the special master through 2004, the parties continued to debate compliance with the 2000 orders.²⁵ In October 2004, the plaintiffs again filed a motion requesting the court to hold the defendants in contempt for violation of the 2000 orders, claiming that the plan still had not been enacted.²⁶ The court agreed that the plan had not been implemented and ordered the special master to develop a remedial plan to correct TennCare’s insufficiencies, which the special master did.²⁷ In November of 2004, the defendants objected, claiming that the October 2004 orders and the special master’s suggested plan were the product of “*ex parte* communications” between

17. *Id.* at 451.

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.* at 452.

22. *John B.*, 531 F.3d at 452.

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.*

the judge and the special master.²⁸ As a result of the dispute, the orders and plan were set aside and the judge recused himself.²⁹

In February of 2006, the defendants finally claimed compliance with the 2000 orders, causing the plaintiffs to request the production of electronically stored information relating to and confirming the purported compliance.³⁰ The defendants produced the requested information in hard copy format, as opposed to electronic, leading the parties to debate the required production format for electronic discovery requests.³¹ After extended debate and negotiations, the parties failed to reach an agreement, and in October of 2006, the plaintiffs filed a motion to compel discovery.³²

The court issued two orders in response.³³ The first order required the defendants to provide responsive documents in electronic format.³⁴ The second order required the defendants to give the court and the plaintiffs a written description of the technical specifications of the defendants' electronic data and required the parties to create a plan for the production of additional electronic records.³⁵ The defendants acknowledged that some previous discovery responses had been incomplete, which prompted the court to allow the plaintiffs to obtain assurances as to the completeness of future discovery responses.³⁶ In December of 2006, an "experts only" conference was held, during which the parties outlined an electronic discovery protocol, including an agreement on keyword search terms.³⁷ Unfortunately, this conference did not resolve all of the disputes surrounding electronic discovery, which continued during the next ten months.³⁸

Finally, in October of 2007, the court granted the plaintiffs' most recently filed motion to compel discovery.³⁹ The court stated that the repeated disputes stemmed from the defendants' failure to preserve and provide electronic information.⁴⁰ While the court recognized that it could sanction litigants for failing to preserve data in preparation of litigation, it refused to impose sanctions until the electronic discovery was completed.⁴¹ The court's order granting the motion to compel provided that the plaintiffs' technical expert would "inspect the Defendants' computer system to assess whether any changes have been made to hinder the ESI production" and also examine the defendants' preservation

28. *John B.*, 531 F.3d at 452.

29. *Id.*

30. *Id.* at 453.

31. *Id.*

32. *Id.*

33. *Id.*

34. *John B.*, 531 F.3d at 453.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.* at 454.

39. *Id.*

40. *John B.*, 531 F.3d at 454.

41. *Id.*

procedures to determine whether previous orders had been honored.⁴² As a result, the parties debated over what the scope of the original orders were, as the passage of time made proof of compliance difficult, and requested clarification as to the most current orders.⁴³

Finally, the plaintiffs asked the court to impose sanctions on the defendants for failure to comply with previous orders, and the plaintiffs also filed a motion to compel the defendants to obey the most recent discovery orders.⁴⁴ In response, the court issued the controversial orders central to this case, which permitted the plaintiffs' computer expert to "make forensic copies of any computer inspected to ensure the preservation of all existing electronically stored information ("ESI")."⁴⁵ Additionally, the court ordered a United States Marshal to accompany the computer expert to ensure compliance with the order.⁴⁶ The defendants contended that the order was broad and intrusive and requested limitations and clarification as to the boundaries of such an order.⁴⁷ The court clarified that the United States Marshal would maintain custody of the forensic images and further stated that the experts could make forensic images of personal as well as state-owned computers.⁴⁸ The defendants asked for and were granted an emergency stay from these orders, and the Sixth Circuit eventually granted mandamus relief from the forensic imaging order.⁴⁹

IV. ANALYSIS

The Sixth Circuit recognized that the district court's orders compelled the imaging of personal and state-owned computers, which would likely produce confidential and private data that was unrelated to the litigation.⁵⁰ The court examined five factors to determine whether mandamus relief was proper: (1) whether the petitioning party has any other satisfactory means of attaining the requested relief; (2) whether the petitioner will be damaged or prejudiced in a way that would not be correctable on appeal if the orders were permitted to stand; (3) whether the district court's orders are clearly erroneous as a matter of law; (4) whether the district court's orders are an error that is often repeated or is a persistent disregard of federal rules;⁵¹ and (5) whether the district court's orders raise new and important problems, or issues of law that are of first

42. *Id.*

43. *Id.* at 455.

44. *Id.*

45. *Id.*

46. *John B.*, 531 F.3d at 455.

47. *Id.* at 456.

48. *Id.*

49. *Id.*

50. *Id.* at 457.

51. The court did not address this factor in its analysis, so it likely did not apply to the facts. There is no evidence that there were any general issues with the district court's discovery orders. *See id.*

impression.⁵² Because the court determined that four of the five factors supported granting relief, the court approved mandamus relief and set aside the district court's orders allowing unrestricted forensic imaging.⁵³

The issues that the court examined when determining whether mandamus relief was appropriate are common to many other situations in which courts analyze requests to compel forensic imaging. These issues include privacy, confidentiality, privilege, responsiveness, suggested restrictions, other preservation methods available or already attempted, and the associated costs.

This section will follow the Sixth Circuit's reasoning in the *John B. v. Goetz* decision, and it will discuss some of the facts that are unique to this case and whether their absence would change the court's outcome. It also addresses other important factors courts have considered when determining whether to compel forensic imaging. Finally, it will examine the benefits of forensic imaging and suggest ways to utilize forensic imaging as a discovery tool while still protecting and respecting the parties' interests.

A. *The John B. v. Goetz Court's Analysis*

1. Other Means Available to Obtain Relief

Initially the court examined whether other satisfactory means were available to attain the requested relief.⁵⁴ The court stated that the imaging of computers automatically raised concerns of privacy and confidentiality because by design, duplication increases the possibility of inappropriate exposure.⁵⁵ Once the information is revealed, an appeal could not remedy the impact of disclosure: confidentiality cannot be restored nor privacy returned. Accordingly, the court determined that the immediate consequences resulting from compelling forensic imaging could not be corrected on appeal.⁵⁶

The court further recognized that discovery orders are usually not directly appealable because a party could force review of the order by refusing to comply and appealing if the district court decides to impose sanctions.⁵⁷ However, even if the petitioning party refuses to comply, the orders also apply to individuals not party to the litigation, so the petitioning party's refusal to comply would not

52. *John B.*, 531 F.3d at 457.

53. *Id.* at 461, 457.

54. *Id.* at 457. The court stated that mandamus relief may be used as a "means of immediate appellate review of orders compelling the disclosure of documents and information claimed to be protected from disclosure by privilege or other interests in confidentiality." *Id.* (quoting *United States ex rel. Pogue v. Diabetes Treatment Ctrs. of Am., Inc.*, 444 F.3d 462, 472 (6th Cir. 2006)).

55. *John B.*, 531 F.3d at 457. Logically, once a copy is made, the chances of disclosure are doubled, especially considering that at least one person (the expert) will be exposed to information that he should not otherwise see.

56. *Id.* at 457-58.

57. *Id.* at 458; *see also Dow Chem. Co. v. Taylor*, 519 F.2d 352, 354-55 (6th Cir. 1975) (explaining that discovery orders are generally not directly appealable).

prevent these individuals from obeying the orders and thus revealing the sensitive information.⁵⁸ The court recognized that while these alternatives may provide relief, they were not satisfactory.⁵⁹ Because the defendants were state officers, they had an interest in protecting the confidential state information and thus avoiding the imaging of any relevant computers.⁶⁰ Accordingly, an appeal from either sanctions or a contempt citation would be inadequate.⁶¹

Although the court's analysis is specific to the determination of mandamus relief, based on the facts of the situation and the law, the court decided correctly. Mandamus relief was the only way to ensure the protection of the sensitive information. As the court correctly noted, duplication automatically presents the opportunity for exposure of private or confidential information to parties that should not be privy to it. This initial concern with privacy and confidential information dominated the next section of the court's analysis and is central to courts examining motions to compel forensic imaging.

2. Damage or Prejudice

The court next addressed whether the party seeking to avoid the orders would be damaged or prejudiced in a way that was not correctable on appeal if the orders were permitted to stand.⁶² The court recognized that execution of the orders would inherently interrupt state business to some extent.⁶³ First, the expert would have to interrupt daily tasks performed on the computer in order to create the image, and second, the orders specified that a United States Marshal would accompany the expert.⁶⁴ Clearly, the act of the marshal escorting a computer expert would likely disrupt state business, especially considering the defendant's hostility to both the expert and the marshal.⁶⁵ Although the court expressed concern with the potential interruption, this apprehension was overshadowed by its distress with the privacy and confidentiality issues.⁶⁶ As discussed *infra*,⁶⁷ the court recognized the petitioning party's concern with an appeal's inability to correct the release of private or confidential information.⁶⁸ The court recognized that imaging state and personal computers would result in the replication of both private and confidential information, and that the risk of

58. *John B.*, 531 F.3d at 458.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*; see also *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999) (recognizing the producing party's concern that imaging would disrupt her business and cause financial losses. The court addressed this concern by requiring that imaging occur according to the producing party's schedule).

64. *John B.*, 531 F.3d at 458.

65. *Id.*

66. *Id.*

67. See *infra* Damage or Prejudice section (IV)(A)(2).

68. See generally *John B. v. Goetz*, 531 F.3d 448 (6th Cir. 2008).

exposure remained, even if the images were initially protected by court order.⁶⁹ These two issues were paramount in the court's analysis in determining whether the orders would cause damage or prejudice to the petitioning party.⁷⁰

Many other courts have expressed concerns with these issues, as well as privilege.⁷¹ Although the facts of each case influence the court's decision as to whether forensic imaging should be permitted, common themes appear for both the concerns raised by the petitioning parties and the court's resolution.

a. Privacy

As the court in *John B. v. Goetz* noted, forensic imaging by nature implicates privacy concerns,⁷² which are only magnified when personal computers are included in forensic imaging orders. Privacy is an issue that has become more significant as society has become more technologically advanced.⁷³ Technology has created many convenient solutions to every day problems, including transportation, communication, and document creation, revision, and storage. However, technology has also produced consequences, including increased identify theft resulting from the widespread availability of personal information.⁷⁴ With so much information used during online business transactions or stored on servers, hackers have more opportunities to obtain personal information.⁷⁵ Due to the increased number of security breaches, consumers and legislators have demanded strict security procedures and legislation outlining various data security and notification protocols.⁷⁶

Compelling unrestricted forensic imaging of personal computers implicates the concerns listed above. Many people store personal identifying information on their computer, including banking and financial information, social security

69. *Id.* at 458.

70. *Id.*

71. *See, e.g., In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003) (“The district court must protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs.”) (internal quotations omitted); *Menke v. Broward County Sch. Bd.*, 916 So. 2d 8, 11 (Fla. Dist. Ct. App. 2005) (acknowledging “that unlimited access to anything on the computer would constitute irreparable harm, because it would expose confidential, privileged information to the opposing party”) (citing *Strasser v. Yalamanchi*, 669 So. 2d 1142 (Fla. Dist. Ct. App. 1996)).

72. *John B.*, 531 F.3d at 458.

73. *See generally* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109 (2008) (recognizing that the internet has produced more possibilities for collecting, storing, and exchanging information, and thus has motivated an increased interest in privacy protection).

74. *Id.* at 123-24 (describing two types of identity theft: “new account” fraud which claims 3.23 million victims and “existing account” fraud, which occurs when the thief commits other offenses by using the victim's identity, and affects 6.7 million people).

75. *See id.* at 121 (explaining that outside hackers cause 19% of all security breaches).

76. *See id.* at 119-20. For example, California has implemented a law that requires businesses to notify consumers whose information was compromised due to a security breach. *See* CAL. CIV. CODE § 1798.84(b).

numbers, and tax information. Improperly disclosed information, specifically social security numbers, can lead to identity theft because such information can be used to open new accounts.⁷⁷ By allowing unrestricted forensic imaging of personal computers, third parties are permitted to create and store a copy of this private information completely out of the individual-owner's control and without her consent. Although many forensic imaging experts likely have data security protocols in place, the chance of the data becoming exposed is now doubled simply because a copy exists. It seems unfair to risk exposure of this data, especially when such personal information is generally irrelevant to the litigation.⁷⁸

Additionally, allowing personal data to be copied is an invasion of privacy.⁷⁹ Personal information is often stored on personal computers. Rule 26(b)(1) defines the scope of discovery as any information relevant to the claim or defense.⁸⁰ Personal information copied simply because it is stored on the party's computer and not because of its relevance is outside the scope of discovery.⁸¹ Compelling the imaging of such information amounts to an invasion of privacy, not a furtherance of the discovery process. Accordingly, the court in *John B. v. Goetz* correctly decided to set aside the order requiring unrestricted forensic imaging.

b. Confidentiality

The court also examined the potential exposure of confidential and proprietary information not related to the litigation.⁸² The discovery orders applied to the computers of high ranking state officials, and therefore, imaging would likely produce information relating to classified state matters.⁸³ Other courts have also focused on the issue of proprietary information such as trade secrets and business information.⁸⁴ It is important to recognize, as these courts have, that a company's trade secrets, customer lists, and other proprietary

77. Beales & Muris, *supra* note 73, at 123-25 (discussing "new account" fraud, which is a type of identity theft).

78. The goal of forensic imaging should be to preserve discoverable information, that is, information relating to litigation. *See* FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party.").

79. *See* Menke v. Broward County Sch. Bd., 916 So. 2d 8, 10 (Fla. Dist. Ct. App. 2005) (stating that the expert's examination arguably constitutes a significant invasion of privacy).

80. FED. R. CIV. P. 26(b)(1).

81. *See id.*

82. *John B. v. Goetz*, 531 F.3d 448, 460-61 (6th Cir. 2008).

83. *Id.* at 460.

84. *See, e.g.,* Orrell v. Motorcarparts of Am. Inc., Civil No. 3:06DV418-R, 2007 WL 4287750, at *9 (W.D.N.C. Dec. 5, 2007) (responding to producing party's concern regarding exposure of proprietary business information by confining the forensic imaging to certain non-business computers); Strasser v. Yalamanchi, 669 So. 2d 1142, 1144-45 (Fla. Dist. Ct. App. 1996) (recognizing the producing party's concern that unrestricted forensic imaging, which would include imaging proprietary records including patient files, would violate patient confidentiality).

information are necessary for its survival, and as such, should be protected. Most courts have addressed this concern either by preventing unrestricted forensic imaging or by instituting a protocol to limit the imaging.⁸⁵ Therefore, the court in *John B. v. Goetz* properly determined that proprietary information requires protection, and accordingly set aside the district court's orders allowing unrestricted forensic imaging.⁸⁶

c. Privilege

Although privilege was not an issue in *John B. v. Goetz*, another significant concern during discovery is protection of attorney-client privilege.⁸⁷ As discovery has evolved to include ESI, this issue has become even more important.⁸⁸ Because storage space and cost requirements are minimal, more documents are being retained electronically.⁸⁹ Traditionally, inadvertent waiver occurred when privileged documents were accidentally included with other documents sent in response to a discovery request.⁹⁰ Inadvertent waiver occurs similarly in the production of ESI, but the problems stemming from traditional inadvertent waiver are magnified in the e-discovery context.⁹¹

The number and format of documents stored causes difficulties with privilege review and production. As mentioned above, more documents are stored electronically than would be physically stored, so more information must be reviewed when responding to discovery requests.⁹² In addition to the sheer quantity of documents, information is stored in multiple forms and may need to be converted into a readable or searchable format.⁹³ These characteristics of ESI make the identification of privileged documents more difficult, escalating the time required and cost of privilege review, as well as increasing the probability that a privileged document may inadvertently be produced.⁹⁴ Accordingly,

85. See *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 649-54 (D. Minn. 2002). This case involved a copyright infringement claim, and the plaintiff moved to compel forensic imaging of the defendant's hard drive, claiming that the defendant was destroying information. *Id.* at 650-51. The court outlined a protocol to protect these concerns by implementing appropriate limitations such as allowing the defendant's counsel to review the image and submitting only responsive documents. *Id.* at 653-54. But see *Frees v. McMillan*, No. 05-1979, 2007 WL 184889, at *5 (W.D. La. Jan. 22, 2007) (stating that because the disputed technology is unique and not easily understood, the requesting party must have access to the documents because his counsel would not have the necessary expertise to decipher the information).

86. *John B.*, 531 F.3d at 461.

87. See *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228, 231-32 (D. Md. 2005).

88. *Id.*

89. *Rowe Entm't, Inc. v. William Morris Agency*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002).

90. *Hawkins v. Anheuser-Busch, Inc.*, No. 2:05-cv-688, 2006 WL 3230756, at *1 (S.D. Ohio June 19, 2006).

91. *Hopson*, 232 F.R.D. at 232.

92. *Id.*

93. *Id.*

94. *Id.*

concern with inadvertent disclosure will motivate attorneys to spend more time and manpower reviewing documents, which ultimately increases the total costs to the client.⁹⁵

The inadvertent production of privileged documents, regardless of the reason, may lead to waiver of privilege for all other privileged documents relating to that subject matter.⁹⁶ Courts apply three different methods to determine whether waiver has occurred: the “strict approach,” the “lenient approach,” and the “balancing approach.”⁹⁷

The courts applying the “strict approach” method will almost always determine that a waiver has occurred, reasoning that “once confidentiality is lost, it can never be restored.”⁹⁸ Under the “strict approach,” should a court compel unrestricted forensic imaging of the opposing party’s computer, any privileged documents imaged would be deemed inadvertently waived, and additionally, any other documents related to the subject matter would also lose protection. The ramifications of such an order could be devastating to a case, and although this is the consequence in theory, it is unlikely that any court would enforce such harsh results.

Courts applying the “lenient approach” rarely find waiver, reasoning that attorneys are only human and thus make mistakes.⁹⁹ To find that waiver occurred, these courts require evidence showing that the producing party intended to waive privilege, or did so knowingly.¹⁰⁰ Under the “lenient approach,” compelling unrestricted forensic imaging would have almost no effect, because the production of privileged documents would be the result of an order, and establishing the required intent to waive privilege would be virtually impossible.

Courts applying the “balancing approach” weigh five factors to determine whether the actions that resulted in production should be excused and the privilege protected.¹⁰¹ Courts that use this technique typically examine: (1) the reasonableness of the precautions taken to prevent the disclosure; (2) the number of disclosures contained within the discovery responses; (3) the extent of the materials or information disclosed; (4) any delay in attempting to correct the disclosure; and (5) any underlying principles of justice.¹⁰² The effect of

95. *Id.*

96. *Id.* at 235-36.

97. *Hopson*, 232 F.R.D. at 235-36.

98. *Id.* at 235 (recognizing that the First and Federal Circuits follow the “strict approach”).

99. *Id.* at 235-36 (acknowledging that the lenient approach is followed by the Eighth Circuit and some district courts).

100. *Id.* at 236.

101. *Id.* (recognizing that this approach is followed by district courts within the Fourth Circuit).

102. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 259 (D. Md. 2008). This case employed the balancing test, determining that waiver did occur because the producing party could not prove that its conduct was reasonable. *Id.* at 262. In this situation the only precaution taken to prevent waiver was a simple keyword search that resulted in production of 165 privileged documents. *Id.* at 254-60.

compelling unrestricted forensic imaging under the “balancing approach” is more uncertain. The result of this test depends heavily on the facts, but when considering that the order to compel forensic imaging is likely the result of the producing party’s failure to comply with previous requests, the test could be resolved in favor of waiver.¹⁰³

Although the court in *John B. v. Goetz* did not discuss privilege concerns, many other courts have cited concern with privilege waiver as a reason for their decision either not to compel forensic imaging or to limit it.¹⁰⁴ As one court noted, indiscriminate access to the producing party’s computer could expose privileged correspondence relating to the issues central to the litigation.¹⁰⁵ This statement represents the concern of each court as it considers whether to compel forensic imaging, and why so many courts have correctly refused to allow unrestricted imaging either by denying a motion to compel or by outlining a protocol that provides limitations and safeguards to protect against waiver.

3. Clearly Erroneous

Next, the *John B. v. Goetz* court examined the third mandamus factor and correctly determined that the district court’s orders were clearly erroneous as a matter of law.¹⁰⁶ The court recognized that district courts usually have expansive discretion in discovery issues, but that here, orders requiring forensic imaging of all computers potentially storing responsive ESI constituted an abuse of discretion.¹⁰⁷ The court first stated that generally, the parties have the obligation to preserve all relevant information, including ESI, whenever they become aware that the information may be required for future litigation.¹⁰⁸ Should parties fail

103. For example, when examining the first factor, which focuses on the reasonableness of precautions taken to avoid disclosure, a court may decide that few precautions were taken by the producing party because if the party had only responded to such requests in a timely fashion, it could have had the opportunity to conduct a thorough privilege review. The next two factors depend on the facts because they analyze the number and extent of the disclosures. The fourth factor, however, which examines the delay in attempting to rectify any disclosures could also weigh in favor of waiver depending on the judges. A judge could reason that the delay to attempt to correct waiver began when the producing party failed to timely respond to the requests, because by failing to respond the party failed to take reasonable steps such as initially reviewing for privilege. Finally, the last factor will depend on the facts of the case and the competing interests in the judge’s mind. Admittedly, the above hypothetical may be a bit extreme, but it is a possible effect of compelling unrestricted forensic imaging.

104. *See, e.g., In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003) (recognizing that unrestricted imaging gives the requesting party access to documents that are not discoverable, including privileged information); *Thielen v. Buongiorno USA, Inc.*, No. 1:06-CV-16, 2007 WL 465680, at *2 (W.D. Mich. Feb. 8, 2007) (noting that allowing inspection of the opposing party’s computer may reveal privileged or proprietary documents).

105. *Menke v. Broward County Sch. Bd.*, 916 So. 2d 8, 10 (Fla. Dist. Ct. App. 2005) (granting relief from unrestricted forensic imaging because of concerns of invasion of privacy and privilege).

106. *John B. v. Goetz*, 531 F.3d 448, 458-59 (6th Cir. 2008).

107. *Id.*

108. *Id.* at 459.

to preserve such information, courts may exercise their authority to impose appropriate sanctions.¹⁰⁹ *The Sedona Principles* suggest that courts should impose sanctions only when they find that a party had an affirmative duty to preserve information, which it failed to do, and a reasonable probability exists that the failure will prejudice the opposing party in some way.¹¹⁰ The court continued, stating that it was unclear whether courts could compel unrestricted forensic imaging and production of information in order to preserve ESI, as the district court did here, and that if permitted, such practices should be used in limited circumstances.¹¹¹ The court recognized that while forensic imaging is not uncommon, courts have been cautious when requests are broad and only a tenuous connection exists between the computers and the claim.¹¹² The court explained that mere skepticism that the opposing party has not produced all information is not sufficient to warrant such drastic and intrusive electronic discovery methods.¹¹³ *The Sedona Principles* also urge caution in using and compelling forensic imaging.¹¹⁴

The court stated that although forensic imaging is a useful and generally accepted tool, it is not always appropriate and should not be applied to all situations.¹¹⁵ The court advised that when considering whether to compel imaging, courts should weigh the underlying interests of the situation with the purposes of the imaging, which the district court failed to do.¹¹⁶ The court recognized that while the risks relating to disclosure of privacy, confidentiality, and privilege alone do not prohibit forensic imaging, good cause must be present to subordinate these concerns and compel the imaging.¹¹⁷ The court stated that although the district court found that the defendants failed to comply with discovery orders, there was no evidence in the record to show that the defendants

109. *Id.* at 459-60. *See also* FED. R. CIV. P. 37.

110. THE SEDONA PRINCIPLES, *supra* note 5, at 70 (discussing that sanctions are usually based on the party's culpability). The Sedona Conference Working Group consists of participants who create recommendations and guidelines focused on confronting challenging legal issues. *Id.* at 71. The Sedona Conference played an important role in amending the Federal Rules of Civil Procedure to address e-discovery and continues to work to define other legal areas. *Id.* at 6.

111. *John B.*, 531 F.3d at 459 (recognizing that here, the district court ordered the forensic imaging primarily for preservation purposes because of the defendant's repeated failure to comply with the court's orders by producing the ESI).

112. *Id.* at 459-60; *see also* *Balboa Threadworks, Inc. v. Stucky*, No. 05-1157-JTM-DWB, 2006 WL 763668, at *3 (D. Kan. March 24, 2006) (noting that courts are more hesitant to grant a request when it is broad).

113. *John B.*, 531 F.3d at 460.

114. THE SEDONA PRINCIPLES, *supra* note 5, at 34, 47 (recognizing that imaging should only be permitted in "exceptional circumstances" and that it should always include a protocol to protect privacy, confidentiality, and privilege).

115. *John B.*, 531 F.3d at 460.

116. *Id.* (reiterating the issues of privacy and confidentiality implicated by the district court's order to image both personal and state owned computers that almost certainly contain private and confidential information unrelated to the litigation).

117. *Id.*

intentionally destroyed data or were unwilling to produce information.¹¹⁸ The court then recognized that forensic imaging was not the only method available to respond to the defendant's misconduct, for example, the court could impose monetary sanctions or order a less intrusive method of discovery.¹¹⁹ The court also expressed concern with the use of a United States Marshal and the forced imaging of state officials' computers, because both measures implicated issues of federalism and comity not usually present in civil litigation, which were not proper under these facts.¹²⁰ The court concluded that because other less intrusive means of preservation were available, unrestricted imaging was not appropriate.¹²¹

The court correctly decided that good cause should be shown before forensic imaging is permitted. Courts should require an affirmative showing of substantial noncompliance or unresponsiveness before considering unrestricted forensic imaging, and even such evidence does not automatically permit unrestricted forensic imaging.¹²² Mere skepticism or concern should not be sufficient. Rather, specific examples of noncompliance, such as evidence that the producing party was destroying information or failing to implement preservation mechanisms, should be required before a court should consider compelling forensic imaging.¹²³ Otherwise one party could request forensic imaging on the simple assertion that the opposing party was not responsive, which would allow parties to use forensic imaging as a "fishing expedition" in an attempt to gather information.¹²⁴ Rule 34(a) allows the requesting party to inspect and copy information produced during discovery, but it does not permit unlimited, direct access to the producing party's databases.¹²⁵ If computer hard drives are analogous to filing cabinets,¹²⁶ unrestricted forensic imaging is

118. *Id.*

119. *Id.* at 460-61.

120. *Id.* at 461.

121. *John B.*, 531 F.3d at 460-61.

122. *See, e.g.*, *Calyon v. Mizuho Secs. USA, Inc.*, No. 07 Civ. 02241, 2007 U.S. Dist. LEXIS 36961, at *16 (S.D.N.Y. May 18, 2007) (denying a motion to compel unrestricted forensic imaging because there was no showing that the producing party failed to produce responsive documents); *Balfour Beatty Rail, Inc. v. Vaccarello*, No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3 (M.D. Fla. Jan. 18, 2007) (refusing to grant a motion to compel because there was no evidence that the producing party had not complied with discovery requests, nor did the requesting party specify what information it hoped to obtain from the hard drives); *Strasser v. Yalamanchi*, 669 So. 2d 1142, 1145 (Fla. Dist. Ct. App. 1996) (stating that even if the producing party was unresponsive, unrestricted forensic imaging would not be proper).

123. *McCurdy Group, LLC v. Am. Biomedical Group, Inc.*, 9 Fed. App'x. 822, 831 (10th Cir. 2001) (refusing to permit such drastic measures as forensic imaging because of unsubstantiated concern with responsiveness).

124. *Balfour Beatty Rail, Inc.*, 2007 WL 169628, at *3 (noting that allowing a requesting party access to the producing party's hard drives would allow the requesting party to conduct a "fishing expedition").

125. FED. R. CIV. P. 34(a). *See also* *In re Ford Motor Co.*, 345 F.3d 1315, 1316 (11th Cir. 2003).

126. *See* *Menke v. Broward County Sch. Bd.*, 916 So. 2d 8, 10 (Fla. Dist. Ct. App. 2005).

comparable to requiring the producing party to provide its entire filing cabinet to the requesting party, which is absurd. Also, because of its intrusiveness, forensic imaging should be used only as a last resort.¹²⁷ Accordingly, based on the Sixth Circuit's analysis and conclusion, it correctly decided that the district court's orders were clearly erroneous as a matter of law.

4. Important Matters of Law

The court examined the fifth mandamus factor and determined that the district court's orders impacted the important issues of electronic discovery and forensic imaging.¹²⁸ These orders effectively granted unrestricted imaging of a party's computers without requiring evidence of bad faith destruction of information. These orders, if allowed to stand, would significantly expand discovery and subordinate privacy, confidentiality, and privilege concerns. These orders also implicated issues of federalism and comity, and although such concerns are not typically present in civil litigation, addressing the impropriety of the orders was important.¹²⁹ Because four of the five factors supporting mandamus relief weighed in the defendant's favor, the court correctly granted relief and set aside the district court's orders compelling unrestricted forensic imaging.¹³⁰

B. Facts Unique to *John B. v. Goetz*

Two facts unique to *John B. v. Goetz* may have affected the Sixth Circuit's decision. First, because the defendants were state officials, unrestricted imaging would expose state proprietary information.¹³¹ Second, the orders required a United States Marshal to accompany the computer expert during the imaging process.¹³² While both of these facts were relevant to the court's analysis, neither dominated the court's decision.

First, as previously discussed, because the defendants were state officials, the computers imaged would likely contain highly confidential, state proprietary information.¹³³ The court believed protecting state proprietary information was important to its decision to set aside the orders compelling unrestricted forensic imaging, but it was not the central reason. Existence of state proprietary information is analogous to the existence of business proprietary information

127. See THE SEDONA PRINCIPLES, *supra* note 5, at 47.

128. *John B. v. Goetz*, 531 F.3d 448, 461 (6th Cir. 2008).

129. *Id.* (stating that use of federal law enforcement officers in this situation was improper).

130. *Id.*

131. *Id.* at 448, 461. The defendants in this case were various state officers, including the Commissioner of the Tennessee Department of Finance and Administration, the Assistant Commissioner of the Bureau of TennCare, and the Commissioner of the Tennessee Department of Children's Services.

132. *Id.* at 461.

133. *Id.* at 460-61.

stored on company computers. Courts have repeatedly recognized the need for protection of trade secrets and other business proprietary information, and these concerns have influenced their decisions to restrict forensic imaging.¹³⁴ Although the court wanted to protect state proprietary information here, courts have also protected business proprietary information in other instances,¹³⁵ suggesting that the protection of any type of proprietary information is important. Accordingly, the fact that the proprietary information was related to state matters was not the only reason for the Sixth Circuit's decision to set aside the orders.

Second, although the orders' use of a federal law enforcement officer supported the Sixth Circuit's decision to set aside the orders, it was not the primary reason for the court's conclusion. The court discussed the use of federal law enforcement officers during its examination of the third factor of mandamus relief, which examined whether the district court's orders were clearly erroneous as a matter of law.¹³⁶ During this section of its analysis, the court focused on the lack of evidence supporting the need for forensic imaging, the privacy and confidentiality concerns, and the use of a United States Marshal.¹³⁷ The use of a federal law enforcement officer was mentioned last and discussed only briefly. While it supported the court's rationale and decision, the brevity of the discussion does not suggest that it was the basis for the decision. Accordingly, if the order did not require the use of a marshal, based on its discussion of the lack of evidence supporting the need to compel forensic imaging, as well as the concerns of privacy and confidentiality, the court would still have decided to set aside the orders.¹³⁸

Based on the above analysis, the absence of these unique facts would not have changed the court's decision because neither fact was the cornerstone of the court's analysis. These facts clearly supported the court's conclusion, but neither was the paramount reason for the court's decision. Therefore, the Sixth Circuit seems to have limited the breadth of discovery through its decision not to compel forensic imaging.

134. *See, e.g.*, Orrell v. Motorcarparts of Am. Inc., 2007 WL 4287750, at *9 (W.D.N.C. Dec. 5, 2007) (responding to producing party's concern regarding exposure of proprietary business information by confining the forensic imaging to certain non-business computers); Strasser v. Yalamanchi, 669 So. 2d 1142, 1144-45 (Fla. Dist. Ct. App. 1996) (recognizing the producing party's concern that unrestricted forensic imaging, which would include imaging proprietary records including patient files, would violate patient confidentiality).

135. *See supra* note 134 and accompanying text.

136. John B. v. Goetz, 531 F.3d 448, 461 (6th Cir. 2008).

137. *Id.* at 460-61. The court discussed that affirmative evidence of a party's failure to preserve information or of its destruction of information is usually required before forensic imaging should be compelled, neither of which could be found in the record. *Id.* at 460. Additionally, the court reiterated concerns relating to the privacy issues implicated by imaging personal computers, as well as the confidentiality issues implicated by the imaging of state officials' computers. *Id.* at 461.

138. *Id.* at 461.

C. An Important Factor to Consider: Cost

Another distinction of *John B. v. Goetz*, as compared to other forensic imaging cases, is that cost was not a concern and therefore not analyzed by the court. Because these costs can be staggering, many courts address this issue when examining whether to compel forensic imaging.¹³⁹ The presumption as to cost allocation is that the producing party pays the costs for retrieving and producing responsive information because in theory, that party controls how many records it keeps, as well as how the information is stored.¹⁴⁰ However, because of the evolution of technology and the increasing popularity of electronic storage, this premise is no longer valid.

Parties retain more information than ever before, primarily because of the low costs and ease of electronic storage.¹⁴¹ In the past, information was printed on hard copy documents, which were then boxed and stored. Storage of these boxes was expensive because of the space required, and therefore, parties would regularly review the information kept in these boxes to determine which documents should be kept and which could be destroyed. However, now that documents are stored on a computer hard drive or server, a party may be less motivated to destroy unnecessary documents.¹⁴² The increased number of stored documents now leads to more production during litigation, which increases the ultimate cost of discovery.

Rule 26(b)(2)(C) allows courts to protect the producing party from undue burden or expense during discovery by either preventing production or shifting the costs.¹⁴³ Courts engage in a benefit/burden analysis, which weighs the expected value of the information produced with the costs of production.¹⁴⁴ If

139. See *Citizens for Responsibility and Ethics in Washington v. Executive Office of the President*, No. 07-1707 (HHK/JMF), 2008 WL 2932173, at *3 (D.D.C. July 29, 2008); *Cenveo Corp. v. Slater*, No. 06-CV-2632, 2007 WL 442387, at *1-2 (E.D. Pa. Jan. 31, 2007); *Rowe Entm't, Inc. v. William Morris Agency*, 205 F.R.D. 421, 428-33 (S.D.N.Y. 2002) (all recognizing the costs of forensic imaging and comparing the costs with the expected benefit).

140. *Rowe Entm't, Inc.*, 205 F.R.D. at 429 (stating that by choosing to store information electronically, the costs associated with retrieving the information in a readable format are foreseeable).

141. *Id.* (“Information is retained not because it is expected to be used, but because there is no compelling reason to discard it.”).

142. *Id.*

143. *Cenveo Corp.*, 2007 WL 442387, at *1 (acknowledging that the court may limit discovery if: “(i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues”).

144. *Rowe Entm't, Inc.*, 205 F.R.D. at 429.

the anticipated benefits outweigh the burdens, then production will likely be compelled, although the court may shift costs if appropriate.¹⁴⁵

Courts typically examine eight factors when applying the benefit/burden test.¹⁴⁶ The first factor examines the specificity of the discovery requests, and usually, the broader the request, the more likely the court will shift the cost or refuse to compel production.¹⁴⁷ The second factor analyzes the likelihood of discovering key information, and if the requesting party fails to provide evidence that the discovery request will likely produce useful information, that party should bear the expense.¹⁴⁸ The third factor examines the possibility of obtaining the relevant information from other less expensive sources.¹⁴⁹ The fourth factor looks at the purpose of the producing party's retention of the information, and if the information is used often and easily accessible, the producing party will likely pay.¹⁵⁰ The fifth factor analyzes the benefit to the producing party, and if it would likely benefit from the production, then that party should logically bear the expense.¹⁵¹ After all, if the producing party would have produced the information in support of its own claim or defense, there is no purpose in shifting the cost to the requesting party. The sixth factor looks at the total costs of the requested production, and if the costs are not substantial, there may not be a reason to shift them.¹⁵² The seventh factor weighs the ability of the parties to control the costs associated with production.¹⁵³ Courts will sometimes allocate costs to the party that controls the extent of the discovery to ensure that the production occurs as efficiently as possible.¹⁵⁴ The

145. *Id.* at 429-32.

146. *Id.* at 429 (employing the balancing test to determine whether to shift costs and deciding that the costs should be shifted to the requesting party).

147. *Id.* at 429-30 (stating that when a "party multiplies litigation costs by seeking expansive rather than targeted discovery, that party should bear the costs").

148. *Id.* at 430 (recognizing that this method of allocation should deter frivolous discovery requests); *see also* McPeck v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) ("The more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the [responding party] search at its own expense. The less likely it is, the more unjust it would be to make [that party] search at its own expense.").

149. *Rowe Entm't, Inc.*, 205 F.R.D. at 430 (discussing that discovery may be denied or costs shifted if the same information can be accessed from a less expensive source or in a more accessible format).

150. *Id.* at 430-31. If the producing party maintains the information for everyday use, it is likely easy to access and produce, and that party will likely bear the cost of production. *Id.* However, if the producing party retains it for no identifiable purpose, maybe simply because it has failed to discard it or has kept it for emergency purposes, the requesting party would likely have to pay for production. *Id.* at 431. Backup tapes, for example, would fall into this latter category. *Id.*

151. *Id.* at 431.

152. *Id.*

153. *Id.* at 431-32.

154. *Id.* at 432 (stating that when the "discovery process is going to be incremental, it is most efficient to place the burden on the party that will decide how expansive the discovery will be").

final factor considers the parties' resources in relation to the costs of production.¹⁵⁵

Forensic imaging can be very costly, even for relatively minor imaging.¹⁵⁶ Obviously, the costs of imaging are directly related to the amount of information imaged. Unrestricted imaging entails copying all files stored on a hard drive, and as discussed above, more data is now stored electronically. If the presumption as to cost allocation is followed in the context of forensic imaging, the producing party would have to pay for the imaging of an entire hard drive, including information that is irrelevant to the litigation, and these costs may be over burdensome. Therefore, the court should carefully weigh the factors from above, and in most instances, the principles of fairness would seem to require that the requesting party should bear the costs associated with the imaging.¹⁵⁷

D. Forensic Imaging as a Tool

Forensic imaging, when used properly, can be a valuable tool to aid in the discovery process. It acts like a camera, taking a picture of the designated segments of a computer hard drive, and preserving the information.¹⁵⁸ The information stored on a computer changes constantly, as data is written over or destroyed during daily use.¹⁵⁹ Accordingly, forensic imaging can allow parties to preserve the information as required for litigation purposes without depriving them of use of their computers.

155. *Rowe Entm't, Inc.*, 205 F.R.D. at 432 (acknowledging that even a modest costs can consume all of one party's resources, which may justify shifting the costs to the other party).

156. *See* *Citizens for Responsibility and Ethics in Washington v. Executive Office of the President*, No. 07-1707 (HHK/JMF), 2008 WL 2932173, at *3 (D.D.C. July 29, 2008) (recognizing that the expected benefits do not outweigh the costs of imaging: "the typical cost of forensic imaging a 100GB hard drive is between \$400 and \$1,000 and it takes approximately two to three hours to complete the imaging").

157. When the factors are weighed, a party requesting unrestricted forensic imaging should bear the costs. Here, unrestricted forensic imaging contains no specificity because it requires the indiscriminate imaging of the entire hard drive. Additionally, it is not possible to know whether the search would be successful, nor if the information could be recovered from another source because unrestricted imaging does not target specific information, it targets all of it. Also, as discussed above, a party stores a substantial amount of information on hard drives, and it is likely that some of the information imaged would not be stored for business reasons. Yet, the producing party would be required to pay the costs of production for all the information, even if it is unrelated to the litigation. Additionally, the producing party does not stand to benefit from unrestricted forensic imaging, especially considering the dangers of privacy, confidentiality, and privilege discussed. *See supra* Damage or Prejudice section (IV)(A)(2); *see also supra* Clearly Erroneous section (IV)(A)(3). Finally, the costs are very high, and the requesting party could control these costs by outlining a limited request for forensic imaging, as opposed to unrestricted access. Therefore, the costs should be shifted to the requesting party.

158. *Balboa Threadworks, Inc. v. Stucky*, No. 05-1157-JTM-DWB, 2006 WL 763668, at *3 (D. Kan. March 24, 2006) (recognizing that forensic imaging assures preservation of information, which can be difficult to do considering how easily information can be erased).

159. *See* *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 650-51 (D. Minn. 2002) (acknowledging that data stored on the hard drive is overwritten during the every day use of the computer).

However, forensic imaging poses some dangers. To effectively protect the concerns discussed above, forensic imaging should only be permitted if either the parties or the court outlines appropriate limitations prior to the imaging. Parties should use pretrial conferences to outline a mutually agreeable strategy containing potential solutions to protect these concerns. Additionally, should the court decide to compel forensic imaging, it should outline its own protocol to address privacy, confidentiality, and privilege. If these safeguards and protocols are used, most of the parties' concerns should be alleviated.

1. Potential Solutions to Address Privacy, Confidentiality, and Privilege Concerns

As discussed above, the request for relief in *John B. v. Goetz* was for writ of mandamus, and by granting the petition, the court set aside the district court's orders.¹⁶⁰ Thus, the Sixth Circuit did not have the opportunity to outline solutions to the issues of privacy, confidentiality, and privilege. However, courts can and have used potential solutions to the above mentioned concerns.¹⁶¹ These solutions include instituting protective orders, allowing the producing party the right to review the image before the requesting party receives it, utilizing search terms, and creating and accepting claw back agreements. When used properly, many courts agree that such precautions will protect against disclosure of private and confidential information, as well as privilege waiver.¹⁶²

a. Protective Order

The first potential solution to address the concerns listed above is for the court to institute a protective order.¹⁶³ If constructed properly, the order can address privacy and confidentiality concerns, as well as prevent inadvertent privilege waiver. The order can prevent any documents seen by opposing counsel from constituting a waiver of privilege or breach of confidentiality, and the order can also prohibit the expert from revealing any information observed

160. *John B. v. Goetz*, 531 F.3d 448, 461 (6th Cir. 2008).

161. *See generally Antioch Co.*, 210 F.R.D. at 653-54; *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-42 (S.D. Ind. 2000); *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1054-55 (S.D. Cal. 1999).

162. *See, e.g., Equity Analytics v. Lundin*, 248 F.R.D. 331, 334 (D.D.C. 2008) (stating that by adopting a claw back agreement into an order, judicially compelled disclosure would not act as a waiver); *Simon Prop. Group, L.P.*, 194 F.R.D. at 641-42 (allowing the producing party to review documents for privilege before the requesting party receives them); *Playboy Enters., Inc.*, 60 F. Supp. 2d at 1054-55 (declaring that because the expert was an officer of the court and subject to a protective order, no waiver of privilege could occur); *Etzion v. Etzion*, 796 N.Y.S.2d 844, 846-47 (N.Y. Sup. Ct. 2005) (outlining a protocol to generally protect privacy and privilege concerns).

163. *See Balboa Threadworks, Inc.*, 2006 WL 763668, at *4-5 (recognizing that confidentiality could be protected through a protective order and use of search terms).

during the imaging process.¹⁶⁴ Finally, the order can punish anyone who violates it by holding them in contempt of court.¹⁶⁵ In addition to instituting a protective order, a court can also make the computer expert an officer of the court, and thus a neutral party, which also prevents privilege waiver.¹⁶⁶

However, these two safeguards may not adequately address all concerns relating to privacy, confidentiality, and privilege.¹⁶⁷ Depending on the circumstances, the requesting party will likely pay the expert, which creates the appearance of an employer/employee relationship, which arguably instills a sense of loyalty in the computer expert. The producing party may be concerned with the safety of imaged information in the hands of a paid employee of the requesting party.¹⁶⁸ Therefore, some danger that private, confidential, or privileged information may be disclosed exists. The magnitude of this risk depends on how well the computer expert understands her duty and responsibilities under the protective order and her respect of the legal system. Although the hope is that she will remain neutral under the protective order, the possibility that disclosure may occur should be recognized.

b. Opportunity to Review

Another potential solution is to allow the producing party to review the image before disclosure to the requesting party so that the attorneys provide only responsive, unprivileged documents.¹⁶⁹ Although the process of reviewing should prevent the disclosure of private, confidential, and privileged documents unrelated to the litigation, this is not a complete solution for two reasons. First, the expert is still exposed to these documents while she images the hard drive, which may constitute an invasion of privacy.¹⁷⁰ Additionally, because the expert may be exposed to confidential information while imaging the hard drive, a breach of confidentiality may still occur. Finally, waiver of privilege may be prevented depending on whether the court has instituted a protective order.

Second, even though the producing party's counsel has the opportunity to review for privilege, the possibility of inadvertent waiver still exists. Because of

164. See *In re Honza*, 242 S.W.3d 578, 583-84 (Tex. Ct. App. 2008) (providing that the order protected both confidentiality and privilege and prohibited the requesting party from later asserting a waiver claim or using any revealed data).

165. See *id.*

166. See *Simon Prop. Group L.P.*, 194 F.R.D. at 641; *Playboy Enters., Inc.*, 60 F. Supp. 2d at 1054-55.

167. See *Menke v. Broward County Sch. Bd.*, 916 So. 2d 8, 10 (Fla. Dist. Ct. App. 2005) (acknowledging the producing party's concern that any confidential or privileged communications would be revealed to the opposing party's paid representative).

168. *Id.*

169. *Ameriwood Indus., Inc. v. Liberman*, No. 4:06CV524-DJS, 2006 WL 3825291, at * 6 (E.D. Mo. Dec. 27, 2006) (recognizing that allowing the producing party to review for responsive documents should alleviate privacy and privilege concerns).

170. See *Menke*, 916 So. 2d at 10 (stating that the expert's examination arguably constitutes a significant invasion of privacy).

the time constraints of discovery, the producing party has a short time between when the image is created and production to the requesting party. Therefore, the inherent issues relating to inadvertent waiver are still an issue, including the possibility that privileged documents may be accidentally produced.¹⁷¹ The breadth of the imaging request will significantly affect the number of documents copied, and accordingly, the necessary review time. Because unrestricted forensic imaging of an entire hard drive would produce a substantial number of documents, each of which must be reviewed, it becomes even more probable that inadvertent disclosure may occur. This review process would also force the producing party to review each and every document stored on an entire hard drive, drastically increasing the costs and time associated with production.

Although allowing the producing party to review the image before the requesting party receives it will address some of the privacy, confidentiality, and privilege concerns, it clearly cannot act as a complete solution. Thus, it should be used in conjunction with other methods discussed in this section.

c. Search Terms

Next, the parties can agree to certain terms that the computer expert will use to search for responsive documents to be imaged.¹⁷² While recognized as a good tool to narrow the number of potentially responsive documents on a hard drive, inherent limitations and risks should be recognized.¹⁷³ One of these limitations is that the results may be over or under inclusive primarily because of the vagueness of the English language.¹⁷⁴ For example, many words or word combinations can be used to describe the same concept, and it is virtually impossible to account for them all in a search. Additionally, search terms may not account for misspellings or abbreviations within the documents, and pronouns are often used to reference terms the key words are attempting to retrieve.

For search terms to be used successfully, attorneys should confer with experts to develop a protocol to capture as many responsive documents as possible.¹⁷⁵ Additionally, it is important to critically think about the search terms

171. See *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228, 232-33 (D. Md. 2005) (describing inadvertent waiver and its effects).

172. See *Equity Analytics v. Lundin*, 248 F.R.D. 331, 332 (D.D.C. 2008); *Balboa Threadworks, Inc., v. Stuckey*, No. 05-1157-JTM-DWB, 2006 WL 763668, at *5 (D. Kan. March 24, 2006) (both recognizing that search terms can alleviate concerns with privacy, confidentiality, and privilege).

173. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 260 (D. Md. 2008) (noting that “proper selection and implementation obviously involves technical, if not scientific knowledge,” thus making a successful search more challenging to create).

174. *Id.* at 261 (recognizing that “the inherent malleability and ambiguity of spoken and written English” affect the success of a keyword search) (internal quotations omitted).

175. See *Equity Analytics*, 248 F.R.D. at 333 (“Determining whether a particular search methodology, such as keywords, will or will not be effective certainly requires knowledge beyond the ken of a lay person . . . and requires expert testimony.”); see also *Victor Stanley, Inc.*, 250 F.R.D. at 261.

chosen and understand the reasoning behind each. An explanation demonstrating the reasonableness of each term is vital to determining whether inadvertent waiver of privilege has occurred in a balancing jurisdiction.¹⁷⁶ Again, while search terms are useful, this method has inherent limitations and risks and should not be used as a complete solution.

d. Claw Back Agreements

Parties can enter into claw back agreements, also called non-waiver agreements, to prevent waiver by allowing the producing party to recall privileged materials that were unintentionally disclosed if discovered within a reasonable period.¹⁷⁷ In effect, these agreements allow the parties to contract around the general effects of inadvertent production, most notably, waiver.¹⁷⁸ Claw back agreements attempt to address the difficulty, and sometimes apparent impossibility, of performing an individual document review within the period set by the discovery timeline. Although most courts accept and give effect to claw back agreements, some do not.¹⁷⁹ In order to ensure effectiveness and validity of the agreement, parties should ask the court to adopt the agreement in a court order.¹⁸⁰

One of a court's primary concerns with claw back agreements is that parties will enter into the agreement and then fail to do any document review, believing that they can simply assert privilege when the document is later discovered.¹⁸¹ Parties should only use a claw back agreement to facilitate the discovery process, not as a "get out of jail free" card.¹⁸² In order to protect against this result, courts have applied a balancing test to determine whether privilege should be protected if waiver occurred under a claw back agreement.¹⁸³ First, the party must demonstrate the reasonableness of precautions taken to prevent disclosure in light of the amount of time available and the number of documents searched.¹⁸⁴

176. See *Victor Stanley*, 250 F.R.D. at 261; *Hopson*, 232 F.R.D. at 236 (both discussing and outlining the "balancing approach" to privilege waiver).

177. *Hopson*, 232 F.R.D. at 232.

178. EDNA SELAN EPSTEIN, *THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE*, 286-92 (4th ed. 2001).

179. See *Koch Materials Co. v. Shore Slurry Seal, Inc.*, 208 F.R.D. 109, 118 (D.N.J. 2002) (refusing to accept a claw back agreement, believing that it would lead to poor privilege review which may endanger a client's case).

180. *Hopson*, 232 F.R.D. at 244 (describing inadvertent waiver and its effects and recommending that courts independently determine whether a full privilege review can be accomplished during the timeline, and if not, accepting the agreement into a court order).

181. *Id.* (suggesting that parties should assume a full privilege review is required because of potential effects in a balancing jurisdiction, but regardless of the jurisdiction, should always attempt to complete a thorough privilege review).

182. *Id.*

183. *Id.* at 243. This test is essentially an abbreviated version of the "balancing approach" test for inadvertent waiver. See also *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 261 (D. Md. 2008).

184. *Hopson*, 232 F.R.D. at 242.

Next, the party must show that it took reasonable steps to promptly assert privilege.¹⁸⁵ Finally, the court must have compelled the production of the document.¹⁸⁶ If a party can show that its actions were reasonable and justified, a court will likely protect the privilege.¹⁸⁷

Claw back agreements seem to provide some protection in situations where forensic imaging is compelled. In theory, to protect privilege under a claw back agreement, a producing party needs only to assert privilege to each relevant document in a timely manner. However, although claw back agreements are becoming more accepted, some risks still exist. First, jurisdictions vary in their approach and acceptance of them, so it is important to be aware of local rules. Also, while these agreements are respected in federal courts, waivers that occur under them in state courts may not be protected, and local rules and court discretion will determine their acceptance.¹⁸⁸ Additionally, claw back agreements only apply to privilege, so they do not protect against the invasion of privacy or breach of confidentiality. Therefore, while this is an apparent solution to privilege waiver, it does not address the two other primary concerns discussed above.

2. A Model Protocol

Should the court need to facilitate an agreement as to the parameters of forensic imaging or compel discovery, it is imperative that any protocol provided include restrictions and clear limitations in order to protect the interests of the parties. Several courts have outlined protocols that attempt to address and protect these concerns.¹⁸⁹ One protocol designed by the court in *Playboy Enterprises, Inc. v Welles* has been adopted by other courts.¹⁹⁰ The first step in this protocol was the court would appoint a computer expert to create the image.¹⁹¹ The court stated that the parties could either agree upon an expert, or if they could not reach an agreement, the court would choose an expert from a

185. *Id.*

186. *Id.* (describing inadvertent waiver and its effects). Courts have recognized that disclosure of privileged information is not a waiver if the production was judicially compelled. *See also* *Equity Analytics v. Lundin*, 248 F.R.D. 331, 334 (D.D.C. 2008).

187. *Hopson*, 232 F.R.D. at 243.

188. *See* *Henry v. Quicken Loans, Inc.*, No. 04-40346, 2008 WL 474127, at *1 (E.D. Mich. Feb. 15, 2008) (noting that “absent further Congressional action, the Rules Enabling Act does not authorize modification of state privilege law.” Thus, claw back agreements may not prevent waiver under state law).

189. *See, e.g.*, *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 653-54 (D. Minn. 2002); *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-42 (S.D. Ind. 2000); *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1054-55 (S.D. Cal. 1999).

190. *Playboy Enters., Inc.*, 60 F. Supp. 2d at 1054-55. *See Simon Prop. Group L.P.*, 194 F.R.D. at 641-42 (acknowledging the protocol and adopting the *Playboy* protocol with some adjustments).

191. *Playboy Enters., Inc.*, 60 F. Supp. 2d at 1054-55.

list provided by the parties.¹⁹² The court would then designate the expert as an officer of the court and have him sign a protective order.¹⁹³ Next, the court ordered the parties to agree to a date and time for the imaging based on the producing party's schedule, so that the imaging would only minimally interrupt the producing party's business.¹⁹⁴ The court then stated that the created image should be given to the producing party's counsel for review, who should provide any responsive documents to the requesting party.¹⁹⁵ Finally, the court stated that the producing party's counsel would retain the mirror image until the litigation had concluded.¹⁹⁶

This protocol adequately addresses most concerns of the producing party and balances the needs of the requesting party. Appointment of the expert by the court minimizes concern of loyalty or bias to either party because the expert is appointed by a neutral figure, thus diminishing the appearance of an employer/employee relationship.¹⁹⁷ Declaring the expert an officer of the court and issuing a protective order protects against privacy and privilege concerns to the extent possible.¹⁹⁸ The protocol also provides a period during which the producing party's counsel can review for privilege. In addition to this safeguard, if the parties execute and the court accepts a claw back agreement, all privilege concerns should be alleviated.

While this protocol addresses many concerns, it has some deficiencies. First, the order specifically states that the date is subject to the producing party's schedule.¹⁹⁹ Assuming that forensic imaging is compelled because of the producing party's noncompliance with past discovery orders, allowing the date for imaging to depend on this same party may prove problematic. For example, the party could continually delay the imaging by claiming to be busy. This would hinder the preservation of data and potentially allow data to be lost or destroyed, which would defeat the primary purpose of compelling forensic imaging. To prevent this result, the court should include a deadline by which the

192. *Id.*

193. *Id.* The court believed that if the expert was both an officer of the court and bound by a protective order, the producing party's privacy and privilege concerns would be alleviated. *Id.* The court also stated that the imaging process would not constitute a waiver. *Id.*

194. *Id.* The court also specified that only the producing party's counsel and the producing party could be present while the expert created the image. *Id.* Accordingly, the requesting party could not be present.

195. *Id.* (The court stated that documents withheld based on a privilege claim would be recorded in a privilege log).

196. *Id.*

197. *See Menke v. Broward County Sch. Bd.*, 916 So. 2d 8, 10 (Fla. Dist. Ct. App. 2005) (acknowledging the producing party's concern that any confidential or privileged communications would be revealed to the opposing party's paid representative).

198. Courts generally accept these measures as adequate protection against such concerns. *See, e.g., Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 653-54 (D. Minn. 2002); *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-42 (S.D. Ind. 2000).

199. *Playboy Enters., Inc.*, 60 F. Supp. 2d at 1054-55.

imaging must occur. This would accommodate the producing party's schedule while balancing the need for expediency.

The next deficiency with the protocol is that the producing party retains possession of the only copy of the image.²⁰⁰ Again, assuming that forensic imaging is only compelled if the producing party is either destroying information or failing to preserve it, allowing that same party to retain the only copy of the image poses an obvious danger. The producing party's reputation is already in question, and if that party keeps the only copy of the image, it cannot be verified whether all information is in fact being produced. However, this concern can be avoided if the expert submits a copy of the image to the court, which should be viewed only if necessary.²⁰¹

Additionally, the expert should file a report with the court outlining the work performed and the volume and types of records submitted to the producing party's counsel.²⁰² This would allow the court to compare the number of total documents preserved with the amount of documents provided to the requesting party. Therefore, while the protocol used in *Playboy Enterprises, Inc.* is a good starting point, these extra steps should give the requesting party confidence that the information is adequately preserved and available for discovery while protecting the producing party's interests of privacy, confidentiality, and privilege.

V. CONCLUSION

In 2006 the Federal Rules of Civil Procedure were amended to address e-discovery issues, and courts continue to define the rules and their boundaries. *John B. v. Goetz* is an example of this process. Here, the court correctly set aside orders compelling unrestricted forensic imaging of the defendant's computers.²⁰³ The court determined that the issues of privacy and confidentiality significantly outweighed the need to compel unrestricted forensic imaging.²⁰⁴ Unrestricted forensic imaging should rarely, if ever, be compelled because it potentially results in an invasion of privacy, breach of confidentiality, and waiver of privilege. Therefore, the *John B. v. Goetz* court correctly applied this principal and in doing so, effectively limited the breadth of e-discovery.

200. *Id.*

201. For example, if reasonable suspicion exists that the producing party is not providing relevant information that may be stored in the image, the court should review its copy.

202. See *Simon Prop. Group L.P.*, 194 F.R.D. at 641-42. The court here adopted a protocol similar to that used in *Playboy Enters., Inc.*, but it made a few adjustments. *Id.* One of these changes was to require the expert to provide the court with a report that outlined the general work performed and the results (volumes and types) recovered. *Id.*

203. *John B. v. Goetz*, 531 F.3d 448, 461 (6th Cir. 2008).

204. *Id.* at 460-61.